Finance & Cyber Security: Uncovering Underlying and Consequential Costs of Security Breaches and Investments



Dennis D. Malliouris
New College
University of Oxford

A dissertation submitted for the degree of Doctor of Philosophy

Trinity Term 2021

Acknowledgements

First and foremost, thanks to Professor Andrew Simpson, who continuously provided outstanding supervision, prompt and helpful feedback, encouragement, and advice, despite the difficulties introduced by COVID-19. His support greatly facilitated my academic and professional development.

My sincere appreciation and gratitude to Kerstin. Your help and encouragement have been priceless. I am also very grateful to my family for instilling me with a strong sense of ambition and determination, and for tirelessly backing me throughout my years of studies. A big thank you to all friends in Oxford, London, and beyond, without whom this academic journey would not have been as much fun as it was.

Furthermore, my thanks go to all lecturers and previous academic supervisors at Oxford, LBS, UCL, and FOM who imparted their wisdom and encouraged me to pursue this DPhil. I thankfully acknowledge scholarships and grants by New College, the EPSRC/Centre for Doctoral Training in Cyber Security, Willis Towers Watson, and Altana Wealth. Thank you to Alphons and Max, as well as 2iQ, for the continuous interest in my work and for helping me collect some of my research data.

Abstract

Severe security breaches can be costly for publicly listed firms. In order to deploy scarce resources in the most efficient way, information security decision makers in such firms need to conduct holistic economic cost-benefit analyses that take into account all costs associated with security breaches and strategic investments in countermeasures. In addition to obvious direct costs following security breaches and investments, there are also multiple indirect underlying and consequential costs introduced or elevated by such events. In this dissertation, four novel cost elements affecting firms' financing costs that are prone to be overlooked in basic cost-benefit analyses are discussed. Over the course of four empirical studies, the effect of security investments on firm value (via abnormal returns) as well as the effect of security breaches on cost of equity (via systematic risk), cost of debt (via credit default swap spreads), and information asymmetries (via insider trading-induced abnormal returns) are analysed. These studies reveal four cost elements that can all be characterised as indirect underlying/consequential financial costs, which ought to be considered in holistic economic information security cost analyses.

Analysing a US-centric sample of 202 severe security breaches between 2005 and 2019 revealed that severe security breaches are associated with significantly positive increases of insider trading abnormal returns (hence information asymmetries) and systematic risk (hence cost of equity). However, the examination of CDS spread changes following the same severe breach announcements indicated that CDS spreads (hence default spreads and by implication cost of debt) do not increase significantly in the immediate days surrounding the event, suggesting that costs of debt are subject to different dynamics.

Furthermore, assessing an international sample of 221 security investments, the dissertation reveals positive and negative effects on firms' market value following upon small-scale and large-scale security certificate investments, respectively. These market reactions constitute secondary benefits and underlying/consequential costs that also ought to be taken into account for the purpose of expected net benefit of information security (ENBIS) analyses. Collectively, these insights suggest highly relevant information security-induced implications for cost of capital that need to be recognised in ENBIS calculations.

Given the absence of a formal definition of the cost type *underlying/consequential costs* and a framework or model to facilitate assessments of such costs, this dissertation also provides a novel nuanced definition of indirect costs of information security and the Iceberg Model of Information Security Costs, which will help guide further academic research and practitioners' investment endeavours.

Contents

1 Introduction **1**

1.1 Motivation, Overview, and Research Problem 1
1.2 Contributions 5
1.3 Structure 7
1.4 Publications and Research Dissemination 9
1.4.1 Peer-Reviewed Publications 9
1.4.2 Personal Contributions 11
1.4.3 Other Dissemination of Research Findings 12

2 Background and Motivation **13**

2.1 Financial Economics of Information Security and the Firm 14
2.2 Information Security Investments 19
2.3 Costs of Information Security Investments and Breaches 24
2.3.1 Costs of Information Security Investments 24
2.3.2 Costs of Information Security Breaches 25
2.4 Cost Classification: Underlying and Consequential Costs of Security Investments and Breaches 28
2.5 Financing Costs 33
2.6 Security Investment Costs: Firm Value 37
2.7 Security Breach Costs: Cost of Equity 43
2.8 Security Breach Costs: Cost of Debt 47
2.8.1 Cost of Debt and CDS Spreads 48
2.8.2 Prior Empirical Studies and Hypothesis Development 53
2.9 Security Breach Costs: Information Asymmetries 58
2.9.1 Firm-Level Events' Impact on Information Asymmetries 59
2.9.2 The Need for an Advanced Measurement of Information Asymmetries 61
2.9.3 Alternative Information Asymmetries Measurement and Hypothesis Development 63

3 Methodology **68**
3.1 Data Sources and Sample Characteristics: Empirical Dataset Security Investment Costs . . . 68
3.1.1 Cyber Essentials (Plus) . . . 68
3.1.2 ISO/IEC 27001 . . . 70
3.1.3 Combined Regression Sample . . . 72
3.2 Data Sources and Sample Characteristics: Empirical Dataset Security Breach Costs . . . 73
3.3 Other Data and Ethics Approval . . . 76
3.4 Empirical Methodology: Investment Value Creation and Destruction / Asset Disposal . . . 77
3.4.1 Analytical Procedure: Abnormal Returns Analysis . . . 77
3.4.2 Illustration of Abnormal Returns Analysis . . . 80
3.4.3 Analytical Procedure: Regression Analysis . . . 81
3.5 Empirical Methodology: Systematic Risk / Cost of Equity . . . 82
3.5.1 Analytical Procedure: Betas and Dual-Betas . . . 82
3.5.2 Illustration of Beta and Dual-Beta Analysis . . . 85
3.5.3 Analytical Procedure: Regression Analysis . . . 86
3.6 Empirical Methodology: Credit Default Swap Spreads / Cost of Debt . . . 87
3.6.1 Analytical Procedure: Changes in CDS Spreads . . . 87
3.7 Empirical Methodology: Insider Trading Abnormal Returns / Information Asymmetries . . . 94
3.7.1 Analytical Procedure: Changes in Insider Trading Abnormal Returns 95

4 Security Investment Costs: Firm Value **100**
4.1 Overview . . . 100
4.2 Empirical Results Cyber Essentials (Plus) . . . 101
4.3 Empirical Results ISO/IEC 27001 . . . 103
4.4 Empirical Results Regression Analysis . . . 105
4.5 Summary of Empirical Results . . . 105
4.6 Discussion of Empirical Results . . . 108
4.6.1 Cyber Essentials (Plus) Certificates . . . 109
4.6.2 ISO/IEC 27001 . . . 111
4.6.3 Factors Influencing Security Certification Abnormal Returns . . . 113
4.6.4 Limitations . . . 114
4.7 Conclusion on Security Investment-Induced Firm Value Implications . . . 115

5 Security Breach Costs: Cost of Equity **117**
5.1 Overview . . . 117
5.2 Empirical Results Regular Beta . . . 118
5.3 Empirical Results Upside Beta . . . 120
5.4 Empirical Results Downside Beta . . . 122
5.5 Empirical Results Regression Analysis . . . 124
5.6 Summary of Empirical Results . . . 125
5.7 Discussion of Empirical Results . . . 126
5.7.1 Illustration of Changes in Cost of Equity . . . 127
5.7.2 Changes in Regular, Downside, and Upside Beta . . . 127
5.7.3 Factors Influencing Changes in Beta . . . 131
5.7.4 Limitations . . . 132
5.8 Conclusion on Breach-Induced Changes in Cost of Equity . . . 132

6 Security Breach Costs: Cost of Debt **136**
6.1 Overview . . . 136
6.2 Empirical Results Matching-Portfolio Approach . . . 139
6.3 Empirical Results Regression Model Approach . . . 141
6.4 Discussion of Empirical Results . . . 144
6.4.1 Irrelevance to Public Debt Investors . . . 145
6.4.2 Cost of Debt Impact Substantiates Subsequently . . . 147
6.4.3 Cost of Debt Impact Substantiates Priorly . . . 149
6.4.4 Limitations . . . 150
6.5 Conclusion on Breach-Induced Changes in Cost of Debt . . . 151

7 Security Breach Costs: Information Asymmetries **155**
7.1 Overview . . . 155
7.2 Empirical Results Regression Model . . . 156
7.3 Discussion of Empirical Results . . . 162
7.4 Conclusion on Breach-Induced Changes in Information Asymmetries . . . 169

8 Conclusion **172**
8.1 Contributions & Implications . . . 172
8.1.1 Empirical Contributions . . . 172
8.1.2 Methodological Contributions . . . 174
8.1.3 Overarching Model Contributions . . . 176
8.2 Future Research . . . 180

8.3 Conclusion 185

A Cyber Essentials (Plus) Certifications Sample 234

B ISO/IEC 27001 Certifications Sample 249

C Severe Security Breaches Sample 258

D Indices Used To Establish Abnormal Investment Returns 265

E Indices Used To Proxy The Market Portfolio 266

F Descriptive Statistics: Regular Beta per Event 267

G Descriptive Statistics: Upside Beta per Event 274

H Descriptive Statistics: Downside Beta per Event 281

I Descriptive Statistics: Changes in Regular, Upside, and Downside Beta per Event 288

J Overview Matched CDS Control Portfolios 295

K CDS Competitor Portfolios 299

L CDS Regression Sample: Country Indices, Risk-Neutral Rates, Volatility Indices 311

Chapter 1
Introduction

This chapter provides the general motivation for the research topic. It sets out the relevance of the field, the overarching research question, a summary of the underlying empirical studies, and the contributions of this dissertation. Some paragraphs describing previous work are based on [1] and [2].

1.1 Motivation, Overview, and Research Problem

Security vulnerabilities and malicious actors pose a material threat to for-profit firms in the 21st Century. Substantial costs of data breaches for organisations [3], the increasing number of annual security breaches [4], and regulators' GDPR-fuelled power to fine organisations failing to handle breaches appropriately have put information security issues higher up on boardroom agendas [5].

From a high level perspective, corporate information security[1] constitutes an exemplary case of what economics, business, and social policy scholars refer to as a "wicked problem". Defining the problem and formulating influencing factors is difficult, information is incomplete, interdependent and contradictory, immediate heuristics or tests of potential solutions do not exist, and there is no finite solution to the overarching problem [7–12]. Information security is hence not exclusively a technical, social, or individual concern, but rather an issue that merits and requires multidisciplinary research and consideration of interconnected sociotechnical aspects to manage risk.

Taking an economic perspective on information security is thereby not a necessary evil to facilitate a holistic approach towards secure systems and societies. Instead, it is possible to argue that economic considerations actually inform the entirety of all individual and

[1] Throughout this dissertation, the term information security is used to refer to the confidentiality, integrity, and availability of data in for-profit organisational settings (see ISO/IEC 27000:2018 [6]). Synonymous terms such as system security, computer security, or cyber security are understood to be referring to similar concepts.

organisational actors' security-related actions and behaviour (cf., [13]), which led to the emergence of information security economics as a research field [13–16]. This dissertation contributes to this nascent field of research by using corporate financial economics to work towards solutions of fundamental information security issues.

Suffering from severe security breaches can be costly for organisations, but so is investing in security countermeasures. Strategic investments in security systems and processes hence constitute a major issue within information security economics. Organisational actors generally, and for-profit organisations specifically, are fundamentally concerned with the most efficient deployment of capital [17, 18], and hence strive to invest in information security strategically in a value-maximising way as to avoid unnecessary costs and generate excess returns[2].

Security executives thereby need frameworks and metrics to guide their investment processes. Suitable noteworthy tools such as ENBIS[3] exist. However, despite the plethora of studies and surveys revealing direct and obvious costs to organisations induced by information security breaches and investments, there is little to no evidence discussing other major indirect economic costs introduced or elevated by information security breaches and investments, although such hidden costs may actually exceed direct costs in gravity [26] (see also [27–30]). Accordingly, economic frameworks and metrics do not account sufficiently for indirect costs and virtually neglect what in this dissertation is termed *underlying and consequential costs*, that is, indirect non-obvious or hidden costs of intangible nature that can lead to higher observable direct costs or that manifest themselves subsequent to direct costs elicited by a breach or investment.

As a result, there is a gap in the literature pertaining to indirect underlying / consequential costs associated with investments in and breaches of information security. This dissertation presents research that worked towards closing this gap in the literature by promoting a more holistic perspective on information security costs[4] and revealing empirical evidence of four novel underlying / consequential cost elements that all contribute to changes in financing costs. The research reported on in the following chapters worked towards closing the gap in the literature by finding an answer to the overarching research question:

[2]Excess returns are returns realised in excess of a benchmark [19,20]. Common benchmarks are alternative investments and the risk-free rate, proxied by government debt instruments.

[3]ENBIS is the Expected Net Benefit of Information Security, which quantifies the benefit of investing in security controls by taking into account mitigated losses (λ) and the costs (c) to achieve the lower level of losses. See [21–25] and Section 2.2 for further explanations of this metric and framework.

[4]Here, information security costs refers to costs incurred by firms investing in information security and costs associated with security breaches.

> "How can publicly listed firms leverage financial market data to achieve a better understanding of costs associated with information security to conduct more thorough information security investment cost-benefit analyses?"

Ideally, this dissertation would provide a definitive and conclusive list of all potential direct and indirect costs of information security. Unfortunately, such a list, and thereby a universal answer to the overarching problem of quantifying ENBIS, is highly context-specific, potentially impossible to find, and hence out of the scope of the present dissertation. Similarly, the dissertation does not aim to make claims as to the optimal amount of security investments or the quality of particular information security measures. Instead, the dissertation

- adds four novel indirect underlying / consequential cost elements, which all affect financing costs, to metrics such as ENBIS, and
- introduces a novel cost classification and model to assist security executives in thinking more holistically about information security costs.

This dissertation concentrates on financial market data, as such data offers the major advantage of being both conveniently and cheaply accessible to corporate decision makers. Given that there is only scarce empirical evidence on indirect underlying / consequential costs, existing security investment frameworks such as ENBIS do not sufficiently account for such costs. Accordingly, there is a need to provide evidence of indirect, and specifically underlying and consequential, costs that go beyond direct and obvious costs to inform more holistic ENBIS-based analyses and facilitate information security investment decision making.

One type of underlying / consequential cost *category* is financing costs, which can be subdivided into multiple different underlying cost *elements*. In this dissertation, a particular emphasis is placed on underlying / consequential financing costs as these are particularly relevant due to their twofold nature. On the one hand, changes in financing costs can be regarded as one-off cost factors influencing a particular investment decision at hand via metrics such as ENBIS. On the other hand, more generally, financing costs also constitute long-term costs affecting virtually all corporate operating, investing, and financing activities inter alia via firms' expected returns and discount rates[5].

[5]All terms, including underlying / consequential costs, financing costs, expected rate of return, and discount factors are defined in Chapter 2. Sections 4.6, 5.7, 6.4, and 7.3, and Chapter 8 will demonstrate why covert and often neglected underlying / consequential financing costs can actually be of greater relevance than direct or obvious costs.

In order to work towards an answer of the overarching research question, empirical evidence of, and a novel cost classification and model for, analysing information security investment- and breach-induced costs imposed on publicly listed organisations are provided. In this dissertation, multiple perspectives on the effect of information security events[6] on financing costs are analysed. In the context of four empirical research projects, four novel underlying / consequential cost elements are rendered more salient. Specifically, the effect of security investments on stock prices as well as the effect of security breaches on cost of equity, cost of debt, and information asymmetries are demonstrated. The novel insights on underlying / consequential costs, and the realisation that the ENBIS framework should consider these costs, is leveraged to conceptualise a new model to distinguish information security costs and promote more holistic economic thinking about information security investment generally.

Working towards an answer to the overarching research question constitutes an important contribution to information security economics and is of significant interest to information security executives and policy makers. Previous research has predominantly focused on direct costs and benefits of investments in countermeasures, and has thereby neglected indirect underlying and consequential costs. Establishing a comprehensive information security costs model that accounts for underlying and consequential costs will allow corporate executives and institutional legislators to make better informed decisions with regards to security investments and policy making (e.g., pertaining to security breach notification laws). More generally, by demonstrating additional costs to senior corporate decision makers, they might become more inclined to invest resources in information security. Accordingly, from a security perspective, the research endeavour to make underlying and consequential costs more salient might result in a safer cyber security environment for society at large, given the negative externalities caused by the interdependence of security systems [31]. From a financial perspective, revealing additional information security costs can inform investors' price discovery processes and lead to more efficient markets as public firms exist in a multilaterally-interacting complex economic ecosystem. Moreover, it is hoped that future academic studies might benefit from the new cost classification and framework by prompting researchers to think more holistically about potential costs and benefits associated with information security investments.

[6]Here, information security events refers to breaches of information security and investments in countermeasures.

1.2 Contributions

This dissertation works towards closing the gap in the literature pertaining to indirect information security costs by promoting a more holistic perspective. The two overarching contributions, providing evidence of novel underlying / consequential cost elements and introducing a new cost classification and model, are based on four empirical contributions revealing evidence of four novel underlying / consequential cost elements that substantiate either subsequently to or simultaneously with direct costs and all affect firms' financing costs.

There are multiple possible perspectives on financing costs. Three major ones are firms' information asymmetries, the weighted average cost of obtaining external capital, and the ability to generate internal financing. In this dissertation, all three major perspectives on public firms' financing costs are analysed across four empirical contributions (**C1** – **C4**), revealing four novel indirect underlying / consequential cost elements, which all affect one cost type — financing costs — that ought to be considered in holistic ENBIS analyses.

C1 constitutes the first study to quantitatively analyse the impact of information security standards implementation on firms' market values across different types of standards and multiple countries. The study shows that investments in ISO/IEC 27001 certificates are associated with indirect consequential costs in the form of equity value destruction, whilst Cyber Essentials (Plus) investments carry negative costs (i.e., secondary benefits) in the form of equity value creation. **C1** contributes evidence of changes in the value of an internal financing instrument, namely assets in the form of treasury shares[7]. Due to the necessity to obtain alternative sources of capital to maintain a set level of available capital, an increase or decrease in share prices thereby implies changes in financing costs that ought to be considered as an additional cost or secondary benefit element in the information security investment costs part of ENBIS calculations (c).

C2 consists of the provision of novel empirical evidence on underlying and consequential costs imposed on firms by security breaches. Previous work that used small and now-outdated samples [33–35] is extended by using a new self-produced dataset, which allows for presenting more holistic, useful, and updated empirical insights into the effect of security breaches on firms' systematic risk. Additionally, this is the first analysis of "a more appropriate measure of portfolio risk" [36, p. 265], namely dual-beta models, in addition to regular betas. The analysis reveals that cost of equity in terms of regular and downside betas increase following

[7]Treasury shares are shares a firm has repurchased but not cancelled [32]. Firms may sell treasury shares to inside and outside investors, award them to executives as part of their remuneration packages, or use them as a means of payment, particularly in mergers and acquisitions.

security breaches, which leads to an increase in weighted average cost of capital (WACC) and hence financing costs that needs to be considered in the λ part of ENBIS calculations.

C3 is based on the first scholarly analysis of changes in credit default swap (CDS) spreads following security breaches. The study provides insights into asymmetrical breach-induced increases in firms' cost of debt, another underlying and consequential cost of information security breaches. Analysing CDS spreads reveals that cost of debt increases following security breaches, which lead to an increase in WACC and hence financing costs that needs to be considered in the λ part of ENBIS calculations, are not driven by short-term changes in default risk as proxied by CDS spreads.

C4 constitutes the first analysis into long-term principal-agent information asymmetries, a cost type underlying many other directly observable costs associated with information security breaches. Using insider trading abnormal returns, a measure that is still nascent to the corporate strategy-related literature[8] and which relies on difficult-to-collect data[9], as a proxy, it is shown to what extent information asymmetries are exacerbated by security breaches. The study reveals that security breaches lead to increases in information asymmetries that in turn result in elevated financing costs and hence an additional cost element in the λ part of ENBIS calculations.

In response to the overarching research question of how publicly listed firms can use financial market data to achieve a more holistic understanding of information security costs, this dissertation makes a threefold **overarching contribution**.

- First, on a fundamental level, this dissertation confirms that executives in publicly listed firms intending to invest strategically in information security can conveniently use financial market data to establish indirect information security costs.
- Second, by providing novel empirical evidence of four underlying / consequential cost elements within the category of financing costs, the dissertation demonstrates that

[8]Insider trading means corporate insiders buying/selling financial instruments in their own firms (see Section 2.9.3 for more detailed explanations). The term "corporate strategy-related literature" is used here to refer to the academic literature on the strategic deployment of corporate resources to undertake capital expenditure generally. Using insider trading abnormal returns as a proxy for information asymmetries to analyse corporate decision making is novel, in fact, my paper [37] is amongst the first to do so. Accordingly, as the approach is new to the literature on corporate investments generally, it is also very novel to the literature on corporate finance economics of information security specifically.

[9]US-based companies are required to file forms pertaining to corporate insiders trading shares of their own firms with the SEC. In Europe, insider transaction filings are more dispersed and need to be obtained from the respective country's market authorities, stock exchanges, financial news, and company websites.

current security investment models and metrics need to be extended by also taking into account costs that go beyond direct and obvious costs. The more explicit introduction of different manifestations of financing costs as well as secondary benefits of investments in the ENBIS metric are suggested (see Figure 8.1 in Chapter 8).

- Third, the empirical insights leading to the ENBIS extension, and the peer-reviewed [2] cost classification introduced in the dissertation (see Section 2.4), are leveraged to conceptualise a new model to distinguish information security costs and promote more holistic economic thinking about information security investments generally (see Figure 8.2 in Chapter 8)[10].

The main beneficiaries of this research are publicly listed firms and their executives[11]. The Iceberg Model of Information Security Costs, alongside the specific ENBIS extensions, will enable executives to achieve a more holistic understanding of information security costs. Moreover, the overarching contributions will facilitate further academic research on the underexplored category of underlying and consequential costs of information security.

1.3 Structure

The dissertation will proceed as follows. Chapter 2 introduces the relevant literature in which this dissertation is grounded. Key concepts and terminology, including the novel cost classification distinguishing between obvious and underlying / consequential costs, are introduced. Extant conceptual and empirical literature on financial losses induced by corporate information security investments and breaches is summarised. The focus is thereby on information security financial economics, and in particular corporate finance considerations. Furthermore, we discuss the motivation for analysing underlying and consequential costs of information security in more detail.

Chapter 3 outlines the thorough data collection processes and empirical analysis methodologies used to generate the quantitative insights into underlying and consequential costs of information security investments and breaches. Sections describe how costs in terms of abnormal stock returns, increasing costs of equity and debt, and elevated information asymmetries were measured. The advantages and limitations of using particular data sources and empirical methodologies are also discussed.

[10]The Iceberg Model of Information Security Costs distinguishes between: direct obvious, indirect obvious, indirect underlying / consequential non-financial, and indirect underlying / consequential financial costs.

[11]See Soomro et al. [38] for a recent literature review on the role and high relevance of (senior) managers for information security issues.

Chapter 4 discusses underlying and consequential costs of information security investments. The results of the empirical study are presented and discussed to reveal both negative and positive costs following investments in security standards. It is shown that large-scale investments are associated with significant negative abnormal returns and are hence firm value destructive, whereas in the case of less costly investments, positive abnormal returns indicate firm value creation.

In Chapters 5, 6, and 7 we consider underlying and consequential costs of information security breaches. Chapter 5 outlines the results and implications of the empirical study on increases in financial systematic risk following severe security breaches. Besides using a larger sample than any prior academic study on breach-induced changes in cost of equity, this dissertation's study also uses a more accurate measure. Significant increases in regular, downside, or upside beta thereby indicate heightened cost of equity for breached firms.

Chapter 6 builds upon the previous chapter by considering the other part of firms' cost of capital, namely cost of debt. This chapter provides empirical evidence on the extent to which the financial cost of borrowing capital in terms of credit default swap spreads are increased by security breaches.

Chapter 7 is based on the notion that secretive and difficult-to-analyse firms are associated with heightened information asymmetries. Here, we provide and discuss empirical evidence as to what extent security breaches are associated with increases in information asymmetries vis-à-vis investors.

Chapter 8 unites the four empirical contributions by referring back to the overarching research question. The four empirical contributions culminate in the threefold overarching contribution of this dissertation: demonstrating that security executives can use financial market data to establish indirect information security costs; providing novel evidence of financing costs that ought to be introduced in ENBIS metrics; and establishing a new cost classification and model that might facilitate security executives' more holistic approach towards information security costs. This chapter concludes the dissertation by summarising key insights and their relevance for information security financial economics research and practice. Furthermore, obstacles encountered during the course of the DPhil are reflected on and potential areas of future research are outlined.

Figure 1.1 provides an overview of the structure of this dissertation and how chapters and contributions map onto publications.

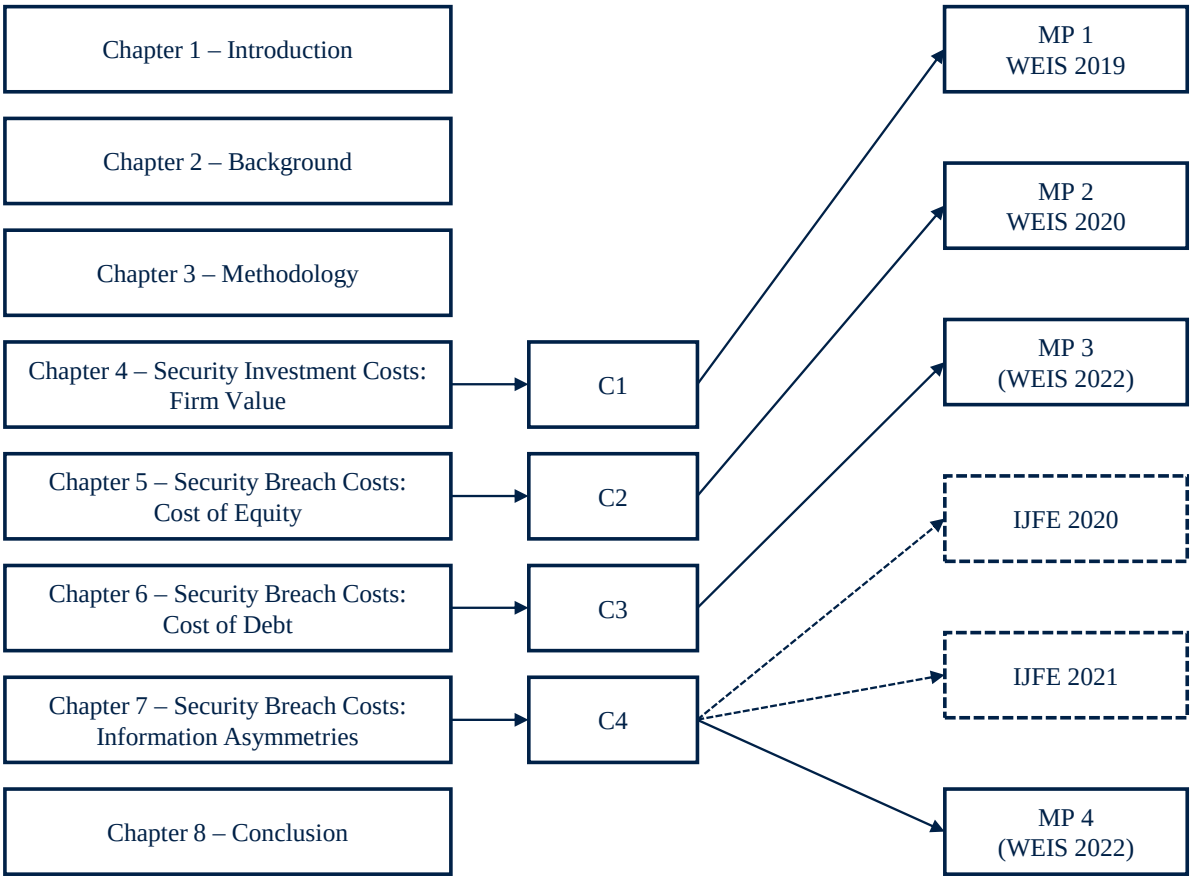


Figure 1.1: Chapters & Contributions

1.4 Publications and Research Dissemination

This section lists the publications of which parts are included in this dissertation and explains my personal contributions to these publications.

1.4.1 Peer-Reviewed Publications

Over the course of my DPhil research pursuit, I authored multiple publications, some of which directly contribute to my endeavour to answer the aforementioned overarching research question (Main Papers). Two additional papers are of more auxiliary nature and indirectly relevant, using similar reasoning and methodologies, and thereby generating necessary ground work and background for the Main Papers, albeit working towards a different

overarching research endeavour.

The following peer-reviewed publications form the basis of this dissertation (in chronological order):

1. *The Stock Market Impact of Information Security Investments: The Case of Security Standards*, DD Malliouris and AC Simpson, published at the Workshop on the Economics of Information Security (WEIS) 2019 [1] (Main Paper 1, **MP1**, provided the basis for Contribution **C1**)

2. *Underlying and Consequential Costs of Cyber Security Breaches: Changes in Systematic Risk*, DD Malliouris and AC Simpson, published at the Workshop on the Economics of Information Security (WEIS) 2020 [2] (Main Paper 2, **MP2**, provided the basis for Contribution **C2**).

3. *Strategy Uniqueness and Insider Trading: Evidence from Europe*, DD Malliouris, AT Vermorken, and MAM Vermorken, awaiting final editor decision at the International Journal of Finance and Economics [37], established the conceptual framing of abnormal returns following insider trades as a proxy for corporate strategy-related information asymmetries that contributed to the line of argumentation in Contribution **C4**. The paper provided some logic, reasoning, and background, the study and findings presented in the paper itself are, however, not part of Contribution **C4**.

4. *Aggregate Insider Trading and Future Market Returns in the US, Europe, and Asia*, DD Malliouris, AT Vermorken, and MAM Vermorken, published in the International Journal of Finance & Economics [39], revealed further empirical evidence of insider trading and information asymmetries that contributed to the line of argumentation in Contribution **C4**. The paper provided some logic, reasoning, and background, the study and findings presented in the paper itself are, however, not part of Contribution **C4**.

5. *Underlying and Consequential Costs of Cyber Security Breaches: Changes in Cost of Debt*, DD Malliouris and AC Simpson, to be submitted (Potential Main Paper 3, **MP3**, will be based on Contribution **C3**).

6. *Underlying and Consequential Costs of Cyber Security Breaches: Information Asymmetries*, DD Malliouris and AC Simpson, to be submitted (Potential Main Paper 4, **MP4**, will be based on Contribution **C4**).

MP1 and **MP2** provided the basis for paragraphs on previous work in Chapters 1 and 2 as well as Sections 3.1 to 3.5 on data collection and empirical analysis. Results and discussions

in Chapters 4 and 5 and some deliberations on contributions, impacts, and potential future research in Chapter 8 are also based on **MP1** and **MP2**.

Publications [37] and [39] provided the basis for some paragraphs in Chapters 2 and 3. The conceptual and empirical connection between insider trading and information asymmetries contributes to the the line of argumentation in Chapter 7.

Using the relevant sections in Chapters 2 and 3, as well as Chapters 6 and 7, it is intended to submit **MP3** and **MP4** to WEIS, the Journal of Cybersecurity, or Computers & Security.

1.4.2 Personal Contributions

I am the main author and only student author on all aforementioned papers and publications, which are hence based on my research and professional experience. All four Main Papers followed a similar work pattern. First, I generated research ideas, which were subject to an iterative presentation and discussion process with my supervisor, Professor Andrew C. Simpson. I then conducted the respective literature reviews, framed the problem, collected and cleaned data, conceptualised empirical analyses, wrote the statistical code in *R*, placed results in their appropriate academic context, assessed results' professional relevance, and wrote drafts on my own. My supervisor provided me with helpful comments on these drafts and suggested necessary changes, which I then implemented. Prior to submitting **MP1** and **MP2** to WEIS 2019 and WEIS 2020, Andrew Simpson undertook final copyediting work, which did not include making any major changes to the underlying content. **MP3** and **MP4** are expected to follow similar editing procedures.

The ideation of [37] was based on my UCL MRes dissertation. The research topic — strategy uniqueness — resulted from conversations with my then-dissertation supervisor who provided helpful comments throughout the MRes dissertation writing process, but was not involved in the eventual publication. For the purpose of [37], the MRes dissertation merely provided a starting point. The research project underwent a general shift in focus and analytical methodology, and all text was substantially changed, extended, or rewritten. Co-author Alphons Vermorken provided me with the necessary data to explore the research question, whilst co-author Maximilian Vermorken offered comments and general feedback on the final draft. However, I conceptualised the empirical analysis, wrote the statistical code in *R*, discussed results from academic and professional perspectives, and wrote the entire paper on my own. Crucially, I conducted the literature review and came up with the underlying reasoning — which is now also applied to **C4** in this present dissertation — of framing abnormal returns following insider trades as a proxy for corporate strategy-induced information asymmetries.

For [39], one of my co-authors, Alphons Vermorken, introduced me to anecdotal evidence that led to the paper's research question and provided me with the necessary data. The other co-author offered comments and general feedback on the final draft. However, I conceptualised the empirical analyses, wrote the statistical code in *R*, discussed results from academic and professional perspectives, and wrote the entire paper on my own. Crucially, I extended the notion of insider trades-induced abnormal returns as a proxy for information asymmetries — which is now also applied to **C4** in this present dissertation — alone and conducted the necessary literature review and discussions upon which the extension of the idea is based.

1.4.3 Other Dissemination of Research Findings

In addition to the peer-reviewed articles mentioned above, I was also invited to present posters of my research findings at the Oxford CDT Showcase Days 2018 and 2019, Newcastle ACE Winter School January 2020, and Oxford Virtual CDT Showcase Day 2020. Besides, a summary of my work on underlying and consequential costs of information security breaches was published in Willis Towers Watson's *The Willis Research Network Brochure 2021* [40]. The insights generated in this dissertation are also used by policymakers as well as corporate and governmental partners of the CDT with whom I discussed excerpts of my work.

Chapter 2
Background and Motivation

This chapter provides the reader with the theoretical, conceptual, and empirical background necessary to frame and motivate the dissertation's contributions. This chapter hereby also defines the scope of the ensuing analysis. There would be little value in merely reiterating basic theories and frameworks. Instead, the chapter presents the literature upon which the scholarly research and empirical contributions of this dissertation are based. This chapter also expands on the motivation for the dissertation's research, demonstrates the gaps in the literature, explains the cost classification of underlying and consequential financial costs used throughout the dissertation, and delineates how the research outcomes are relevant for a better understanding of these non-obvious corporate losses.

This dissertation aims to work towards an answer of the overarching research question *How can publicly listed firms leverage financial market data to achieve a better understanding of costs associated with information security to conduct more thorough information security investment cost-benefit analyses?*, to extend the prevalent ENBIS metric by underlying / consequential financial costs, and to provide a more holistic framework of information security costs. In order to do so, some information security economics terms and models need to be explained, previously-established cost metrics need to be discussed, and the set-up of the empirical studies revealing additional cost elements need to be outlined.

To this end, the chapter is structured as follows. First, we start broadly by recapitulating that information security issues need to be addressed from a multi-disciplinary perspective and that financial economics provide particularly suitable tools to pursue this endeavour. In the respective section (Section 2.1), the basic concept of how senior executives in for-profit firms make decisions and what constraints their planning processes is introduced.

Second, in Section 2.2 the reader is introduced to one of the major topics of information security economics — information security investments. We attend to the reasons why firms choose to invest in information security countermeasures and the economic cost-benefit analysis tools rational executives use to decide what investments to pursue. From the discussion of economic investment decision making, the need to be thorough and holistic in

the assessment of costs associated with security investments and breaches will emerge naturally. Accordingly, Sections 2.3.1 and 2.3.2 cover costs of security investments and breaches typically considered in the security economics literature. It will become obvious that insufficient attention has been devoted to quantifying underlying / consequential indirect costs of security breaches and investments.

Third, Section 2.4 addresses reasons as to why quantifying costs of security investments and breaches is difficult, and provides a novel cost classification that distinguishes between costs that can actually be observed and quantified relatively easily — termed *obvious costs* — and costs that are indeed hidden or invisible — termed *underlying and consequential costs*.

Fourth, the particular cost category this dissertation focuses on, financing costs, is explained in further detail, and three perspectives on financing costs are delineated. In this dissertation, four studies contributing novel empirical evidence on underlying and consequential costs are conducted to facilitate holistic security investment cost-benefit analyses. Staying within the research tradition of corporate financial economics, these studies highlight additional underlying and consequential financial costs to firms. The backgrounds and motivations for each of these four empirical contributions are explained in this chapter. Introducing previous studies, terms, and hypotheses for Contribution **C1** in Section 2.6, Contribution **C2** in Section 2.7, Contribution **C3** in Section 2.8, and Contribution **C4** in Section 2.9, will lay the necessary groundwork for explanations of empirical methodologies in Chapter 3 and discussions of the respective results in Chapters 4, 5, 6, and 7.

Most of Sections 2.1 to 2.7 is based on publications at WEIS 2019 [1] (**MP1**) and WEIS 2020 [2] (**MP2**). Some paragraphs, particularly on corporate finance theory, insider trading, and relevant previous work, are based on my IJFE 2020 [39] and IJFE 2021 [37] papers, in which the conceptual and empirical connection between insider trading and strategy-related information asymmetries is established, forming the underlying basis for the line of argumentation presented in Section 2.9.

2.1 Financial Economics of Information Security and the Firm

As discussed in Chapter 1, mitigating issues of information security is a "wicked problem" that requires holistic interdisciplinary research and practice approaches [7–12]. The research described in this dissertation applies economic theory and methodologies, specifically corporate financial economics, to find solutions to information security issues.

Anderson and Moore [13–16] were amongst the first to formally introduce economic con-

siderations to information security research and practice. Economic principles and deliberations can be used to interpret and inform incentives and motivations of individuals, corporations, and policy makers with regards to their decision making and behaviour in the realm of information security. Economic theory can thereby explain and predict all individual and aggregate actions. Bruce Schneier [41, p. 3] even went as far as saying that "[i]nformation security is not a technological problem. It is an economics problem. And the way to improve information security is to fix the economics problem." For instance, attackers are constrained in their malicious efforts by resources available at their disposal (e.g., time, knowledge of capabilities, and server capacities) [42]. Similarly, non-corporate white-hat hackers are incentivised to discover security flaws by vulnerability rewards programmes [43, 44]. Users and firms self-selecting whether to invest in anti-virus software contribute to a suboptimal security environment when their infected machines spread malware to others [13].

Recalling the overarching research question, *How can publicly listed firms leverage financial market data to achieve a better understanding of costs associated with information security to conduct more thorough information security investment cost-benefit analyses?*, publicly listed firms are the main unit of analysis in this dissertation. These firms were chosen as the subject of the analyses for multiple reasons. From an information security perspective, they are particularly interesting as they need to manage very substantial risks. Defining risk as the product of the probability of a threat successfully exploiting vulnerabilities and the potential impact on assets and objectives [6, 45, 46], publicly listed firms score high across all factors. Successful attacks may threaten publicly listed firms' core objectives and their very existence, as organisations possess a multitude of valuable digital assets and resources (see [47–50]). Publicly listed firms present a large attack surface due to a plethora of interconnected systems, processes, and people (see [51–53]). Moreover, focusing on corporate information security is beneficial as improved corporate information security and resilience can result in positive spillover effects on other organisations, individuals, and society at large.

From a financial economics perspective, firms' information security behaviour is more interesting to analyse than, for instance, the behaviour of private individuals, as firms invest greater resources and are more incentivised to manage their information security risk economically and rationally. Additionally, even though policy makers introduce legislation intending to contribute to a safer cyber space environment for society in general (see e.g., [54, 55]), firms are not necessarily motivated by such ethical or noble considerations, but rather by financial motivations (see e.g., [18, 56–61]). Put plainly, if the decision to actively manage information security risk is not economically reasonable, a firm would be unlikely to pursue it.

Within neoclassical economic theory, firms are thought of as organisations existing to construct and exploit competitive advantages and to mitigate issues of market failures and transaction costs [62–66][1]. Firms pursue strategies based on combinations of resources, capabilities, and processes that are valuable, rare, inimitable, unsubstitutable, and inelastic-in-supply to increase customers' willingness-to-pay or to reduce costs of supply [47, 67–72]. These corporate strategies are an amalgamation of trade-off decisions striving to find the most suitable answers to the questions what goods and services a firm plans to sell to whom, and most importantly here, *how* the firm intends to conduct its corporate operations [73, 74]. Information security investments and financing costs, the considerations at the centre of this dissertation, can both be considered parts of the overarching corporate strategy making processes.

Traditional neoclassical economic theory postulates that firms' overarching goal is to "make as much money as possible while conforming to the basic rules of the society, both those embodied in law and those embodied in ethical custom" [75]. In practice, this means that corporate executives' inherent task, and part of their fiduciary duty, is to facilitate maximisation of corporate value for stakeholders [17, 76, 77], which implies increasing share prices on behalf of equity investors [18, 75, 78–81]. It is worth noting that the overarching goal of maximising value for all stakeholders, and predominantly shareholders (i.e., increasing share prices), does not necessarily run counter to seemingly unrelated or contradictory goals that might at first glance limit a firm's ability to achieve superior profitability, such as corporate sustainability. Indeed, there is an entire body of research focusing on how such goals can rather be perceived to be of subsidiary nature as they contribute to the overall endeavour of increasing performance in terms of firm value[2] and accounting measures (see e.g., [17,83–85]). Relatedly, executives are also personally incentivised to avert negative stock market returns as they tend to be remunerated in equity or equity-based options [86–88]. Executives are hence professionally and personally highly incentivised to invest their firms' scarce resources[3] in the most profitable way. Corporate decision makers are thereby assumed to be, in the broader sense of the word, economic: they are "boundedly rational" and "satisfice" by making limitedly rational decisions taking into account expected costs, benefits, and utilities to the best of their abilities and knowledge of relevant information [90–93].

In the same vein as corporate responsibility can constitute a subsidiary goal to profit

[1]Human and transactional factors leading to market failures include bounded rationality, opportunism, atmosphere, uncertainty, low frequency of transactions, and information impactedness [63].

[2]Note that firm value, or enterprise value, is the market value of a firm's core business operations to all investors, defined as the sum of a firm's equity value, net debt, preferred stock, and non-controlling interests [82].

[3]See [89] for the concept of Scarcity in economics.

maximisation, corporate information security can also be considered conducive to and of strategic relevance for firms' overarching goals (see e.g., [94]). In this dissertation, the firms' boundedly rational (information security) executives are also assumed to invest strategically in information security in the most economic, shareholder value-maximising manner — by way of maximising cash flows to the firm, investing in the most cost-efficient value-generative information security projects, and mitigating financing costs — whilst not being entirely risk neutral in the strict neo-classical sense, but rather paying particular attention to potential downside risks.

Within the wide-ranging field of information security economics, there are multiple potential theoretical traditions in which empirical research explaining and informing corporate executives' information security investment decision making can be grounded. For instance, a number of studies (e.g., [95–97]) apply the *resource-based view of the firm* [48, 50, 98–100] to postulate that occurrences of security breaches are associated with the heterogeneity in security resources at the firms' disposal.

Whilst the resource-based view of the firm inevitably plays a role in corporate information security investment endeavours, the research described in this dissertation focuses less on the type of information security resources available to the firm, but rather on the decision to invest in such resources in the first instance. The research presented here is primarily informed by corporate financial economics, or specifically, the shareholder value approach, which is sometimes also referred to as the value-based planning, or value-based management, approach [17, 18, 56–61]. In the context at hand, this particular perspective conjectures that security executives base their strategy and investment decisions on quantitative metrics informed by deliberations whether and to what extent information security investments generate positive net economic benefits for shareholders and other capital providers of the firm.

Financial economics, "the study of allocation and deployment of economic resources, both spatially and across time, in an uncertain environment" [101, p. 323], as a stream of research and practice goes back to the works by Irving Fisher [102, 103] and John Burr Williams [104] in the early 20th Century. They argued that firms' main purpose, the maximisation of shareholder value, is driven by considerations of discounted future cash flows[4], which provide an intrinsic valuation to derive market values and stock prices. Fama's Efficient Market Hypothesis (EMH) [108, 109] added an important temporal perspective to financial economics,

[4]The discounted cash flow (DCF) analysis is used to calculate the net present value (NPV) of the firm. The empirical correctness of the original assertions has been empirically proven multiple times (see e.g., [105]). To this day, DCF analyses, which are closely related to Gordon and Shapiro's [106, 107] Dividend Discount Model using dividends and the notion of perpetual growth under conditions of certainty, are amongst the most frequently used methodologies to calculate the intrinsic fair market value of companies [82].

postulating that investors adjust any cash flow and risk expectancies immediately following the release of new information on the respective firm. Most importantly for the analyses in this dissertation, as a publicly listed company is eventually merely the accumulation of all of its operations and assets, the same logic also applies to all operational and capital expenditures, that is, investments. Accordingly, the NPV of ENBIS discussed in Section 2.2 is based on the same principle.

Computing the present value of a firm or project by means of discounting future benefits requires knowledge of expected cash flows and the rationally appropriate discount rate reflecting the underlying risk of said cash flows [110]. A strong body of widely-cited financial principles and models has emerged endeavouring to resolve the discount rate problem. The discount factor is based on considerations of the time value of money, uncertainty, risk, and opportunity costs, and is hence typically calculated based on the cost of capital or investors' expected rate of return [110]. Capital markets are not "perfect" in terms of the Modigliani-Miller theorem, which postulates that in perfectly efficient capital markets, given the absence of taxes, insolvency costs, agency costs, information asymmetries and other market frictions, the value of a firm is independent of its capital structure [111]. As these conditions are violated in practice, the theorem provides the tools to consider changes in discount rates and hence value. Accordingly, appropriate cash flow discount rates are dependent on firms' capital structures, the risk of bankruptcy, market frictions such as information asymmetries, and eventually the resulting after-tax weighted average cost of capital (WACC) factoring in cost of equity and cost of debt [110, 112–116]. Costs of equity are based on the seminal Capital Asset Pricing Model (CAPM), formulated by Sharpe [117, 118], Lintner [119], Treynor [120], and Mossin [121] based on Markowitz's Modern Portfolio Theory [57, 122], which establishes equity investors' expected rate of return on a firm's stock taking into account the expected risk-free rate, the expected market return, and the stock's sensitivity to market risk.

Corporate financial economics leverages the aforementioned concepts, takes the perspective of capital users (i.e., firms), and analyses how such entities make financial decisions. The field of research is concerned with corporate investment and financing decisions, that is, the acquisition of real assets and the sale of securities and other financial instruments. The two most important considerations hence become the expected benefits from investments flowing to the firm, and the way in which capital to finance these investments is obtained [110]. Financial executives use principles of financial economics as laid out above to make decisions and maximise shareholder value. For instance, they use the CAPM to determine their shareholders' expected rate of return; attempt to mitigate their financing costs by minimising WACC; calculate the fair value of an acquisition target using DCFs; and assess potential capital expenditure projects by discounting expected cash flows from the investment at the

appropriate rate determined by their WACC to establish NPVs.

In the context of this dissertation, we are concerned with both elements of corporate finance: investments and financing. First, this dissertation discusses corporate investments in information security and the NPV of ENBIS, the appropriate metric to analyse the economic benefit stemming from information security investments, which — as will be argued in the following sections — ought to be extended by additional cost and benefit elements that are all connected to financing costs. Second, by empirically analysing cost elements that affect financing costs, this dissertation also speaks to the other dimension of corporate finance, namely financing decision.

All financial economics concepts introduced above will be taken up again throughout this dissertation. Relevant concepts will be explained in further detail when applying the respective formulas in the empirical studies. Specifically, in **MP1** (Sections 2.6 and 3.4, and Chapter 4), an extension of the CAPM based on the EMH is applied to calculate value creation in terms of abnormal returns. In **MP2** (Sections 2.7 and 3.5, and Chapter 5), financial models based on the CAPM are used to analyse changes in beta. **MP3** (Sections 2.8 and 3.6, and Chapter 6) and **MP4** (Sections 2.9 and 3.7, and Chapter 7) are based on the rebuttal of the Modigliani-Miller [111] capital structure irrelevance principle and the observation that cost of debt and information asymmetries do indeed matter for firms' corporate investing and financing activities.

2.2 Information Security Investments

Information security investment decision making is a major area of research and practice within the economics of information security [21, 25, 123–127]. This DPhil dissertation builds upon the nascent research tradition grounded in the seminal work of Anderson and Moore [13–16] by combining technical computer science deliberations with financial economics methodologies and principles as introduced in Section 2.1 in order to inform information security strategic investment endeavours. Specifically, this dissertation uses theories and methodologies informed by the financial economics literature to advance the literature on costs associated with security breaches and investments. In order to conduct information security investment deliberations, corporate information security executives require both models and metrics to structure their approach to estimating net economic benefits of investments and knowledge of costs and benefits associated with information security investments. In this section, ENBIS, a commonly used framework to conduct security investment cost-benefit analyses is introduced. It will be noted that the framework requires holistic knowledge of information security costs and that the metric does not account for secondary

benefits beyond reductions in annual loss expectancies. In the ensuing sections, the investment and breach costs typically considered in ENBIS will be discussed, from which the need to pay more attention to less-obvious costs, termed underlying and consequential costs, will follow. One underlying / consequential cost category, financing costs, will then be the major subject of the subsequent empirical analyses.

In order to manage and mitigate information security risks and prevent costly incidents, firms want and have to invest in security. Naturally, for-profit organisations, the main unit of analysis in this dissertation, are interested in reducing negative economic impacts on profitability and are thus inherently motivated to invest in information security measures. Besides, national and international cyber security policy makers, who "take a broader perspective and consider the close relationship between the digital economy, national security and societal interests" [128, p. 435], require firms to invest in information security [129]. For instance, the General Data Protection Regulation (GDPR) introduced mandatory data protection impact assessments (DPIA) for 'high-risk' data [130]. Conducting DPIAs can lead companies to realise the necessity to invest in security, but leaves them unaware as to which measures might be the most efficient ones to invest in. In the United States, Section 404 of the Sarbanes-Oxley Act of 2002 on the assessment of internal controls has motivated publicly-listed companies to place greater emphasis on information security [54, 55, 131].

Addressing the necessity to invest in information security, firms may consider multiple alternatives geared towards enhancing their vulnerabilities with regards to identifying, protecting their organisations from, detecting, responding to, and recovering from cyber attacks [132]. For instance, organisations may opt to insure against risks, outsource information security, or invest in systems, processes, and staff [125]. Firms may thereby invest substantial information security budgets [133–135].

Information security executives' tasks include the planning, execution, and revision of security investments. To allocate resources economically[5], they require models, frameworks, and data to guide their decision-making process. Decision variables include, for example, the type, frequency, and intensity of information security investments [25, 127]; the fundamental characteristics of information security[6] on which a firm decides to focus [136, 137]; and the timing of security investments [138, 139].

As information security investments can be considered to be of a similar nature to firms' other strategic capital expenditures [21], a key element of consideration for rational stakeholder value-maximising security executives contemplating information security investments

[5]See Section 2.1 for elaborations on what constitutes rational, economic, utility- or profit-maximising decision making.

[6]The fundamental characteristics of information security are information confidentiality, integrity, and availability.

is the cost-efficient mitigation of negative economic impacts of security breaches [17, 18, 124]. This approach towards information security risk mitigation is referred to as quantitative appraisement or expected value analysis [140]. This type of economic cost-benefit analyses, which strives to assign specific values to the costs of both security investments and breaches [141], is based on the premises that any investment in information security should not be associated with greater costs than the issue the investment attempts to mitigate and that a level of complete security is therefore not reasonably achievable [142–144].

Information security executives are incentivised to invest allocated budgets in the most efficient way to enhance their firms' cash flows by reducing risk-adjusted losses or by generating returns greater than the investments [124]. In light of the need to invest in information security in order to mitigate potential costs and comply with legislative requirements, information security decision makers are faced with a dilemma. Presented with inherently limited resources, they need to establish gains and losses associated with security breaches and investments in countermeasures to facilitate effective cost-benefit analyses and justify security investments to stakeholders inside and outside the organisation.

In order to allocate scarce resources economically and demonstrate the necessity to invest in information security, CSOs, CISOs and similar executives thus require models and frameworks to support their analyses and guide their investment decision-making process [21, 25, 30, 123, 127, 136, 137, 140, 145–147]. Both conceptual and empirical research aiming to advance scholarly understanding of organisational behaviour and to aid firms' information security investment decision making has been conducted. Noteworthy research on models to describe and support information security investing has been undertaken, based on, for instance: Expected Net Benefit of Information Security, Net Present Value, and Annual Loss Expectancy [22]; case studies on investment strategies [148]; real options frameworks [149–151]; and game theory and combinatorial optimisation [152, 153].

For instance, taking into account the vulnerability of information confidentiality, integrity and availability, as well as the potential loss from such vulnerability, Gordon and Loeb [21] proposed an economic model to determine the optimal amount a firm should invest in information security. Contrary to intuition, they demonstrated that information security investments are only economical for medium levels of information vulnerability and only up to a limited fraction of the expected loss incurred by a security breach. Relatedly, Cavusoglu and colleagues [154] provided a comprehensive model for evaluating IT security investments. The authors also showed that, with increasing quality of security systems, the cost of security decreases.

Most information security investment models correctly take into account the initial and follow-on costs of making investments, as well as the direct benefit of increasing information

security resilience and thereby mitigating potential breach losses. The corporate finance-driven notion that costs for information security measures need to be balanced against the cost of compromising data (i.e., be cost-effective) actually dates back to the 1980s (see e.g., [155]), but was particularly brought to academic attention by Gordon and Loeb [21]. Following [21–25,156], the Expected Net Benefit of Information Security (ENBIS) constitutes a fundamental high-level metric frequently applied to decide whether an information security investment opportunity is cost-efficient and should be pursued. The metric is based on the Annual Loss Expectancy (ALE), defined as

$$ALE = p * \lambda \tag{2.1}$$

where p is the probability of loss in the considered period of time and λ is the expected loss in the same period of time. Assuming monotonicity of security with increased spendings, the benefit of security investments is thereby defined as the difference between ALE_0, the expected loss without security investment, and ALE_s, the expected loss at security controls level s. $ENBIS$, the metric of interest here, is then defined as

$$ENBIS = ALE_0 - ALE_s - c \tag{2.2}$$

where c denotes the cost to achieve security level s. A security investment should accordingly be pursued if $ENBIS > 0$, i.e. $ALE_0 - ALE_s - c > 0$.

Accordingly, ENBIS is a cost-based framework, and decisions to pursue information security investments are inherently dependent on potential losses incurred by breaches and the costs to mitigate them. In line with the ENBIS metric, firms' benefits obtained by security investments are based exclusively on reductions of costs. Information security executives therefore need to be aware of and quantify the probability of being successfully attacked, the losses associated with such an attack, the extent to which ALE can be mitigated with security investments, and the costs associated with such investments. It is worth noting that the benefit proportion of the ENBIS equation only explicitly accounts for reductions in ALE, but no other potential secondary benefits obtained from investing in information security. To factor in such additional benefits, one would need to account for them individually by introducing an additional term in the ENBIS equation, or alternatively by recognising a *negative* cost element in the c vector of investment costs.

In Section 2.1, the dissertation addressed the subject of discounting future benefits to present values in order to account for inter alia the time value of money, uncertainty, risk, and opportunity costs. According to these concepts, to compute the present monetary value of ENBIS over multiple periods, costs and benefits can be aggregated as follows [23–25, 156].

$$NPV = -c_0 + \sum_{t=1}^{n} \frac{ALE_{0,t} - ALE_{s,t} - c_t}{(1+r)^t} \tag{2.3}$$

Here, c_0 denotes the initial information security investment costs at $t = 0$, c_t denotes recurring or follow-on costs incurred in later periods t, $ALE_{s,t}$ is the annualised expected loss for period t at security level s, and r is the discount rate typically calculated based on investors' expected rates of return and hence corporate financing costs [110].

It becomes obvious that financing costs bear a dichotomous relevance for cost-benefit assessments of information security investments. On the one hand, changes in financing costs can be regarded as cost factors that ought to be considered as part of the probability-weighted annual losses stemming from security breaches (ALE). On the other hand, greater financing costs lead to greater discount rates (r). Following the value-based planning, or shareholder value approach, value creation on project-level is commonly defined in terms of net present value (NPV), which decreases with greater discount factors [110, 157]. Accordingly, greater financing costs result in lower investment project NPVs, which might render some security projects economically unreasonable to pursue. On a firm-level, cash flow- and terminal value-based company valuations also decrease with greater discount factors [105].

Despite the value of existing security investment models (such as [21–25, 148, 151–154]), they do not conclusively resolve the dilemma of reliably quantifying threat impacts and costs to mitigate these risks. Extant conceptual models inherently assume that information security executives are simply aware of or can measure costs of security breaches and investments. In Sections 2.3.1 and 2.3.2 cost categories and types typically considered in previous conceptual and empirical studies are highlighted. However, some costs cannot be easily observed by, or are even not previously known to, security executives. Therefore most prior models suffer from a tendency to exclusively focus on obvious or direct costs. To conduct holistic cost-benefit analyses and justify security investments, decision makers need to be aware of *all* potential costs associated with security breaches and investment countermeasures. As less-obvious indirect costs — such as financing costs — can severely impact organisations on multiple levels per the explanations provided above, more empirical research on such costs is required to enable more accurate and holistic information security cost-benefit analyses. Moreover, while existing models consider information risk mitigation as the main benefit of security investments, they tend to neglect potential secondary benefits obtained from investing in information security (i.e., negative costs c arising in addition to security breach mitigation benefits).

Accordingly, after introducing typically considered costs, this dissertation goes on to provide a new cost classification distinguishing between *obvious* and *underlying / consequential*

information security costs to shift executives' and researchers' focus more towards the latter kind of losses. The dissertation hereby focuses predominantly on security breach costs λ, required to calculate the primary benefit of security investments, and to some extent on security investment costs c, incurred to achieve a particular level of information security. After discussing different types of costs associate with security investments (c) and security breaches (λ), the dissertation goes on to provide empirical evidence of four elements of underlying / consequential costs that all affect firms' financing costs. The empirical studies demonstrate novel cost elements as well as secondary benefits obtainable from security investments.

2.3 Costs of Information Security Investments and Breaches

In this section, costs of security investments and breaches typically considered in the security economics literature will be discussed. This will be followed by a novel cost classification distinguishing between obvious and underlying / consequential costs to provide the foundation for the ensuing empirical analysis of underlying and consequential financial costs.

2.3.1 Costs of Information Security Investments

Besides considerations as to the effectiveness of security controls as the main benefit associated with investments in information security, we established that corporate information security executives need to be aware of two types of losses in the ENBIS calculation: costs of security investments and costs of security breaches. This subsection considers costs of information security investments and argues that costs of less visible nature, i.e. underlying / consequential investment costs, need more exploration as they have been underrepresented in the literature.

Naturally, investing in countermeasures to prevent information security breaches is a resource-intensive endeavour. Economic models of firms' investments into information security generally assume investment expenses to average 0.025% of firms' annual revenues [158]. Although information security surveys tend to suffer from self-reporting, selection, and response biases — amongst multiple other methodological issues and potentially misaligned incentives (see e.g., [159–161]) — researchers and practitioners alike agree that firms can invest substantial budgets in information security measures. For instance, based on Gartner surveys, worldwide information security spending has been growing and is estimated to have reached almost $121 billion in 2019 [162]. In the United Kingdom, according to the UK

Cyber Security Breaches Survey, large British businesses invested an average of £149,000 in 2018 [134]. In comparison, the mean amount invested in information security at large Italian non-financial firms in 2016 was €187,750 [135].

Costs of security investments are thereby typically classified as direct vs indirect, fixed vs variable, one-off vs recurring, and sunk vs recoverable costs [23]. Expenses are often considered on machine, installation, and fixed infrastructure level [22]; and cover technology acquisition, deployment, and maintenance costs [25].

Indirect costs, the cost class the dissertation particularly focuses on, may thereby include "time lost due to forgotten credentials, the inconvenience of transferring data between security zones, or incompatibilities of security mechanisms slowing down essential processes" [25, p. 12]. Despite this concept of indirect costs suggesting that a wide range of costs are encapsulated, most negative economic impacts described in the literature are actually either still directly attached to the respective investment, in that there is an obviously perceivable connection, or they are difficult to quantify and hence not recognised in security executives' cost-benefit analyses. Accordingly, the academic and professional understanding of indirect security investment costs should be extended further to include other indirect costs that are not necessarily visibly connected with the investment in security controls but are of a rather hidden nature.

Moreover, the literature on quantifying security investment costs is focused on losses incurred to achieve a particular level of security as the main benefit of the investment. In terms of the ENBIS metric, the only benefit considered is a reduction in ALE. To account for additional secondary benefits from investing, the investment costs c would need to feature *negative* costs as well.

2.3.2 Costs of Information Security Breaches

In Section 2.2, we established that information security executives in for-profit organisations require knowledge of two types of costs in the ENBIS calculation to conduct well-informed cost-benefit analyses, namely security investment costs and security breach costs. Section 2.3.1 discussed costs of security investments and the need for further research on indirect hidden investment costs. Similar deliberations pertain to costs of security breaches, arguably the major aspect of economic net benefit considerations in the context of information security strategies and investments. Hence, this subsection considers the literature on costs of security breaches and argues for the need to analyse further empirical evidence on less visible indirect costs of security breaches, termed underlying / consequential costs, which will be explained in the cost classification in Section 2.4.

Despite the observation that surveys on data breach costs have a tendency to be subject to particular preconceived policies and agendas, potentially resulting in exaggerated depictions of cybercrime realities, researchers and practitioners agree that security breaches do incur substantial costs for firms and society at large [27–29, 163, 164]. While recognising that some might question the underlying assumptions and the methodology employed, the Ponemon Institute and IBM estimated the average cost of data breaches to be $3.92 million, with an average $150 per record breached [163]. Similarly, incorporating insurance claim data, average breach costs for large companies were found to be $1.2 million in NetDiligence's 2019 Cyber Claims Study [165]. Cybercrime costs faced annually by organisations as a consequence of attacks have risen by 72% over the last five years and are now expected to amount to $13.0 million annually [166]. It is reasonable to expect that the annual mean and cumulative costs of data breaches will rise even further in the future [164].

Some other studies estimate the costs of security breaches to be slightly less substantial. For instance, Romanosky [158] found that costs of typical breaches are lower than $200,000 per incident. In its most recent survey, the UK Department for Digital, Culture, Media and Sport established that the mean annual cost for businesses that lost data or assets following a security breach was £4,180, whereby average costs incurred by large firms amounted to £22,700 [167].

The — potentially inflated — estimation surveys categorise negative economic impacts of security breaches for instance into costs related to detection and escalation, notification, ex-post response, and lost business cost [163]. Alternatively, security breach costs can be divided into "internal cost activity centres" and "external consequences and costs" eliciting direct, indirect, and opportunity costs, as per the Ponemon Institute and Accenture's Cost Framework For Cybercrime [166, p. 33]. Here, indirect security breach costs are rather restrictively defined as "the amount of time, effort and other organizational resources spent, but not as a direct cash outlay" [166, p. 33], omitting costs that are not necessarily visibly connected with the security breach but are of rather hidden, albeit monetary or financial, nature.

Besides the aforementioned practitioners' reports and surveys, there are also multiple studies in the academic literature focusing on estimations of economic losses associated with information security breaches. Some researchers (e.g., [147, 151, 168, 169]) use economic or stochastic modelling approaches to determine total costs of information security events and according investments. This dissertation is, however, primarily concerned with empirical evidence and the corresponding cost frameworks and models guiding security investments' net benefit considerations.

Academic studies of security breach-induced costs typically distinguish between *direct*

and indirect costs [27–29, 147]. Direct costs contain inter alia the expenses for cleaning systems from malware [29]. Indirect costs constitute intangible costs including the costs of announcing a security breach to the public and the ensuing loss in reputation, trust, and consumer confidence [29, 30].

Similarly, Anderson and colleagues [27, 28] define direct losses of cybercrime as "the monetary equivalent of losses, damage, or other suffering felt by the victim as a consequence of a cybercrime" and indirect losses as "the monetary equivalent of the losses and opportunity costs". Indirect costs thereby include reputational or brand damage, missed business opportunities, and weakened competitiveness due to losses of intellectual property [27, 28].

Cavusoglu et al. [30] introduced a slightly different nomenclature, distinguishing between *tangible* (e.g., breach-induced personnel and material costs, costs of lost sales, and insurance costs) and *intangible* costs (e.g., trust-related difficult-to-calculate costs). Furthermore, [30] differentiates between transitory (i.e., short-term) and permanent (i.e., long-term) costs. The former pertain to losses from detecting, containing, mitigating, and repairing breaches as well as lost business and decreased productivity. Permanent costs relate to customers' and business partners' loss of trust, loss of customers switching to competitors, inability to generate new customers, legal liabilities, and a perceived increase in business risk potentially leading to increased insurance costs and greater cost of capital [30]. It is hereby worth noting that Cavusoglu et al.'s costs of security breaches framework distinguishing between tangible and intangible costs, as well as short- and long-term costs, is not incompatible with the notion of direct vs indirect costs. Instead, indirect costs might feature both tangible and intangible (as well as short- and long-term) costs.

Romanosky [158] differentiates between *first- and third-party* losses when analysing security breach costs. He defines first-party losses as those incurred by the firm directly as a result of the incident, including expenses for forensic investigations, notifying customers, PR campaigns, and customer support such as credit and identity theft monitoring. Third-party losses are defined as expenses stemming from private litigations, fines and fees from government institutions, and losses of financial theft.

Indirect costs of security breaches are of central interest to this dissertation. One major area of research within the literature on quantifying such indirect costs — and one of the very few well-established metrics for indirect costs of security breaches — is the impact on breached firms' equity value [26, 30, 170–183]. Such negative capital market valuation effects can be considered a proxy for the level of all costs associated with a security breach (see [30]) and an individual cost element within the category of indirect costs for the purpose of conducting holistic cost assessments (see [2]).

There is a general consensus in the literature that disclosures of security and privacy

breaches lead to significant average stock value decreases. Based on Spanos and Angelis's [179] systematic literature review on information security events and stock prices, all statistically significant effects of security breaches on firms' market value were indeed negative ones. Cavusoglu and colleagues [30] were amongst the first to conduct a large-scale study establishing the effect of corporate information security breaches on share prices. They found that breached firms suffered an average 2.1% destruction of market value, equating to an average of $1.65 billion per security breach, within two days of the breach announcement. Similarly, Campbell et al. [171] demonstrated negative abnormal stock returns of up to -5%. A more recent study established mean cumulative abnormal returns of -0.27% in firms following privacy breach disclosures [180].

In efficient capital markets, share prices are a function of rational investors discounting future cash flows [110]. Therefore measuring the impact of security breaches on stock prices is by definition a metric taking into account long-term implications of the breach. However, the actual stock price impacts and hence the costs to firms, executive management, and shareholders only tend to be of short-term nature [184–187]. Additionally, in analysing market capitalisation impacts in terms of short-term abnormal returns, such studies provide only one potential metric accounting for difficult-to-measure costs, and are by definition limited to short-term economic impacts. Accordingly, there is a noteworthy gap in the literature pertaining to other measures of indirect costs of security breaches and metrics for medium- to long-term indirect costs. The empirical analyses in this dissertation contribute evidence to both. By assessing underlying / consequential financing costs, additional elements to quantify indirect costs are demonstrated. As these costs can have wide-ranging long-term implications, the dissertation also provides cost metrics that go beyond short-term costs. The following sections provide the novel cost classification distinguishing between *obvious and underlying / consequential costs* (Section 2.4) and lay the basis for the empirical analyses of underlying and consequential costs (Chapters 4, 5, 6, and 7).

2.4 Cost Classification: Underlying and Consequential Costs of Security Investments and Breaches

Section 2.1 delineated how rational information security executives are driven by corporate financial economics, resulting in ENBIS considerations (see Section 2.2). Sections 2.3.1 and 2.3.2 further discussed that some costs are of more immediate and visible nature, as well as the relevance of also holistically considering all potential cost elements in the ENBIS metric, including those that are rather subtle or consecutive. Now, we shift our attention

to the latter type of indirect costs. To facilitate the empirical analysis of underlying / consequential financing costs and to eventually contribute a framework promoting more holistic ENBIS analyses, this section provides the novel cost classification distinguishing between *obvious and underlying / consequential* information security investment and breach costs.

This dissertation contends that losses elicited by security events can be divided into obvious costs and underlying or consequential costs. Indirect costs stemming from information security events are a major area of concern for corporate decision makers (see [179]), who need to be aware of all potential costs associated with security breaches and investment countermeasures in order to conduct thorough cost-benefit analyses. Alas, holistically and accurately measuring information security costs is difficult. Therefore studies, surveys, and academic frameworks considering negative economic impacts of security breaches, and hence economic models, tend to focus exclusively on visible or "obvious" costs associated with security breaches and investments (e.g., [163,188]), while not accounting sufficiently (in any meaningful way) for "underlying and consequential" ones. For instance, in the context of analysing cybercrime, empirical studies tend to only recognise the "*identifiable* indirect costs" [28, p. 2][7].

Establishing frameworks, models, and tools to aid policy and decision making has been a major part of the nascent field of information security investments. However, there remain fundamental uncertainties regarding threats, vulnerabilities, attackers' motivations, attack consequences, mitigation techniques' effectiveness, and — most relevantly for this research — breach costs [123]. Due to a plethora of reasons, security breach impact, breach likelihood, and organisational resilience are difficult to quantify [123, 188–190]. Generally, there tends to be a significant lack of quality data available for researchers to analyse [158]. For both insiders and outsiders of the firm, assigning costs to security risks and countermeasures is a complex undertaking requiring substantial preliminary work [191]. Indirect costs are substantially more difficult to quantify than direct costs, but there is a broad consensus in the literature that these costs may actually exceed direct costs significantly [26–30]. The particular difficulty of quantifying indirect and derivative costs is one major reason for the absence of evidence on underlying / consequential costs (see [29]).

Due to this inherently limited data availability and substantial dependence on qualitative judgements, the immediate return on information security investment is difficult to measure (see [123, 189, 192]), and only a small minority of firms evaluate their information security spending by means of calculating *any* post-investment metrics [126, 133]. Accordingly, previous research called for a stronger emphasis on empirical analysis, as opposed to analytical

[7] Emphasis mine.

or economic models, to inform future discussion and development of investment models and theories [16, 22].

This dissertation works towards remedying this absence of empirically supported research on indirect costs in order to establish more holistic cost-benefit analyses quantifying costs of information security breaches and investments. Defining obvious and underlying / consequential costs of security investments and breaches, this dissertation follows and extends the notion of distinguishing between direct and indirect costs, which is widely accepted in the economics of information security literature [27–29, 147].

For the purpose of this dissertation generally, the model specified in Chapter 8 specifically, and aiding security executives in their investment decision-making process, the following peer-reviewed ([2]) definitions shall apply.

Definition 1 ***Obvious costs****, which can be direct as well as indirect costs, are defined as expenses that are easily observable and can be directly related to line items on a firm's profit and loss statement. Such costs are immediate expenses explicitly connected to cyber attacks and their mitigation and remediation. Obvious is to be understood in the broader sense of the word, in that obvious costs are observable and easily noticeable.*

Obvious security investment costs include initial investment costs incurred by firms allocating resources towards systems, people, or processes [23, 25], as well as yearly follow-on costs paid to auditors and other contractors. Examples for obvious security breach costs include forensics and audit fees, customer notification costs, legal and regulatory expenditures, and increased customer acquisition and retention costs [163, 193, 194]. Invoices for goods or services received by investing or breached firms constitute a clearly attributable cash outflow and are straightforward elements of obvious costs.

As information security investments are subject to the correct assessment of potential losses from breaches, firms that only focus on easily-observable costs instead of all types of costs are likely to underinvest in information security [30]. Therefore, besides these obvious costs, executives also need to consider underlying / consequential costs.

Definition 2 ***Underlying and consequential costs****, in contrast to obvious costs, are non-obvious. They constitute negative economic impacts to breached firms, those at the risk of suffering from a security attack, their peers in the industry, and society at large that cannot be directly attributed to billable items and are of a more collateral, subsidiary, secondary, implicit, or indirect nature. Underlying / consequential costs are less apparent, hidden, more derivative, and more wide-ranging. They are not inherently connected with billable expenses. Based on this definition, and the aforementioned academic studies of information security*

costs typically distinguishing between direct and indirect costs, underlying and consequential costs are naturally always constituents of the indirect category of negative economic impacts. Hidden underlying / consequential costs imposed on firms and society have had significantly less light shone upon them.

Negative economic impacts in the underlying and consequential costs category include statistically significant negative market reactions following the announcement of security investments [1, 195, 196] and security breaches [26, 30, 170–183, 197]. Such studies on share price reactions are indeed considered one of the scarce examples of well-researched non-obvious costs associated with successful information security attacks [26]. Breached firms are also associated with increases in audit fees [198], elevated CEO compensation [199], greater corporate social responsibility spending [199], as well as decreases in sales growth, increases in leverage, and worsened financial health [200, 201]. Other examples include the finding that security breaches cause deteriorating product and service quality [202][8], declines in firm productivity [203], and more frequent senior executive turnover [204]. From a wider social perspective, security breaches also pose underlying / consequential costs to society as they elicit market inefficiencies in the form of negative abnormal returns and increases in audit fees for non-breached peer firms, as well as negative equity value implications for information security insurers [205]. Additionally, breached firms reduce cash outflows in terms of dividend payments and R&D expenses, which affects investors in and suppliers of such firms [199, 206]. Moreover, there are negative firm value spillover effects to other non-breached firms following security breaches in a focal firm [30, 179].

Taken together, underlying and consequential costs both manifest themselves in addition to or alongside with direct costs. Consequential costs can be thought of as costs that conceptually or temporally follow security breaches or investments in a more indirect way. For instance, akin to negative share price reactions following security breaches, financial market reactions subsequent to security investments (see Chapter 4) and changes in information asymmetries (see Chapter 7) substantiate in the days or weeks following the respective information security event[9].

Underlying costs are negative economic implications that can influence or lead to more obvious costs. As demonstrated when discussing increases in cost of equity (see Chapter 5) and cost of debt (see Chapter 6) following security breaches, these metrics are not only

[8]For instance, Choi and Johnson find that hospital data breaches increase 30-day acute myocardial infarction mortality rates [202].

[9]It is worth noting that negative abnormal returns (i.e., stock price drops) assessed via standard event study methodology are by definition limited to short-term economic impacts [26, 30, 170–183]. Underlying / consequential financial costs in terms of information asymmetries are of more fundamental nature and might hence take longer to substantiate after a security breach.

cost elements but also underlying factors applied to, for instance, NPV calculations, corporate valuations, and stock price estimations. Indirect costs — such as changes in financing cost, the cost category analysed in the following empirical studies — that are underlying calculations of more obvious costs might very well only substantiate in the medium- to long-term following a security breach or investment event. Accordingly, it is not always possible to differentiate effectively between underlying and consequential costs. Throughout this dissertation, these non-obvious or hidden cost elements discussed are hence referred to as "underlying / consequential costs".

It is worth noting that the classification of obvious versus underlying / consequential security costs differs from extant notions delineated in Section 2.3.2, but does not intend to contradict previous frameworks. Instead, the novel cost classification is aimed to expand previous literature on and knowledge of indirect costs. Specifically, the well-accepted distinction of direct and indirect costs (see [27–29, 147]) is considered given and the dissertation focuses on particularly difficult-to-identify indirect costs. The dissertation argues that indirect costs *can* be associated with (increased) cash outflows, in contrast to the Ponemon Institute and Accenture's Cost Framework (see [166]). Anderson and colleagues, employing what may be considered a resource-based view onto firms' security breaches, consider indirect losses to be almost exclusively associated with weakened competitive positions and reputational damage [27, 28]. This dissertation on the contrary contends that financial metrics quantifying other negative economic impacts equally need to be considered indirect costs as well. Cavusoglu et al.'s [30] classification distinguishes between intangible and tangible costs, but not between direct and indirect costs. Here, the dissertation conjectures that underlying and consequential costs are in fact indirect intangible costs that are worth exploring empirically. Furthermore, whilst empirical studies analysing the negative impact of security breaches on stock prices [26, 30, 170–183] can be considered one of the very few established metrics of underlying and consequential indirect costs, this dissertation argues that holistic cost-benefit assessments also ought to take into account costs that are of greater longevity and have greater long-term impacts on a wide-ranging multitude of firm activities than immediate short-term share price drops.

Accordingly, the cost classification unites two prevalent schools of thought on distinguishing costs of information security (direct vs indirect costs [27–29, 147] and tangible vs intangible costs [30]) by introducing a more nuanced perspective on indirect costs, which are divided into obvious and underlying / consequential costs. To contribute to a more advanced ENBIS metric and a more holistic model of information security costs, this dissertation first provides evidence of one type of underlying / consequential costs, namely financing costs. Section 2.5 introduces three perspectives on financing costs and delineates how the disserta-

tion's four empirical studies reveal four cost items that all affect firms' financing costs.

2.5 Financing Costs

Section 2.1 introduced the dissertation's problem domain and unit of analysis. Furthermore, the section delineated how senior executives are driven by financial economics considerations, which led to the deduction that publicly listed companies' utility-maximising information security executives are similarly influenced by cost-benefit and profitability analyses. In Sections 2.2 and 2.3, we discussed that rational information security decision makers can use the NPV of ENBIS as a metric to facilitate assessments of potential security investments' economic efficiency and what types of costs need to be known to calculate ENBIS. Furthermore, we established that financing costs bear a twofold relevance for cost-benefit assessments of information security investments. Section 2.4 emphasised the difficulties in establishing reliable figures for security investments costs and particularly indirect security breach costs. In order to work towards an improved understanding of information security costs, and hence an advanced ENBIS metric, the section also introduced a novel cost classification distinguishing between obvious and underlying / consequential costs.

Now, in this section, the dissertation provides further background on one particular underlying / consequential cost type, namely financing costs, and the trichotomous manifestation of such costs: costs of internal financing sources, costs of external financing sources, and information asymmetries. All three aspects are dissected into four cost elements which are analysed in the ensuing sections.

Financing costs are all costs incurred by firms in the process of obtaining capital to generate or procure assets, to undertake their intended operations, and to deploy executives' intended strategies [110]. Financing costs are highly related to cash outflows, but include implicit costs, imputed costs, and other opportunity costs, and do hence not necessarily constitute cash outflows[10].

There are multiple possible perspectives on financing costs. Figure 2.1 shows major considerations of relevance for publicly listed firms. In order to maximise profitability, such companies aim to minimise financing costs. To achieve the lowest possible financing costs, firms have to decide on the optimal capital structure whilst paying attention to fundamental considerations. Firms' funding sources can be subdivided into internal financing (i.e.,

[10]For instance, cost of equity is the return expected by and hence theoretically paid to equity investors. Holistic considerations of cost of equity can include expenses associated with dividend payments. However, as firms are not mandated to pay shareholders dividends, cost of equity do not constitute an immediate cash outflow. Similarly, a firm's cost of debt figure is not the exact return on investment gained by every debt investor, but rather a reflection of what the average investor (e.g., bond holder or bank) might expect.

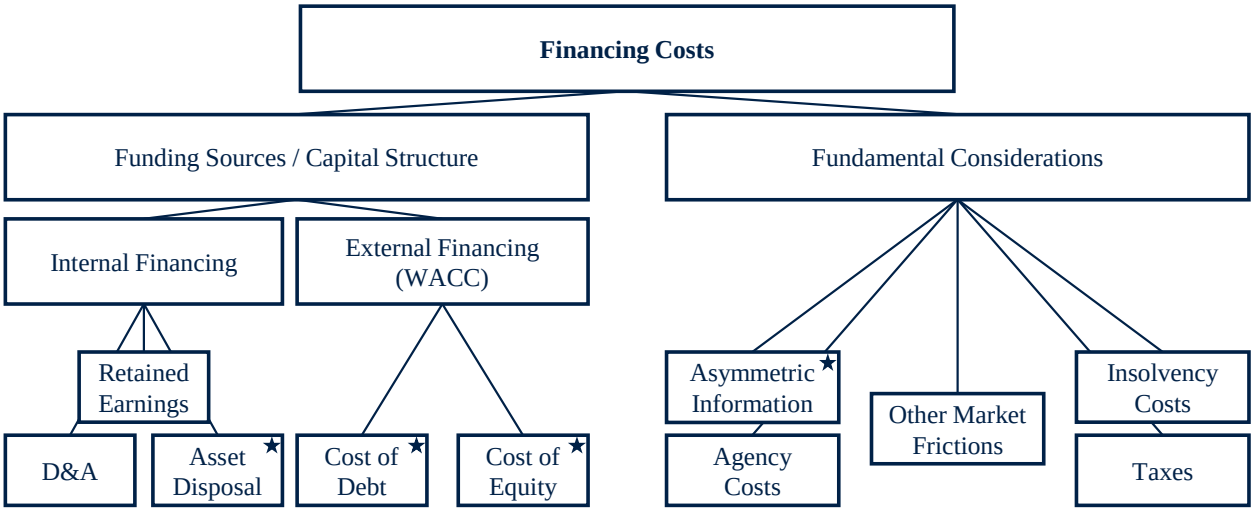


Figure 2.1: Overview Financing Costs

obtained from within the firm: mainly retained earnings, depreciation & amortisation, sale of assets) and external financing (i.e., obtained from outside the firm: debt, equity, mezzanine). Fundamental considerations of information asymmetries, agency costs, insolvency costs, taxes, and other market frictions are in line with the refutation of the Modigliani-Miller irrelevance theorem introduced in Section 2.1 [110, 112–116].

The three major perspectives onto financing costs considered in this dissertation are the value of internal financing instruments, firms' weighted average cost of capital (WACC), and information asymmetries (all highlighted by asterisks in Figure 2.1). The different perspectives on financing costs are naturally interrelated. For instance, greater information asymmetries may cause firms to sell their assets at lower prices (leading to lower availability of internal funds) as well as greater cost of debt (as debt investors' ability to assess their investment risk is impeded). This in turn might necessitate firms to consider accessing more expensive sources of financing, i.e., issuing new equity. However, as each of the three perspectives can be correlated with an individual cost element, for instance in terms of the ENBIS metric (see Section 2.2), they are all worth analysing individually. The following paragraphs introduce the three perspectives leading to four cost elements which will be subject to empirical analysis in the ensuing chapters of this dissertation.

Internal Financing — Asset Disposal First, internal financing capital, which is usually the cheapest source of funding for a firm [110,112,113], is obtained via retained earnings [110, 207], depreciation and amortisation (D&A) [110, 208], and asset disposal [209, 210].

Firms' ability to profitably dispose of assets, and use the proceeds as a funding source, thereby naturally relies partially on the resale value of assets. All assets that can be used in such a way can be considered internal financing instruments. When the market value of an internal financing instrument increases, a firm is able to realise greater gains from its sale, resulting in less need to obtain financing from additional sources, and vice versa. One asset a firm may hold is treasury shares, i.e., shares a firm has repurchased but not retired, that is, cancelled [32][11].

Firms may sell treasury shares to inside and outside investors, award them to executives as part of their remuneration packages, or use them as a means of payment, particularly in merger and acquisition situations. A decrease in the value of treasury shares held by a firm suggests an increase in financing costs due to the necessity to obtain alternative sources of capital to maintain a particular level of capital needed to conduct a transaction (e.g., paying staff or for an acquisition target), and vice versa. Put differently, from an internal financing and asset sale perspective, executives interested in minimising financing costs are incentivised to maximise share prices as to achieve greater economic benefits from deploying treasury shares. In summary, "(...)a higher stock price is tantamount to a decrease in a firm's cost of capital" and vice versa [214, p. 2].

The first empirical study in this dissertation analyses changes in share prices following Cyber Essentials (Plus) and ISO/IEC 27001 certifications. Measuring abnormal returns following certification events provides a metric to quantify security investment-induced value creation and destruction, and accordingly decreases and increases in the value of treasury shares. In terms of the financing costs perspective, information security investments might affect the value of internal financing instruments and hence financing costs. Such additional underlying / consequential costs ought to be considered in the ENBIS metric. Sections 2.6 and 3.4 provide further background on and a metric to quantify changes in equity and firm value following information security investments.

External Financing — Cost of Equity and Debt Second, the WACC figure, which can be dissected into cost of equity and cost of debt, is a summary of the rate of return

[11] Treasury shares are referred to as treasury stocks in the United States, whereas treasury stocks in the UK are gilts issued by the UK Government. Technically, on a firm's balance sheet, treasury shares are not recognised as an asset, but on the contra-equity account, a negative account which is deducted from total shareholders' equity, and gains are recognised in paid-up capital instead of retained earnings. However, "future economic benefit" can be obtained from treasury shares, and they can be sold and used like financial assets hold in other firms, which are recognised as intangible assets. Treasury shares hence possess properties similar to Intangible Assets and Financial Instruments (see International Accounting Standards 38-39 and International Financial Reporting Standard 9 [211–213]), and are considered an "asset" for the purpose of this analysis.

investors expect to be paid and firms obtaining external financing are hence expected to pay their financiers [110].

A firm's after-tax WACC is calculated as follows [110][12]:

$$WACC = \frac{E}{D+E} * K_e + \left(\frac{D}{D+E} * K_d * (1-t) \right) \tag{2.4}$$

Here, E and D are the market values of a firm's equity and debt, K_e is the cost of equity, K_d is the cost of debt, and t is the marginal corporate tax rate. To minimise their WACC, firms might engage in active corporate tax planning or change their level of leverage (i.e., the amount of debt financing relative to equity financing used). Most importantly, firms aim to manage their costs of equity and debt.

Cost of equity, the subject of the dissertation's second empirical study, is typically defined as investors' expected rate of return. Sections 2.7 and 3.5 explain further details on cost of equity and provide a formula for measuring changes in cost of equity. Cost of debt, thematised in the third empirical study, is the effective interest rate a company pays on debt instruments such as bonds and loans. There are multiple possible ways of estimating a firm's cost of debt which are further discussed in Sections 2.8 and 3.6.

WACC is applied in corporate valuations, project and investment planning, performance measurement, and regulatory processes [110, 215, 216]. Both cost of equity and cost of debt are driven by investors' risk considerations. Information security breaches are likely to increase (perceived) investment risks, which would lead to greater costs of obtaining equity and debt financing, and hence greater financing costs. Security breach-induced changes in costs of equity and debt ought to be considered in ALE calculations when estimating security investments' ENBIS.

Fundamental Considerations — Information Asymmetries Third, information asymmetries between firm insiders and outsiders emerge as management teams possess greater access, abilities, and incentives to understand and evaluate complex strategies and stocks' fair value than investors do [112, 113, 217, 218]. In line with Akerlof's "market for lemons" logic [219][13], executives' informational advantage can enable them to mask low-quality strategies and projects, creating adverse selection problems, which impede valuation and risk assessment processes and thus increase investors' required returns, diminish share prices, and

[12]The calculation presented in 2.4 assumes absence of mezzanine financing and other hybrid financial instruments.

[13]Equity markets constitute "markets for strategies" [217] on which managers may sell low-quality products (i.e., strategies). When investors cannot easily distinguish between good and bad strategies, high-quality ones are also subject to discounts (see [219]).

raise financing costs [112, 113, 214, 217, 218, 220, 221].

Information asymmetries are relevant for firms' cost of capital not only because they are synonymous with greater valuation uncertainty and hence greater discount factors if investors are risk averse [214], but also because greater information asymmetries are associated with lower investor demand for shares in the underlying firm, which results in lower stock prices [222].

The significance of information asymmetries for financing costs is also illustrated in Myers and Majluf's Pecking Order Theory [112,113,223], which postulates a positive correlation between investor-manager (i.e., principal-agent) information asymmetries and financing costs. Pecking Order Theory argues that due to adverse selection and signalling problems of issuing potentially overvalued equity, firms prefer internal financing over raising debt over issuing new equity to benefit from lower information costs associated with debt issues [112]. In the extreme case, some potentially profitable investments might not be pursued by companies that cannot obtain the requisite funding from public markets due to asymmetric information levels.

Security breaches can lead to changes in information asymmetries. The announcement of a breach might induce outside investors to realise that firms' insiders possess better information on security breaches than they do. As greater information asymmetries lead to increases in financing costs, breach-induced increases in information asymmetries ought to be considered when conducting ENBIS cost-benefit assessments. Sections 2.9 and 3.7 explain the notion of and a well-accepted proxy for information asymmetries used in the fourth empirical study of this dissertation.

2.6 Security Investment Costs: Firm Value

This section discusses the background and motivation for contribution **C1** in Chapter 4. It starts by summarising related literature and formulating the main hypothesis. Noting the study's background and hypothesis is relevant to frame the samples and analysis methodologies as described in Sections 3.1 and 3.4, respectively. Chapter 4 then presents the empirical results obtained and provides a discussion of these results.

When considering security investments that potentially lead to a positive ENBIS (see Equation 2.2), corporate decision makers are presented with a plethora of options. One common type of information security investment executives may contemplate pursuing is security standards certification. Such certifications are an interesting type of investment to study for multiple reasons. First, they serve as a platform for (potentially substantial) secondary security investments. In order to become and remain compliant with security stan-

dards, prior investments in systems, people, and processes are required. Second, due to the fact that such standards cover multiple control areas, they have a greater potential to reduce security breach probabilities and costs than individual, disjoint discrete investments. Third, being awarded with a security standard certification implicitly carries a greater public-facing meaning. That is to say, a security certificate is an investment 'badge' that can be publicly displayed. Other, potentially more tangible (or more effective) security investments do not feature such an explicit signalling value, and hence do not offer the opportunity to enhance a firm's reputation. Moreover, given the inherent public-facing nature of security standards investments, they are particularly suitable to being studied using empirical methodologies.

In this dissertation, two security standards are considered: Cyber Essentials (Plus) and ISO/IEC 27001. These standards were chosen as they both provide firms with the potential advantages listed above. Specifically, both standards may: serve as guidelines for further investments; reduce security breach probabilities and costs; and convey a positive signalling value. However, despite their similarities, they differ significantly in terms of governmental requirement, geographical reach, and comprehensiveness. Compliance with the Cyber Essentials programme is mandatory to become a supplier to many UK Government departments, the programme is only intended for British companies, and it only demands that organisations meet a basic level of information security. An ISO/IEC 27001 certification is not required to bid for governmental contracts, the standard is globally applied, and it is more extensive in terms of its controls. Thus, the two standards create a favourable scenario for a study aspiring to establish generalisable results.

The aim of the first empirical study of this dissertation is to investigate whether becoming certified according to Cyber Essentials (Plus) or ISO/IEC 27001 leads to material market reactions which suggest firms' value destruction or creation. The study thereby focuses on successful awards of certification, as opposed to mere announcements of plans to become compliant. Furthermore, certifications of entire organisations and subsidiaries are considered to be events.

Accordingly, the following research question is explored over the course of contribution **C1**: *Are corporate investments in security certificates associated with value destruction (i.e., hidden underlying / consequential costs) or creation (i.e., secondary benefits or negative underlying / consequential costs) as evidenced by stocks' abnormal returns?*

Empirical studies attending to the issue of quantifying security investment costs and potential secondary benefits can evaluate value creation in terms of stock price reactions associated with organisational investments in information security.

Academic investigations of event-induced stock market reactions necessitate the validity of the Efficient Market Hypothesis (EMH) in its semi-strong form [108, 109]. The semi-

strong EMH postulates that stock prices reflect all publicly available information on the underlying firm and that they quickly adjust to the publication of additional news items. In the context of this study, stock markets are considered to be semi-strongly efficient with respect to awards of security certificates (and entries in databases such as the ones used for this study) constituting or acting as news items.

Event studies analyse the extent to which actual stock market returns in firms differ from expected returns following a corporate event [224–228]. In this study, the investment in an information security certificate is considered an event, and event study methodology is used to determine and assess abnormal returns. Event study methodology can be considered "*the* method of choice for analysing market reactions to news" [229, p. 19][14], and has frequently been used in the context of information security economics (e.g. [182, 229–231]).

The area of research investigating abnormal returns associated with information security investments builds on the strong body of literature on positive market reactions in terms of abnormal returns induced by general IT investments [232–237]. Based on this strand of literature, some researchers have analysed the short-term impact of IT security investments on the market value of firm specifically.

Previous research on the corporate value implications of information security investments is scarce [179, 238]. These studies predominantly indicate a positive association between information security investments and stock prices [124, 231, 238–240]. Applying event study methodology to a sample of 101 information security investment announcements of US firms between 1997 and 2006, Chai et al. [124] found significant positive abnormal returns of up to 1.89% [-2, 2]. Using generic search terms, such as 'information security' and 'information assurance', the authors covered a broad range of (unspecific) security investment types. Chai et al. [124] also demonstrated that information security investments with commercial exploitation and investments which took place after the introduction of the Sarbanes-Oxley Act are associated with higher abnormal returns. Their findings were corroborated in a later study which also demonstrated significant positive abnormal returns following security investments which can be commercially exploited, but significant negative abnormal returns upon investments which are exclusively intended for security improvements [239].

Bose and Leung [231, 240] concentrated on a specific form of information security investment — identity theft countermeasures. Analysing events associated with "keywords such as anti-identity theft, 2FA, digital certificate, dynamic password generator, digital signature, and one-time password" [231, p. 757], they revealed statistically significant short-term mean cumulative abnormal stock returns of 0.63% following the announcement of such investments. The authors also showed that early adopters, and firms which invest in more sophisticated

[14]Emphasis mine.

identity theft countermeasures, are associated with stronger positive short-term market returns.

Recently, Deane et al. [238] analysed the effect of 111 public announcements of successful ISO/IEC 27001 completions in the United States between 2005 and 2015. Analysing primarily new certifications (as opposed to re-certifications), the authors found that the announcement of successful ISO/IEC 27001 certifications in news media outlets such as Bloomberg and Reuters is associated with statistically significant positive abnormal returns. For instance, in the event window including one day prior to the certification announcement and the event day/announcement day itself, the mean cumulative abnormal stock return was 0.72%.

However, there is also some contradictory evidence in the literature indicating that security investments elicit significant negative short-term market value impacts or no significant impacts at all [195, 196, 241, 242]. Analysing 35 investments into cloud computing security following cloud security breaches from 2006 to 2010, one study found a significant negative short-term impact on market value [195]. The authors also established a negative spillover effect following countermeasure investments, i.e. competitors' stock market value also decreases as a result of a focal firm's post-breach investment [195].

Jeong et al. [241] investigated 98 information security investment announcements between 2010 and 2017. They found no evidence of significant positive changes in market value following IT security investments. Additionally, the authors found their hypothesis that security investments create positive abnormal returns in competitors to be only partially supported [241]. Another study focusing on security investments of e-banking firms also provided weak evidence in support of the notion that security investments are not associated with statistically significant market value implications [242]. Finally, assessing 63 investment announcements under multiple timing scenarios, Szubartowicz and Schryen [196] revealed negative abnormal returns following the news of intended and accomplished investments into information security if these investments are not preceded by previous security incidents.

The short-term value-creative benefits of IT investments has been thoroughly investigated. Research on information security investments generally, and holistic security standards specifically, however, remains scarce and inconclusive, which motivates further empirical investigation of positive and negative costs imposed on companies in the form of value destruction and creation following security certifications. The study presented in Chapter 4 extends earlier findings ([124, 231, 238, 240]) and thereby advances the scarce empirical evidence of information security investments. The majority of past empirical studies centred on information security investments generally, as opposed to on specific types of investment, and is therefore of limited utility to compare and discuss particular investments. There

is currently a gap in the literature concerning information assurance standards' ability to generate or destruct value besides their primary intent to enhance information security, resilience, and regulatory compliance. Chapter 4 addresses this gap by contributing insights on the economic value of information security investments to the security economics literature. This is the first study to quantitatively analyse the impact of information security standards implementation on firms' market values on an international sample across different types of standards and geographies. It is also the first study to provide novel evidence on firm characteristics elevating or exacerbating the effect of security investments on stock prices.

Both sets of security standards, Cyber Essentials and ISO/IEC 27001, can be considered broadly effective. The controls featured in the Cyber Essentials programme (see [22]) and the ISO/IEC 27001 Information Security Management System (see [243]) were developed by experts with input from academics and practitioners and undoubtedly have the potential to mitigate organisational information security risk. Empirical research has demonstrated that voluntary and proactive security investments lead to fewer security failures [244,245]. Investments in information security standards can be considered a proactive type of investment given that they can constitute a platform for further systems, processes, and staff training in which firms may invest. A proactive approach towards acknowledging security threats and taking steps to mitigate them also enables firms to generate higher revenues and focus more on core business activities [246]. Additionally, Liu et al. [245] showed that continuous investment in effective security countermeasures significantly reduces the probability of severe security incidents. As firms need to become re-certified annually (Cyber Essentials) or every three years (ISO/IEC 27001), certifications facilitate continuous information security improvements and can thus be expected to reduce breach probabilities significantly. Given the potential to reduce breach probabilities and costs, investments in security can also lower information insurance premiums [247–250].

Following the reasoning of the aforementioned aspects, it can be conjectured that market participants might be led to expect greater positive future cash flows, which would result in equity value creation as evidenced by positive short-term abnormal returns. This in turn would constitute an increase in the value of treasury shares and hence a decrease in financing costs. Accordingly, an investment in security certificates would constitute a secondary benefit, or negative investment cost c as per Equation 2.2.

However, despite the aforementioned positive aspects, there are potential caveats worth considering[15]. First, Cyber Essentials controls do not necessarily cover all potential threats and attack vectors, which is why additional security investments might need to be made [22].

[15]These caveats are not to be understood as a commentary on regulations, but rather statements as to the complexity of the valuation problem.

Moreover, Heitzenrater and Simpson [22] empirically demonstrated that firms ought to exercise caution when implementing Cyber Essentials controls, as potential economic benefits might be eradicated quickly given the amount of time (and thus money) per machine invested. Relatedly, Bose and Leung [231, 240] noted that effective security countermeasures are often associated with substantial costs, which may even prohibit firms from pursuing security investments.

In addition to high initial costs, firms are also likely to incur material follow-up costs. For instance, Moore et al. [126] noted that the ISO/IEC 27001 standard is frequently used by firms as a framework to guide future information security investments. Given the necessity to become re-certified after pre-defined periods of time, and that security standards function as a platform for further investments, market participants may rightfully expect substantial consequential costs stemming from further investments.

Prior research has demonstrated that firms which have suffered from a security breach are significantly more likely to invest in information security in the following year, and that security investments are positively associated with the probability of being attacked in the future [135]. Following an investment in certification, market participants might thus be inclined to assume that the investing firm did not publicise a previous breach. Moreover, although there is not necessarily a causal relation between security investments and attack frequency, malicious actors might become aware of the firm as a potential target, and investors might be reminded by a security investment that the focal firm is susceptible to security breaches.

From a shareholder's perspective, one might argue that a security breach is only relevant (and thus necessitating investments in countermeasures) if it leads to a significant negative share price impact. Despite the plethora of studies demonstrating that security incidents are associated with short-term negative abnormal returns (e.g. [179]), there is some evidence suggesting that such negative stock price shocks are only of short nature and do not impact firms in the long run [184–187]. Assuming that the share price impact of a security breach might be negligible, an investment in countermeasures might be perceived to be a waste of scarce economic resources.

The considerations mentioned above might lead market participants to expect greater negative future cash flows, which would eventuate in equity value destruction as signified by negative short-term abnormal returns. This in turn would lead to a decrease in the value of treasury shares and hence an increase in financing costs. Accordingly, an investment in security certificates would constitute an additional hidden, or underlying / consequential, investment cost element c as per Equation 2.2.

In summary, investments in information security standards have the potential to reduce

financial penalties and losses associated with data breaches, enhance reputation, win new business, and improve business processes. However, the initial investment is costly, necessitates follow-on expenses, and might conceivably be perceived as being associated with greater attack frequencies. In any case, investors, analysts, and other market participants can be expected to alter their future cash flow expectations following investments in holistic security standards. Taking into account that existing research is inconclusive as to whether security investments are associated with significant (positive or negative) abnormal returns, and that evidence suggests positive as well as negative future cash flows following initial investments in security standard certifications, ex ante, directionality cannot be assume. Instead, this study aims to investigate whether becoming certified according to Cyber Essentials (Plus) or ISO/IEC 27001 has significant equity value implications for the certified firm. To this end, it is hypothesised as follows:

C1-H1. The official certification of a firm with information security standards is associated with significant abnormal returns.

2.7 Security Breach Costs: Cost of Equity

An improved understanding of changes in systematic risk is of relevance to information security economics researchers and practitioners alike. For researchers, an increase in cost of equity following changes in the underlying exposure to financial systematic risk (i.e., beta) might inform frameworks and models on information security investments based on cost-benefit analyses. Increases in systematic risk and cost of equity might also help to explain a multitude of corporate phenomena following security breaches. From a practitioner's perspective, a holistic understanding of potential impacts of security breaches is essential to facilitate economic decision making. Changes in cost of equity resulting from increases in financial systematic risk are also of concern to corporate executives, as the measurement relates to all major corporate finance activities including capital raising, share issues and buybacks, as well as shareholder value management. Similarly, for investors, an increase in cost of equity, and consequentially an increase in cost of capital, implies an increase in a firm's risk [111].

This section gives consideration to the background to, and the motivation for, contribution **C2** in Chapter 5, in which changes in firms' cost of equity following severe security breaches[16] are analysed. It conjectures that changes in cost of equity due to changes in systematic risk can be considered an item of underlying or consequential cost, and should

[16]The term severe security breaches is defined in Chapter 3.

hence be considered in holistic cost-benefit security investment analyses. The discussion of relevant previous literature here provides the necessary theoretical background to and foundation for the sampling and empirical analysis procedures described in Sections 3.2 and 3.5. The present section also introduces financial systematic risk, the two-beta model, and the conceptual connection between security breaches and changes in systematic risk. Chapter 5 discusses the results stemming from the empirical analysis and the respective implications for researchers and practitioners. Chapter 8 considers how additional research could further extend the literature on impacts on systematic risk specifically and corporate security breach impacts generally.

The gap in the literature — marked by the absence of analyses on holistic cross-industry samples, current data, and consideration for different market environments — motivated two research questions, which can be stated thus:

- *Do severe security breaches increase firms' cost of equity by elevating systematic risk?*
- *Do severe security breaches affect firms' cost of equity differently in bearish and bullish markets by affecting downside and upside risk differently*[17]*?*

Accordingly, the aim of the study is to establish the impact of severe security breaches on firms' cost of equity as evidenced by increases in systematic risk (regular beta), systematic upside risk (upside beta), and systematic downside risk (downside beta).

Unsystematic and systematic risk are commonly considered to collectively constitute a financial asset's overall risk level [251]. This operationalisation of risk is described by the capital asset pricing model (CAPM), established following the work of Sharpe [117, 118], Lintner [119], Treynor [120], and Mossin [121], based on Markowitz's Modern Portfolio Theory [57]. The CAPM divides a company's risk, i.e., the volatility of its stock returns, into systematic (market, undiversifiable) risk and unsystematic (unique, idiosyncratic, diversifiable) risk. Systematic market risk — denoted beta — is the sensitivity of a firm's stock returns relative to the returns of a broad market index. Based upon the CAPM, cost of equity is the rate required by shareholders to compensate for the investment risk incurred. A major component in determining the risk premium is beta, a measure of exposure to non-diversifiable, systematic, or market risk. Beta is a measure of correlated relative volatility that indicates the extent to which a public company's stock return volatility is correlated with the relevant index volatility indicating risk and exposure to general market movements [118–121]. Accordingly, the stock market's beta is always 1. Stocks which are more volatile than the market have a beta factor greater than 1 and vice versa [110].

[17] Bearish markets are falling markets characterised by negative index returns; bullish markets are rising markets characterised by positive index returns.

A security breach can induce equity investors to alter their risk assessment of a firm's ability to generate future cash flows. For instance, investors might price additional reputational hazard, which can result in lower revenues and greater revenue volatility. Rational economic agents expect to be remunerated accordingly for additional risk and in turn may require greater equity returns, which can be reflected in terms of beta. For instance, Chegg Inc., an education technology company, which suffered from a security breach affecting more than 40 million users in 2018, experienced an increase in regular, downside, and upside beta factors, turning a low-risk stock (with betas <1) into a greater-risk one (with betas >1)[18].

Despite its frequent use by both academics and practitioners [251–258], the CAPM has its limitations. For example, it does not distinguish between bullish and bearish markets, i.e., time periods in which market returns are positive (up) or negative (down). However, risk exposure to general market movements is not necessarily symmetrical in Up and Down Markets. By extending the work of Fabozzi and Francis [259], Kim and Zumwalt [260] were among the first to suggest a model which resolves this issue. They proposed and successfully tested a model that incorporates two different betas: one for periods of time featuring positive market returns and one for negative return periods. This dual-beta model allows for beta coefficients to reveal different figures in Up and Down Markets. The downside beta included in such a dual-beta model is considered to be a more appropriate measure of risk than the CAPM's regular symmetric single beta [36, 260–266]. Thus, the dual-beta approach, in addition to the regular CAPM beta, is used in this dissertation to examine whether changes in systematic risk associated with security breaches behave differently in economic recession or expansion periods.

Generally, beta factors change with the release of firm-specific news as investors adjust their estimates of risk associated with their investment in the respective firm [267–269]. Extant literature features only limited empirical evidence on information security breaches and the impact on firms' systematic risk. In their study on five breached consumer electronics firms between 2011 and 2015, Hinz et al. [33] showed that the aggregate change in firms' systematic risk of 0.022 was positive, but insignificantly small. Their findings thereby implied that breached firms' cost of equity, and hence cost of capital, do not increase [33]. Similarly, Nicholas-Donald et al.'s [35] examination of 29 security breaches between 2000 and 2010 revealed an insignificant increase in the risk factor of about 4%. These results are contradicted by a study published in 2012, in which, in a sample of 38 events from 2002 to 2008, it was established that firms' beta factors increased significantly following a security breach announcement [34].

Relatedly, Havakhor et al. [270] recently presented evidence suggesting that information

[18]See Sections 3.5.2 and 5.7.1 for further discussions of this exemplifying case study.

security investments can reduce cost of capital. Given that information security investments are intended to mitigate negative economic repercussions stemming from potential security breaches, the effect of breaches should be precisely diametrical to that of investments. Put differently, security breaches are likely associated with increases in cost of capital. As cost of equity is one constituent of cost of capital, an increase in cost of obtaining equity financing should be observable following a security breach.

Extant literature features only limited and contradictory evidence as to security breach-induced impacts on financial systematic risk, a measure at the core of firms' cost of equity (see [33, 271]). Additionally, there is no empirical evidence on how security breaches affect firms' systematic downside and upside risks. As prior literature on security breaches and financial systematic risk (a) is relatively scarce, (b) tends to be industry-specific (and typically not generalisable), and (c) is exclusively focused on symmetric systematic risk, there is ambiguity with regards to whether, and to what extent, security breaches affect organisations' exposure to market risk (i.e., systematic risk).

Based on limited previous empirical evidence, it is reasonable to assume that rational investors assign greater systematic risk (i.e., higher beta factors) to breached firms' stock and hence expect greater returns on investment to compensate for their risk incurred. Accordingly, it is hypothesised as follows.

C2-H1. Severe security breaches in publicly listed companies are associated with increased cost of equity, as indicated by positive changes in systematic risk (i.e., regular beta).

C2-H2. Severe security breaches in publicly listed companies are associated with increased cost of equity in a bull market, as indicated by positive changes in systematic upside risk (i.e., upside beta).

C2-H3. Severe security breaches in publicly listed companies are associated with increased cost of equity in a bear market, as indicated by positive changes in systematic downside risk (i.e., downside beta).

It is thereby expected that changes in downside beta exceed those in upside beta, as downside beta is considered to be a more appropriate measure for risk associated with an investment [36], and investors are expected to be more wary and aware of a firm's negative news history during Down Markets relative to Up Markets[19].

[19]The argument that investors pay more attention to negative firm news is in line with Kahneman and Tversky's Prospect Theory and Utility Theory [272–274].

2.8 Security Breach Costs: Cost of Debt

This section provides the background to and motivation for Contribution **C3** in Chapter 6, in which changes in firms' cost of debt following severe security breaches[20] are assessed. **C3** builds upon **C2**, which established that security breaches increase systematic risk, thereby by implication elevate cost of equity and eventually a firm's weighted average cost of capital (WACC).

As delineated above (see Sections 2.5 and 2.8), WACC is one of the most important metrics in corporate finance as it indicates investors' expected rate of return and hence external financing costs. A thorough investigation of financing costs as an underlying / consequential cost category for the purpose of ENBIS assessments requires an analysis of the other constituent of WACC — cost of debt (i.e., cost of raising capital from debt markets) — as well. Ceteris paribus (i.e., keeping all other elements of WACC unaltered), firms with lower cost of debt feature lower cost of capital, and thus the abilities to command higher company valuations and to invest in lower-return projects [105,157,255]. Contribution **C3** is accordingly based on the argument that increases in cost of debt, as proxied by wider credit default swap (CDS) spreads, should also be considered as an underlying / consequential cost item in holistic ENBIS investment analyses. The dissertation conjectures that similar to increases in cost of equity, changes in cost of debt can easily be overlooked by security executives, but should be incorporated into firms' considerations of breach-related costs and security investment decision making.

There is currently very little evidence on information security breaches-related changes in cost of debt, and no evidence on the relationship between security breaches and credit default swap spreads — which, as will be argued in this section — constitute the most suitable proxy for analyses on changes in cost of debt around security breach announcements. More generally, given the relative novelty of the CDS market, there is little academic research on the implications for corporate financial practice [275]. These gaps in the literature motivated the research question, which can be stated thus: *Do severe security breaches increase firms' cost of debt by elevating perceived default risk?*

The literature review in this section provides the requisite knowledge to frame the methodology in Section 3.6 and the eventual contribution in Chapter 6. This section thereby explains CDS spreads and their conceptual relevance for firms' cost of debt, financing costs, and hence cost-based ENBIS assessments. Chapters 6 and 8 then reflect on the empirical results and implications and provide ideas for further research into changes in cost of debt following information security breaches.

[20]The term severe security breaches is defined in Chapter 3.

The results of this study are of high relevance to information security decision makers attempting to quantify the negative impact of security breaches and hence pertinent to the overarching goal of this dissertation. Additionally, the results contribute to theoretical research on CDS market efficiency and professional credit trading practice.

2.8.1 Cost of Debt and CDS Spreads

Cost of debt is the rate of return debt investors expect to earn on their investments. This rate can also be thought of as the opportunity cost of capital for investors holding a firm's debt [110]. Conceptually, cost of debt is fundamentally influenced by the default risk of the debt-issuing firm, but also by investors' considerations of current levels of interest rates on the market and the tax advantage stemming from the tax deductibility of interest payments [215, 216]. The pre- and post-tax cost of debt can thereby be defined as [216]:

$$\begin{aligned} K_d &= r_f + \textit{default spread} \\ K_{d_{pt}} &= (r_f + \textit{default spread}) * (1 - t) \end{aligned} \tag{2.5}$$

Here, K_d and $K_{d_{pt}}$ are the pre- and post-tax cost of debt, respectively, r_f is the country- or industry-appropriate risk-free rate, *default spread* is the default spread[21], and t is the marginal corporate tax rate. The risk-free rate is exogenous to the firm and relatively easily observable. For many debt instruments, particularly private ones, the London Interbank Offered Rate (LIBOR) has been used as a proxy for the risk-free rate, which results in such debt instruments being quoted as a spread over LIBOR. Spreads over the LIBOR benchmark rate indicate the rate charged for borrowing capital in excess of LIBOR. Financial debt instruments thereby rely on LIBOR as a benchmark in order to protect both borrowers and lenders from interest rate volatility. As corporate tax rates and risk-free rates can often be regarded as given, the difficulty in the ex-ante estimation of cost of debt lies in establishing appropriate default spreads[21], which hence become the central element of analysis and negotiation. Credit rating agencies such as Moody's Investors Service, S&P Global Ratings, and Fitch Ratings provide issuer- and issue-level credit ratings. Current and implied credit ratings can be used to estimate default spreads. For instance, in 2019 the global corporate default rate for the rating category B was 1.49%, whereas CCC/C-rated debt had a default rate of 30.05% [276].

It is worth noting that from a more holistic perspective, a firm's total cost of arranging debt finance could also include considerations pertaining to search costs, underwriting fees, expenses for legal and financial advisors, and other arranging costs; however, such considerations are of less significance for the analysis of expenses paid to obtain debt financing in

terms of both amounts and theoretic and professional relevance, and are thus not considered herein.

Changes in costs of debt (K_d) — **C3**'s object of analysis — can be observed from three major perspectives: post-issue book value-based interest rates, at-issue interest rate spreads, and, most importantly, post-issue market-based spreads.

First, from a post-issue book value-based perspective, effective interest costs can be computed from financial statement data via dividing interest expenses by the average book value of financial debt [277–280]. However, measuring cost of debt generally, and changes in the metric specifically, according to this perspective is problematic. Measuring cost of debt in terms of (book value-normalised) interest expenses, merely leads to an ex post facto measurement of cost of debt. Moreover, changes in cost of debt cannot be measured in a timely manner and can hence not be attributed to individual events. As this present study is interested in quantifying the effect of security breaches on cost of debt, a forward-looking market-based metric that adjusts to news items in a timely manner is needed.

Second, cost of debt is often approximated by taking the at-issue promised yield[21] on recently issued debt [58]. In the case of bank loans, analysts can observe the spread of the interest rate paid on the loan relative to a benchmark rate such as the LIBOR. In the case of bonds, one could observe the coupon rate, yield to maturity, or yield to worst. As firms do not necessarily issue new debt instruments frequently, changes in cost of debt cannot be measured in a near-real time way, and individual events' impact can hence not easily be singled out.

[21] From a strictly theoretical perspective, one might distinguish between promised (or redemption) yield, expected yield, expected default loss, and expected risk premium (see [215, 281, 282]). The promised yield (i.e., redemption yield) on a debt instrument, which is the coupon or interest payments on the debt, is equal to the risk-free rate plus the sum of the expected default loss and the expected risk premium. Technically, the expected debt investors' return (i.e., cost of debt) should be defined as the promised yield net of the yield equivalent of expected default losses. Put differently, the expected return rate (i.e., cost of debt) is the appropriate discount rate when discounting coupon and principal payments — both adjusted for default risk assumptions — to the present value of a bond. The difference between the expected rate and the risk-free rate is the risk premium that should be included in the cost of debt, the difference between the expected rate and the promised rate is the expected default loss. The expected rate is thereby always lower than the promised rate if the default risk is non-zero.
However, although default risk might actually only account for approximately half of the total cost of debt [278], the distinction between expected default loss and expected risk premium is uncommon in research, and even more so in practice. First, distinguishing between the two components and estimating the expected rate of return according to this particular definition is difficult and "based on assumptions that are unlikely to hold in reality" [283, p. 74]. In practice, it is hence "not recommend[ed] to adjust the promised interest rate or redemption yield" [281, p. 136]. Second, particularly for investment-grade issuers of debt, the difference between the promised and the expected yield is negligible, and using the promised yield hence only results in low levels of divergence from the "theoretical" cost of debt [215]. Third and foremost, information security and financial executives in publicly listed firms, the main unit of analysis in this dissertation, are unlikely to make the aforementioned distinction and can safely be assumed to simply assess cost of debt in terms of promised yields and as a function of the risk-free rate plus an appropriate default risk factor (i.e.,

Third, post-issue market-based estimations of cost of debt are generally viewed preferentially, as up-to-date data on outstanding debt provides a good metric of expected cost of debt reflecting the present risk of default [82]. A market-based assessment of cost of debt is commonly approximated by the volume-weighted blended yield on outstanding debt instruments, using the observable current yield on publicly traded bonds and an equivalent market-based yield rate in the case of private debt [82]. Changes in post-issue debt spreads can provide a more timely indication of breach-induced changes in cost of debt, particularly in the case of post-issue changes in publicly traded debt, for which updated prices are available in a timely manner (e.g., on a daily basis). Bond yields accordingly constitute a major cost of debt indicator for market participants and corporate finance professionals [216, 284].

Credit default swap (CDS) spreads constitute another post-issue market-based indicator that can be used to estimate firms' cost of debt. CDS contracts are over-the-counter (OTC) credit derivatives quoted on public markets that are essentially insurance agreements guaranteeing the payment of a notional value to the buyer in case the underlying referenced firm defaults on a referenced corporate bond. The buyer of a CDS pays the seller the quoted spread multiplied by the notional value as a quarterly-paid annuity until either a default occurs or the stated maturity is reached. The CDS buyer is granted the right to sell bonds equal to the agreed notional value at their face value to the seller of the insurance if the issuing firm defaults on the underlying bond (i.e., the credit event[22]). The credit event must be documented as set out amongst other terms in the Confirmation Form of the original OTC CDS transaction [110, 285–288].

For instance, suppose that a buyer of bonds with principal payments totalling \$10 million at the end of the bonds maturity wishes to buy protection for the full face value of debt owned, to protect against the default of the underlying issuer. Suppose further that said investor buys full protection via a single-name credit default swap with a 200 basis point (bp[23]) premium. The buyer of the CDS pays the seller a premium of $A/360 * 200$ per quarter, typically in arrears, for protection, with A denoting the actual number of days during a quarter (see [289]). The CDS buyer in return obtains the right to sell bonds with a face value of \$10 million at this value to the seller of the protection should the referenced

default spread). Accordingly, this dissertation does not distinguish between expected default and expected return premium in the way presented in this footnote, but instead — as common in practice and empirical research — refer to pre-tax cost of debt simply as a function of a risk-free rate plus a credit risk rate (i.e., the default spread) as presented in Equation 2.5.

[22]The referenced entity's failure to pay is typically the credit event specified in OTC CDS transactions. Other common credit events may include bankruptcy or (debt) restructurings of the referenced entity.

[23]Note that one basis point (bp) denotes an absolute value or a difference of one hundredth of a percent, i.e., 0.01% or $\frac{1}{10,000}$. For instance, a change of 0.50 percentage points is equal to a change of 50 basis points.

firm suffer from a default event[24]. The parties to the protection agreement may agree to either a physical settlement or cash settlement in case of a credit event (see [289]).

CDS spreads are particularly suitable to measure changes in firms' cost of debt. First, prices are quoted constantly and potential increases can thus be observed on a frequent (e.g., daily) basis, whereas new loan issues can only be observed every once a while and are thus subject to confounding events diluting the impact of a particular security breach event. Moreover, CDS spreads can be observed directly, whereas bond prices are based on selecting risk-free rates as reference points, seniority, embedded options, and covenants. Bond spreads also include elements unrelated to default risks and imply time-to-maturity effects. In contrast, new standard-maturity CDS contracts are issued on a daily basis. The market for CDS contracts is also more liquid than the secondary corporate bonds market, with smaller bid-ask spreads, which renders the CDS market more efficient and prices more reliable. Furthermore, CDS spreads offer a "purer" indication of default risks given their standardised and homogenous nature [285, 288–295].

Second, measuring cost of debt in terms of CDS spreads closely resembles an outside investor's perspective on cost of debt [296, 297], which is in line with the perspective this dissertation takes in the context of establishing the severe security breaches database used for $\mathbf{C2} - \mathbf{C4}$[25]. A practitioner's perspective is arguably the most relevant one, as financial practitioners (i.e., financial firms' analysts) are the economic agents responsible for assessing companies' risk levels and thus dictating the terms for obtaining fresh capital on debt markets.

Third, and most relevantly, given that cost of debt are essentially a representation of a company's default risk [289], CDS spreads are by definition theoretically and conceptually close to default spreads. As CDS contracts constitute an insurance against company defaults, CDS spreads can be considered the most suitable measurement to estimate default risks and the closest to an ex-ante metric to estimate changes in cost of new to-be-issued debt issuances following corporate events.

CDS spreads represent market-based assessments of a company's default risk. This implies that CDS spreads are a more direct measurement of risk relative to, for instance, corporate bond spreads which inherently require an arbitrary choice of a baseline risk-free rate [285, 288, 298]. In general, the implied probability of default can be approximated from

[24]Or, more specifically, should the referenced underlying bond be subject to a credit event.

[25]The overall aim of the sample construction approach/sampling process was to mirror the information gathering and decision making process of equity analysts, investors, and other market participants following security incidents in publicly listed companies.

CDS spreads as follows (see [299, p. 360] and [215])[26].

$$\overline{\lambda} = \frac{s(T)}{1 - R} \tag{2.6}$$

Here, $\overline{\lambda}$ is the average hazard rate of default occurring between time zero and time T, $s(T)$ is the CDS spread for maturity T, and R is the recovery rate (i.e., the proportion of the principal of the defaulted debt investors can expect to recover despite the credit event in per cent).

Put differently, CDS spreads provide a market-based approximation of investors' average loss rate expectations and the implied default probability. Given that firms' credit spreads, and accordingly cost of debt, are mainly a function of default risk [114, 289], and that credit risk is the most relevant indicator of CDS spreads [215, 301][27], CDS spreads that accurately reflect average default risk provide a near-real time metric to measure changes in cost of debt. Assuming a recovery rate R of zero, that is, the underlying firm defaults and is not able to pay back any of the principal on its corporate bonds, the CDS spread *is equal to* the default risk, and can thus be used as a direct proxy for *default spread* in Equation 2.5 when calculating firms' cost of debt (see e.g., [297]). Relatedly, to re-emphasise the connection between default spreads, CDS spreads, and bond spreads, in a frictionless arbitrage-free market, and given the absence of other costs, a CDS spread is equal to a floating-rate bond spread over the risk-free rate [286]. In practice, as the CDS market has been gaining in maturity since 2008, banks have increased the practice of so called market-based pricing whereby borrowers' interest rate spreads are explicitly coupled with their CDS spreads [304].

In summary, "the [...] attraction of CDS spreads is that no adjustment is required: they are already credit spreads." [290, p. 2792]. CDS spread changes thereby stem from changes in the yield curve and in credit risk (see [289]). The analysis in this dissertation thereby deducts the components associated with changes in the yield curve to establish the effect of information security risk events on changes in credit risk. CDS spreads are accordingly ideally suited to measure market-based changes in default risk and hence differences in cost of debt following corporate events. Consequently, changes in CDS spreads following security breaches are analysed in this dissertation to represent changes in investors' expected rate of return on debt investments, i.e., firms' cost of debt.

[26] Equation 2.6 is a simplification of the relationship between CDS spreads and default risk, see e.g., [286, 290, 299, 300] for further considerations and the valuation of CDS options.

[27] Other explanatory variables for CDS spreads include leverage, market liquidity, market and business cycle indicators (see [288, 301–303]).

2.8.2 Prior Empirical Studies and Hypothesis Development

Contribution **C2** published in [2] has shown that security breach events are correlated with an increase in firms' cost of equity [2]. The aim of Contribution **C3** is to establish whether severe security breach announcements are also associated with a statistically significant impact on cost of debt as measured by widening CDS spreads that function as a proxy for default spreads. Due to the nature of underlying / consequential items in the ENBIS cost-based framework[28], there is currently very little evidence on information security-related changes in financing costs generally, and security breach-induced changes in cost of capital (i.e., cost of equity and cost of debt) specifically.

As this study is the first to empirically analyse the impact of severe security breaches on CDS spreads around the breach announcement, previous publications exploring (public) credit markets' reaction similar to this present one are scarce. Security breaches' negative impact on equity market valuations is well-established [26, 30, 170–182]. Given the inherent inverse relationship between equity and debt markets (i.e., share prices and CDS premia), one can reasonably expect to observe widening CDS spreads in the short-term surrounding breach events on the OTC off-exchange CDS market whilst average public exchange-based stock prices go down. Relatedly, an increase in cost of debt does not only suggest elevated company default risks stemming from, for instance, diminished cash flow (stability), but might also result from reduced abilities to attract equity investors.

The study closest to Contribution **C3** is a recent (non-peer reviewed job market) paper by Binfarè [201]. The author primarily analysed security breach-induced changes in at-issue debt spreads, establishing that in the four years following a security breach, lenders to attacked firms charge 15 to 20% larger spreads over LIBOR relative to similar non-breached peers, which is economically and statistically significant. However, [201] also found that such an at-issue cost of debt increase mainly applies to lenders such as banks, but not to new issues of corporate bonds. Specifically, average corporate bonds' at-issue-spread (i.e., the difference between a corporate bond's yield to maturity (YTM) and a government bond's YTM of similar duration) does not increase at a statistically significant level. In theory, CDS spreads are approximately equal to the spread of a same-maturity bond's yield over the risk-free rate [290, 305]. Following the results of Binfarè [201], when measuring changes in cost of debt after a security breach in terms of CDS spreads, one can also not necessarily expect to observe an increase in premia.

In a related recent study by Huang and Wang [306] on 139 data breach events from 2004 to 2014, the authors compared bank loans from within three years before a breach to

[28] The concept of underlying / consequential cost items is explained in Section 2.8.1.

those issued three years after a security breach. The researchers found that breached firms are subjected to greater increases in bank loan spreads, collaterals, and loan covenants than control firms [306]. On average, successfully attacked firms are associated with a 22.1 percent (i.e., 39.85bp) increase in loan spreads in the year after a security breach. The effect is more pronounced in cases of criminal attacks as well as larger breaches in terms of records lost.

Whilst Binfarè's [201] and Huang and Wang's [306] findings are highly relevant and motivate the present study, they differ from Contribution **C3** in the empirical set-up employed to generate insights into investors' perceived changes in operational risk. As delineated in Section 2.8.1, there are three major temporal perspectives on firms' cost of debt. Whilst at-issue (promised) rates provide indications as to the level of return debt investors expect to generate on their investment (i.e., their default risk assessments) at the time the particular debt instrument is issued, at-issue rates do not provide a near-real time measurement of severe security breaches' effect on cost of debt around their announcements. Only post-issue market-based spreads can reliably isolate the effect of a particular event on credit markets and indicate near-event shifts in investors' risk perception. Nevertheless, post-breach changes in CDS spreads convey information about investors' expected shifts in default risk assessments that are likely to also carry over to subsequent new debt issues. Accordingly, any trends established around the security breach announcement are likely to also be reflected by later at-issue rate changes and vice versa. Following this line of argumentation, one should be able to observe changes in CDS spreads around a security breach as well. However, given that CDS spreads are conceptually closer to the public debt market on which corporate bonds are issued and traded, based on Binfarè [201], it is also plausible to argue that there should not necessarily be a statistically significant connection observable.

As explained in Section 2.8.1, post-issue market-based bond yields provide a more indicative measurement of changes in cost of debt. There is currently no explicit empirical evidence on security breaches' effect on bond yields. However, analysing 643 security breaches across 401 firms between 2005 and 2016[29], Iyer et al. [307] recently found that bond prices do also not exhibit statistically significant changes in the three-day, eleven-day, and 31-day event windows surrounding a security breach announcement. Only the two-month event window centred on the security breach revealed a statistically significant association indicating that bond prices decrease by approximately 2% following a security breach. Given the inverse relationship between bond prices and yields, the authors' study implies that bond yields (and accordingly cost of debt) increase in the long run following security breaches. How-

[29]Larger sample studies such as the one studied by Iyer et al. [307] do typically not differentiate between severe and non-severe security breaches. In fact, [307] emphasises that only 24% of the security breaches in their sample met materiality criteria pertaining to the nature and scope of the respective security breaches.

ever, similar to Binfarè's [201] findings, the study on abnormal bond returns suggests that credit markets do not react significantly to the multitude of negative economic repercussions stemming from security breaches in the short-term around a successful attack.

Relatedly, Havakhor et al. [270] recently presented evidence suggesting that information security investments can reduce cost of capital. Given that information security investments constitute countermeasures intended to mitigate negative economic repercussions stemming from potential security breaches, the effect of successful attacks should be precisely diametrical to that of investments. Put differently, security breaches are likely associated with rises in cost of capital. As cost of debt are the other major constituent of cost of capital besides cost of equity, an increase in cost of debt should be observable around a security breach.

The information security economics literature provides only sparse evidence on security breaches' effect on cost of debt, and no analysis of CDS spread changes particularly. Whilst the corporate financial economics literature is rife with studies on multiple types of corporate events' impact on equity markets, there is also relatively little research on corporate events' and characteristics' effect on credit markets and specifically CDS markets (see [275]). This is due to the fact that the market for such credit derivatives is relatively young, given that it has only grown and matured noteworthily since the first versions of standardised CDS contracts were published by the International Swaps and Derivatives Association in 1998 (see e.g., [288, 290, 308]). Nevertheless, the body of research on CDS levels, changes, influencing factors, and their relevance for financial market participants has been growing constantly since the first CDS contracts were traded in the early 1990s[30].

It is generally well-accepted that credit market participants consider relevant information in their pricing process. For instance, lenders and underwriters have been shown to consider firms' disclosures in annual and quarterly reports, press releases, and public announcements to reduce uncertainty when assessing firms' default risk premiums and hence cost of debt (see [284]).

Various previous studies have thematised the effect of corporate events on CDS spreads. Given the inherent conceptual and empirical connection between credit quality, default risk, and CDS premia [276, 303], one particularly well-studied area is the relationship between credit ratings and CDS spreads. Rating agency announcements, which convey fundamentally important information to credit investors, are thereby inversely related to CDS spreads. The studies presented in Hull et al. [290] and Norden and Weber [310] are amongst the most noteworthy ones on event-induced changes in CDS spreads. Hull et al. [290] was one of the first to show that CDS spreads react to firm events. Analysing spreads before and after credit rating events between 1998 and 2002, [290] showed that in the 90 days before a

[30]For a broad literature review on CDS contracts see [309].

rating downgrade event, CDS spreads surge by almost 38 basis points. In the event window including the two days immediately around a review for downgrade event, CDS spreads on average increase by almost 10 bps.

Similarly, assessing credit rating downgrades and reviews for downgrades between 2000 and 2002, Norden and Weber [310] found that CDS spreads adjust upwards prior to such rating events and in the event window immediately surrounding the downgrade event. The effect is, however, only existent for negative but not significant for positive credit rating events. These early seminal findings have since been corroborated by subsequent studies analysing the impact of credit rating announcements on corporate CDS markets [311–316].

It is also well-documented that accounting earnings, which arguably constitute the most important information metric available to investors due to the nearly perfect correlation between cash flows and market value [58,105], have a significant influence on CDS prices [288, 295, 308, 317–325]. For instance, Callen et al. [288] demonstrated that earnings, cash flows, and accruals are significantly negatively correlated with CDS spreads. Particularly, analysing CDS prices in a three-day event window surrounding preliminary earnings announcements, the authors revealed that CDS premia are inversely related to the direction of earnings surprises. Shivakumar et al. [295] showed that management earnings forecasts significantly affect credit default swap premia, and that such reactions are particularly pronounced for companies with lower credit ratings and during periods of greater market uncertainty. Given that security breaches can affect firms' earnings potential, a connection between breaches and CDS premia can reasonably be expected.

More recently, several studies have broadened the body of literature by providing additional evidence pertaining to the impact of other corporate events and characteristics on CDS spreads analysing, for instance, the adoption of the Sarbanes-Oxley Act [285] and International Financial Reporting Standards [326, 327], the narrative disclosure of risk factors in corporate filings [328], financial institutions' stress test results [329], corporate social responsibility ratings [330], short sale disclosures [331], index revisions [332], and corporate diversification [333].

CDS spreads are a function of credit quality [290]. As delineated in Section 2.3.2, security breaches are associated with a plethora of obvious and underlying / consequential costs that all have the potential to negatively affect earnings quality, profitability, and cash flow volatility. Successful information security attacks might hence hamper firms' ability to service debt interest and principle payments, leading to greater credit risk (i.e., likelihood of defaulting). If severe information security breaches in fact convey new information to the market indicating that firms' ability to service their debt might be reduced, CDS spreads should react accordingly.

Put differently, an expected decrease in earnings can imply a worsening in operating and financial performance and therefore a greater probability of bankruptcy. A breach-induced worsening of credit quality (i.e., a greater credit default risk) is likely to be recognised by credit market participants in their private debt, bond, and CDS pricing models in terms of greater *default spread* factors. Such considerations might accordingly be reflected by widening CDS spreads, which are an ideal proxy for credit risk, and might eventually lead to debt investors demanding greater returns on investment and hence elevated cost of issuing new debt.

In summary, security breaches are known to elicit severe disruptions and a multitude of obvious as well as underlying and consequential negative economic consequences, potentially reducing firms' stable cash flow generating abilities and thereby introducing credit risk for debt investors who are particularly sensitive to unfavourable news given their asymmetric payout profiles. Other types of corporate events — which are arguably more directly related to firms' financial performance and might therefore carry greater informational value to investors — are known to be associated with significant impacts on CDS premia around their respective announcement dates. Overall, extant related empirical and conceptual evidence hence suggests a positive connection between security breaches and cost of debt as proxied by CDS spreads.

However, there is currently only very scarce empirical evidence on the association between security breaches and debt, and no previous analysis leveraging credit data available in terms of short-term CDS premia changes. In fact, there are also indications that successful information security attacks are *not* associated with (short-term) public debt market impacts. On balance, it is nevertheless reasonable to expect security breach announcements to be associated with widening CDS spreads as the conceptual reasoning and strong evidence in support of increases in cost of (private) debt following breaches outweighs counterfactual indicative evidence.

Based on theoretical work and limited previous empirical evidence laid out above, it is reasonable to expect that severe security breaches increase default risk spreads as proxied by CDS premia, indicating rises in cost of debt, similar to the positive change in cost of equity established in Contribution **C2**.

In keeping with the tradition and logic of standard event study methodology [224–228], and its application of the semi-strong form of the Efficient Market Hypothesis, only short-term event windows around the (adjusted) security breach announcement date are analysed in this study. The analysis thereby assumes that market participants fully price in new pieces of information immediately and that short-term changes in CDS spreads provide a holistic time value-adjusted (i.e., appropriately discounted) reflection of *all* expectations on future

developments.

To this end, it is hypothesised as follows:

C3-H1. Severe security breaches in publicly listed companies are associated with increased cost of debt, as indicated by short-term abnormal CDS spread changes.

2.9 Security Breach Costs: Information Asymmetries

In this section, the motivation and literature review pertaining to Contribution **C4** in Chapter 7, which thematises increases in firms' information asymmetries elicited by severe security breaches[31], are introduced. **C4** is based on the notion that security breaches lead to an increase in the (perceived) gap between information possessed by firm insiders (e.g., management teams) and firm outsiders (e.g., investors), and that such an increase in information asymmetries can eventually lead to an increase in financing costs. As discussed in Section 2.5, the level of asymmetric information is therefore one of the elements of fundamental consideration for corporate executives occupied with managing firms' financing costs.

Studies on the effect of information asymmetry on cost of capital go back to classical financial theory (see e.g., [334–336]). Informational differences stem from informed market participants such as firms' executives having greater access, abilities, and incentives to understand and evaluate complex strategies than (retail) investors do. Executives' price-relevant information pertaining to their firms put them in a better position to examine the quality of their firm's strategy and stock's fair value. Informed market participants may also trade on (their expectations of) future disclosures. In most jurisdictions, corporate insiders — one particular group of "informed market participants" — can legally trade in securities of their own firms as long as such trades are not based on material non-public information (see e.g., [39, 337]).

Theory and empirical studies posit that both temporary and permanent increases in information asymmetry decrease liquidity, dampen investors' ability to make efficient stock allocation decisions, and eventually elevate expected stock returns [214, 222, 338–341]. The direct connection between principal-agent information asymmetries — leading to signalling problems and adverse selection issues — and financing costs is, for instance, illustrated in Myers and Majluf's seminal Pecking Order Theory [112, 113, 223], arguing that investors penalise the issuance of financial instruments if executives know more than outsiders about the true value of the firm. Firms are therefore inclined to rely on internal financing first, then debt, and only finally issue equity [112, 113].

[31] The term severe security breaches is defined in Chapter 3.

An overwhelming majority of empirical studies has shown that more pronounced information asymmetries are associated with increases in firms' cost of capital generally [342], and cost of equity [221, 222, 338, 339, 342–348] and cost of debt specifically [284, 349, 350][32].

In summary, the informational advantage possessed by informed corporate insiders impedes valuation and risk assessment processes, creates adverse selection problems, and therefore eventually increases investors' return requirements, diminishes share prices, and increases financing costs [112, 113, 217–220]. Based on their fiduciary duty (see [17, 18, 75–81]) and their equity-based remuneration (see [86–88]), corporate management teams are incentivised to mitigate negative impacts on share prices and financing costs caused by exacerbated information asymmetries.

Even though considerations of information asymmetries are of high relevance to firms' financing costs, there is currently no empirical evidence on security breach-induced long-term changes in information asymmetries that can affect firms' cost of capital. Additionally, no previous academic analyses of the empirical relationship between security breaches and insider trading abnormal returns beyond immediate breach announcement periods — which constitute a particularly strong proxy for principal-agent information asymmetries — have been published so far. These gaps in the literature motivated **C4**'s research question, which can be stated thus: *Do severe security breaches increase firms' cost of capital by elevating information asymmetries in the long run?*

In this section, previous relevant literature is surveyed to inform the methodology presented in Section 3.7, which was used to generate the results for Contribution **C4** in Chapter 7. In this present section, the research question's background and the reasoning for using the aforementioned measurement are explained. In Chapter 7, an analysis of the empirical results and a discussion of relevant implications is provided.

The eventual finding that security breaches are associated with medium- to long-term increases in information asymmetries is highly relevant for information security academics and executives who strive to lower breaches' negative economic impacts, which includes actively managing financing costs. Moreover, the results contribute to the academic literature on market efficiency and insider trading.

2.9.1 Firm-Level Events' Impact on Information Asymmetries

Previous financial management and accounting literature identified various events pertaining to core corporate fundamentals that can affect levels of asymmetric information. Prior

[32]It is worth noting that the argument that the level of information asymmetry between insiders and outsiders affects cost of capital is not entirely uncontroversial (see e.g., [343, 351–353]).

studies thereby predominantly focused on the effect of accounting earnings events on investors' levels of perceived information asymmetry (e.g., [354–363]). Other researchers studied changes in information asymmetries around bankruptcies [364]; auditor changes [365]; open market stock repurchases [366]; and unscheduled announcements, such as acquisition and ratings events [367]. The aforementioned studies established that the release of information fundamental to the issuing firm's performance have a substantial impact on information asymmetries. Generally, positive uncertainty-reducing news items are associated with reductions in information asymmetries and vice versa. Whilst these studies established relevant methodologies and empirical results, the event types analysed are mostly focused on fundamental corporate restructurings or financial performance indicators.

Empirical research on changes in information asymmetries around less frequently occurring events, particularly negative unexpected events is scarce (see [368]). One of the few examples includes Brooks et al. [369]. Examining a potpourri of 21 exogenous shock-inducing events, ranging from refinery explosions to CEO deaths, the authors established wider intraday bid-ask spreads surrounding the events, indicating elevated levels of information asymmetry in the short run [369].

Similarly, there is some evidence that the occurrence of unexpected operational risk events is associated with elevated information asymmetries. Analysing 331 financial firms' operational risk incidences such as fraud, employee malpractice, and most relevantly, system failures between 1995 and 2009, Barakat et al. [368] found that initial disclosures of such events are associated with significant short-term increases in information asymmetries on equity markets as proxied by effective spread, a modification of standard bid-ask spreads, and percentage price impact of trade, an estimate of adverse selection risk based on post-trade price adjustments [368]. Given that information security is generally considered to be part of firms' operational risk assessment responsibilities [144, 370, 371], and that breaches feature characteristics akin to other operational risk events, particularly system failures, it is reasonable to expect similar market reactions following security breach disclosures.

The study closest to Contribution **C4**, and the first empirical study on the asymmetrical information environment around security breaches, is a publication by Rosati and colleagues [372]. Analysing 74 security breaches in 62 firms between 2005 and 2014 in an event study framework, the authors found a significant short-term association between breaches and information asymmetries as proxied by bid-ask spreads and trading volumes on the announcement day. The findings imply that security breaches create greater uncertainty and potential exposure to informed traders for market makers [372]. However, analysing an eleven-day event window centred on breach announcements, Rosati et al. [372] did not establish any negative effects on asymmetric levels of information before or beyond the event

day, leading the authors to conclude that there is little informed trading and that markets are fully efficient with regards to pricing in security breach information.

These findings are corroborated by Bianchi and Tosun [199], who demonstrated significant increases in trading volumes and bid-ask spreads in event firms relative to control firms on security breach announcement dates.

Building upon Rosati et al.'s [372] findings, a study featured in [373] (a recently published DBA dissertation) presented an analysis of security breaches' spillover effect on information asymmetries. Assessing changes in information asymmetries, in terms of abnormal trading volumes and bid-ask spreads, pertaining to breached firms as well as their competitors yielded mixed and contradictory results. Analysing eleven-day event windows centred on security breaches showed weak evidence in support of breached firms being subjected to increased information asymmetries. Specifically, average daily abnormal trading volumes and bid-ask spreads were only significantly different from zero on day t_{-2} relative to a security breach. Additionally, cumulative abnormal turnover was only shown to be significant in the [-1, 0] event window, whilst cumulative abnormal bid-ask spreads were not shown to be statistically significant at common levels in any considered event window.

Analysing the same metrics for breached firms' competitors, it was revealed that daily abnormal trading volumes were significantly greater than zero, indicating greater liquidity and hence lower information asymmetry, for t_{-3}, t_{-1}, t_3, and t_4 around a focal firm's security breach announcement [373]. However, the study also demonstrated contradictory evidence, showing that daily abnormal bid-ask spreads were indeed significantly greater than zero, suggesting increased levels of asymmetric information, on t_{-3}, t_{-2}, t_{-1}, t_2, t_4, and t_5 [373].

2.9.2 The Need for an Advanced Measurement of Information Asymmetries

Although extant empirical results provided by previous studies ([372], [199], and [373]) are of high relevance and motivate the research project at hand, they provide contradictory results and suffer from two significant limitations pertaining to the measurement of information asymmetries that Contribution **C4** resolved.

First, there are issues pertaining to the usage of bid-ask spreads and trading volumes as proxies for information asymmetry generally. Notwithstanding the frequent usage of bid-ask spread as a proxy for illiquidity and information asymmetries in empirical studies (see e.g., [338,339,342,344,348,374]), quoted bid-ask spreads are not necessarily the most appropriate proxy for information asymmetries. Bid-ask spreads are primarily a measurement of market makers' liquidity provision and as such reflect not only information asymmetry, but

also substantial non-information components such as inventory risk, order processing costs, market maker commissions, and geographical effects [356, 368, 375, 376].

Moreover, it is worth re-emphasising that bid-ask spreads are mainly based on market makers' assessments of the presence of informed and uninformed traders in the market and order-related costs (see e.g., [340, 341, 354]). This contribution examines information asymmetries from a financing costs perspective. As financing costs are not driven by market makers, but rather by different types of market participants, it is more appropriate to establish a different market-based measurement of information asymmetries.

Basing assessments of information asymmetry on the other most common proxy, trading volume, is not unambiguous either. Theoretical arguments can be made in favour of both increasing and decreasing trading volumes when investors are faced with intensified information asymmetry issues, depending on traders' price elasticity and timing discretion (see [367, 372, 377–379]).

Both proxies, bid-ask spreads and trading volume, also do not distinguish between buyer- and seller-related information asymmetries. For instance, Rosati and colleagues [372, p. 152] specifically acknowledge that one of the key limitations of their study is that their empirical set-up "does not allow [...] to separate buying and selling activity" which are potentially associated with different market behaviour patterns pertaining to the information asymmetries around security breaches.

The second issue of previous studies that used bid-ask spreads and trading volume as proxies for information asymmetry pertains to time horizons. The two studies closely related to Contribution **C4** ([372] and [373]) only presented analyses of short-term eleven-day event windows. Long-term studies of event-driven changes in information asymmetries are thereby generally scarce[33].

The short-term impact of events on information asymmetries is of high relevance and carries important implications for shareholders and financiers. However, managers concerned with the impact of security breaches on financing costs also require long-term measurements, as information asymmetries may revert to previous (lower) levels in the long run, leaving financing costs eventually unaffected (see [380]).

As delineated in Section 2.3.2, a substantial proportion of security breaches' permanent (i.e., long-term) costs broadly relate to customers' and business partners' loss of trust (see e.g., [30]). The effect of lower levels of trust, raising uncertainty and hence measures of information asymmetry around security breaches (see e.g., [372]), might only substantiate

[33]Even assessments of events that are fundamental to core firm characteristics often only assess intraday or short multiday event windows (see [354, 356, 358–360]). Studies by [363] and [380] constitute two of the few examples of analyses on long-term information asymmetry implications of corporate events.

in the long run. Moreover, Contributions **C2** and **C3** indicated that both equity and debt markets are not necessarily fully efficient in terms of Fama's [108, 109] Efficient Market Hypothesis with regards to security breaches. Accordingly, it is pertinent to analyse long-term changes in breach-induced information asymmetries as well.

Relatedly, the problem of information asymmetries in the context of data security is not only well-established in the management of financing costs and corporate finance literature (see e.g., [112, 113, 217, 218, 220]), but also in the research and practice of cyber risk insurability (see e.g., [247,248,250,381,382]. The overarching narrative in this cyber risk insurance literature suggests that adverse selection and moral hazard, two instances of information asymmetry, also exacerbate insurers' pricing conundrum. Cyber risk insurance scholars and professionals typically assess risk with a long-term view and are not only interested in the short-term costs and uncertainties associated with information security breaches. Accordingly, to inform medium- to long-term assessments of information asymmetry, cyber risk insurers are also likely to benefit from a measurement quantifying information asymmetries that goes beyond the near-event impact of breaches.

2.9.3 Alternative Information Asymmetries Measurement and Hypothesis Development

To strengthen the sparse and contradictory literature on underlying / consequential financing costs generally and information asymmetries around security breaches specifically, and to resolve the two issues delineated above, Contribution **C4** makes use of a novel measurement of principal-agent information asymmetries. Specifically, insider trading abnormal returns — a measure nascent to the corporate strategy-related literature generally (see [37]), and financial economics of information security specifically — were used as a proxy to assess changes in information asymmetries induced by security breaches.

Insider trading is defined as corporate insiders (e.g., executives, directors, and significant stockholders) buying and selling financial instruments in their own firms. In most jurisdictions, such trading is generally considered legal, as long as transactions are not based on material non-public information, duly reported to the relevant authorities, and compliant with local regulations such as those introduced by the US Securities Exchange Act of 1934 or the EU 2014 Market Abuse Regulation (see e.g., [39,337]). Corporate insiders in Europe, the United States, and multiple Asian countries can legally trade in their own firms' securities, but are obligated to report their trades to the relevant market authorities. Assuming that insiders are rational economic agents, who intend to maximise their private wealth, they do not trade randomly, but on superior information or knowledge of future cash flows in their

firms. Their advanced insights into firms' opportunities, threats, and competitive positioning in the market allow insiders to perceive mispricings relative to current share prices as well as future changes in cash flows [383]. When corporate insiders deem current prices too low, they are likely to be net buyers. When prices seem too high, they turn into net sellers.

There is substantial evidence suggesting that legal insider trading filings constitute new and useful information to outside investors, enabling them to price assets more effectively and efficiently, which results in asset prices reflecting the intrinsic value of the underlying firm more accurately [39,384–388]. Previous studies demonstrated that insider trading filings convey firm-specific information to market participants, as insiders trade on superior knowledge or feelings about future performance and perceived stock mispricing [383, 386, 389–393][34].

Insider trading filings are (theoretically) publicly available to all outside investors and other market participants. Following the logic of Fama's [108, 109] Efficient Market Hypothesis, outsiders factor insider transactions into their pricing models and trade on them accordingly. Abnormal stock market returns following insider trades indicate the informational value or information content conveyed to the market [391, 396, 397, 408, 411]. They represent the incremental value of new pieces of information relative to the total amount of information about a firm and its strategy prior to a filing and thus function as a proxy for ex-ante principal-agent information asymmetries. The higher these abnormal returns are, the greater the informational value of an insider filing is, and therefore the more substantial the ex-ante information asymmetries between the firm and its outside investors were.

Abnormal stock market returns following insider trades are a more suitable proxy for changes in information asymmetries around security breaches than bid-ask spreads and trading volumes for multiple reasons[35]. First, insider trading abnormal returns (ITAR) by definition feature a large informational component and actually reveal the level of principal-agent information asymmetries, as opposed to bid-ask spreads that indicate differences between informed and uninformed traders. Second, ITAR are market-based, but not market makers-based, i.e., they are based on an aggregation of market participants' assessments of the informational difference between outside investors and corporate insiders. Third, the mea-

[34]It is well established that corporate insiders profitably trade shares in their own firms on US [394–397], European [391, 398, 399], and Asian [400, 401] markets. Insiders' firm-specific insights may stem from multiple sources. Previous research argued that insiders may base transactions on their interpretation of financial information, which may differ from analysts' expectations, knowledge of internal forecasts, a better understanding of the company's competitive position in the market relative to competitors, or simply a better 'gut feeling' [402–404]. Moreover, insiders benefit from their knowledge of proposed mergers [405], new issue announcements [406], dividend announcements [407], expected R&D outcomes [386, 408], and imminent breakthrough developments and product announcements [389, 409]. Additionally, there are studies revealing evidence of insiders' firm-level market timing skills [410] and their ability to anticipate economy-wide developments [39].

[35]Note that bid-ask spreads and insider trading intensity are actually correlated [412].

sure lends itself to long-term assessments of changes in information asymmetries as insider trades do usually not occur on breach event days, but rather with some time lag on either side of a breach announcement. Finally, using ITAR allows for distinguishing between buy and sell information asymmetry, as the principal-agent information asymmetries indicated by insider selling and buying activities can be examined separately.

Contribution **C4** is related to the emerging strand of information security economics literature concerned with establishing that insiders may trade on their knowledge of imminent security breach announcements to avoid incurring losses [337, 413–422]. For instance, Lin et al. [416] found that insiders avoid average losses of $35,009 by selling shares before the announcement of a security breach, which "(...) sows distrust between stakeholders and the firm's management and serves to erode investor confidence in the integrity of financial markets." [416, p. 14]. Similarly, Mitts and Talley [415] found that mean levels of open interest and trading volumes in put options are higher for breached firms in the two months prior to breach disclosures. This present study builds upon the aforementioned implications, however, it does not thematise insider trading shortly before security breach announcements and the potential necessity to regulate such market activities. Instead, this contribution is concerned with medium- to long-term changes in information asymmetries and focuses on the informational value of insider trades.

There are multiple aspects to changes in principal-agent information asymmetries following security breaches. First, security breaches' negative economic impact is notoriously difficult to analyse. Given the mixed evidence on short- and long-term impacts of security breaches, quantifying the impact on future cash flows is difficult generally, but even more complex for outside investors who have to rely on secondary information, whilst executives are better informed about earnings impacts. Market participants may also question firms' overall resilience and risk management. Investors, who are uncertain as to the exact consequences of security breaches, are likely to perceive even greater levels of valuation uncertainty and an exacerbated disparity between executives' quality and quantity of information and their own knowledge. This widening knowledge gap between informed and uninformed investors is likely to be reflected in measures of information asymmetry.

A security breach event thereby elevates both types of agency problems: adverse selection and moral hazard. Investors are faced with adverse selection issues as they do not have access to full information as to how a security breach affected the underlying firm and what remedial strategies managers pursue. Moral hazard issues occur inter alia as executives can hide their activities and are unlikely to be held personally responsible for the (mis-)management of information security threats and failures. These issues are further compounded by a general post-breach reduction of trust in management (see [30]), as high levels of trust and

trustworthiness are one pivotal element to mitigating agency problems (see e.g., [423–427]).

Even if breached firms' (security) executives act to the best of their knowledge and belief and conceive efficient and effective strategies to mitigate negative repercussions of severe security breaches, principal-agent information asymmetries might intensify anyway. Strategies that are unique, novel, unknown, untested, or less straightforward are generally associated with greater information asymmetries as evidenced by elevated insider trading abnormal returns [37]. As severe security breaches tend to be infrequent events, for which executives might not have a standard "playbook" and lack experience and preparation, breach mitigation strategies are inherently prone to be unique, novel, and untested. Information asymmetries can be expected to rise accordingly.

Given the greater uncertainty as to the future financial and operational performance of breached firms, investors have a greater demand for indications of how the firm and their post-breach strategies fare. Due to these elevated principal-agent information asymmetries, trades by executives and other insiders in breached firms are expected to convey greater levels of informational value to outsiders.

The effect is thereby anticipated to be particularly pronounced in post-breach insider purchase transactions, as insider buy transactions carry greater informational content and therefore generate greater abnormal returns generally [391, 396, 410][36].

Previous research showed that frequent events affecting core firm fundamentals impact levels of information asymmetry [354–367]. Security breach disclosures are conceptually close to infrequently occurring events and operational risk announcements (see [144, 370, 371]), which have been shown to exacerbate the agency problem of asymmetric levels of information as well [368, 369]. Information security breaches, similarly unscheduled events conveying negative surprises and uncertainty to outside market participants, are thus likely to be subject to similar market dynamics.

Contribution **C4** thematises the effect of successful data security attacks on information asymmetries. If security breaches introduce additional uncertainty, for instance, as to the effectiveness of security breach recovery strategies, and corporate disaster prevention and management generally, measures of information asymmetries can be expected to increase.

The studies closest to this contribution ([199, 372, 373]) confirmed that security breaches generate additional uncertainty resulting in elevated intraday information asymmetries. In order for information asymmetry changes to have a lasting effect on financing costs, such surges in uncertainty need to persist beyond the intraday effect of breach announcements.

[36]The observation that insider purchase transactions are more informative than insider selling transactions is largely due to the fact that insiders, who tend to be paid with shares as part of their remuneration packages, regularly sell large numbers of shares due to liquidity needs.

Motivated by the gap in the literature on firms' post-breach information environments, and the absence of empirical evidence on medium- to long-term post-breach information asymmetries, a different empirical set-up was used for Contribution **C4** to investigate whether security breaches are associated with long-term increases in principal-agent information asymmetry.

Based on previous studies and the expectation that post-breach information asymmetries remain at greater levels, with the phenomenon being particularly pronounced in the case of insider purchase transactions, it is hypothesised as follows[37]:

C4-H1. Severe security breaches in publicly listed companies are associated with significant increases in information asymmetries as proxied by insider trading abnormal returns.

C4-H1a. Insider purchase transactions exhibit a stronger association between security breaches and information asymmetries as proxied by insider trading abnormal returns.

[37] **C4-H1** and **C4-H1a** are hereafter referred to as Contribution **C4**'s main hypothesis and sub-hypothesis, respectively.

Chapter 3
Methodology

This chapter delineates the thorough data collection, filtering, and cleaning process applied to generate the samples to analyse underlying / consequential costs of security investments (i.e., abnormal returns following security certifications) and breaches (i.e., increases in cost of equity and debt as well as information asymmetries). The chapter also provides the reasoning for using particular methodologies and explains the empirical approaches used to generate empirical results for subsequent chapters.

Most of Sections 3.1 to 3.5 on data collection and empirical analysis methodologies is based on **MP1** [1] and **MP2** [2].

Some sentences, particularly in Section 3.7, are based on [39] and [37], in which the conceptual framing of insider trading abnormal returns as a proxy for strategy-related information asymmetries was established.

3.1 Data Sources and Sample Characteristics: Empirical Dataset Security Investment Costs

In order to assess the effect of security certificate investments on firms' stock prices, data regarding the selected types of standards needed to be collected. Generally, obtaining access to official databases on Cyber Essentials (Plus) and ISO/IEC 27001 certificates is difficult as certification bodies are generally (and understandably) reluctant to provide such data for competitive reasons. In the following subsections, we first look at the process of establishing the Cyber Essentials (Plus) sample (see 3.1.1), then we discuss the ISO/IEC 27001 sample (see 3.1.2).

3.1.1 Cyber Essentials (Plus)

The UK Department for Business, Innovation and Skills launched the Cyber Essentials programme in 2014, intending to create a common minimum level of capabilities required by

companies bidding for UK Government contracts involving the processing of sensitive and personal information. Since its inception, the Cyber Essentials programme has been intended to provide organisations of all sizes with guidelines pertaining to systems and processes to support basic information technology security [428, 429]. The Cyber Essentials programme is operated by the National Cyber Security Centre (NCSC), which requires IT infrastructure compliance across five technical control categories: firewalls, secure configuration, user access control, malware protection, and patch management [430].

Organisations intending to achieve Cyber Essentials certifications choose a certification body and complete a self-assessment questionnaire. To achieve the Cyber Essentials Plus certification, compliance with the aforementioned five technical controls is verified by one of five certification bodies appointed by the NCSC [431]. In order to retain certificate validity, the certification process needs to be undertaken annually [428].

The sample of Cyber Essentials certification events was constructed as follows. First, a list containing all FTSE 350 Index constituents as of July 2018 was downloaded from *S&P Capital IQ*[1]. The analysis was restricted to organisations which have their primary listing on the London Stock Exchange as the Cyber Essentials programme is primarily aimed at British organisations. The 350 largest firms by market capitalisation were chosen as these index constituents are subject to coherent financial disclosure requirements, more closely followed by the public and financial analysts, and traded at greater liquidity — which facilitates more efficient incorporation of new pieces of information as per the semi-strong form of the EMH [108, 109].

Second, a database containing (re-)certifications of FTSE 350 firms needed to be established. To this end, as there is no official complete database of all certifications provided e.g. by the NCSC, an unofficial database of firms granted a Cyber Essentials certificate had to be constructed. NCSC's Cyber Essentials website provides a list of accreditation bodies[2]. Two auditors issuing Cyber Essentials certificates, *CREST* and the associated firm *IT Governance*, provide lists of firms they certified[3][4]. These lists were downloaded as of July 2018. All FTSE 350 Index constituents were looked up in these lists of certified organisations provided by the two auditors to find associated certification events. Additionally, for every firm, a manual NCSC certificate search[5] was conducted. Combining these two sources of data led to some conflicting data entries, particularly with regards to certificate issuance dates — in which cases priority was given to the NCSC certificate search record. Neither

[1] `https://www.capitaliq.com/`
[2] `https://www.cyberessentials.ncsc.gov.uk/getting-certified/`
[3] `http://www.cyberessentials.org/list/`
[4] `https://www.itgovernance.co.uk/cyber-essentials-certified-organisations`
[5] `https://www.cyberessentials.ncsc.gov.uk/cert-search/`

database allows for differentiating between initial certifications and re-certifications. Both Cyber Essentials and Cyber Essentials Plus certificates are considered in the analysis as the award of either requires cooperation with an official certification body.

For all certification events, the date of the respective certification, the certification type (Cyber Essentials or Cyber Essentials Plus), the name of the certified entity, its organisational hierarchical status (parent/holding company or subsidiary) and the source of the record (CREST/IT Governance, NCSC, or both) were noted, which resulted in the final certification events database used. Event dates (i.e., days on which firms were certified according to the sources used) that fell on a non-trading day were adjusted to reflect the nearest trading day. It should be noted that it is debatable whether this dataset represents an accurate and complete list of all certifications. Specifically, not all firms feature repetitive entries in the database, which suggests that not all firms seek re-certifications[6]. Moreover, although care had been taken to exclude obvious errors, there remains some noise in the data such as seemingly double certifications of the same entity. However, as the database constitutes a sufficiently large sample to test the hypothesised empirical relationship, and is based on official (NCSC) and semi-official (CREST/IT Governance) sources, it is deemed adequate for the intended purpose.

Table A.1 in Appendix A provides details on all certification events assessed in this study. The final sample contains 145 certification events, of which 90 are Cyber Essentials and 55 are Cyber Essentials Plus (re-)certifications, respectively. Of these 145 events, 64 stem from the CREST/IT Governance list, 61 were found via the NCSC certificate search, and 20 records were present in both types of sources. Within the sample, 66 events relate to parent/holding companies and the remaining ones to subsidiaries. The sample represents events in 62 listed firms across 38 different industries. The most frequent industries represented are Human Resource and Employment Services (29 events), Aerospace and Defence (20 events), and Asset Management and Custody Banks (11 events). An overview of the sample is presented in Table 3.1, which shows that there has been a constant year-over-year growth in certifications, indicating that the certificate is becoming increasingly relevant for organisations.

3.1.2 ISO/IEC 27001

ISO/IEC 27001, part of the ISO/IEC 27000 Information Security Management Systems family, provides internationally accepted requirements for Information Security Management Systems [432]. It is developed and maintained by the International Organization for

[6]Firms that do not feature repetitive entries apparently do not pursue annual re-certifications. This appears to be unusual as firms certified once are incentivised to maintain their (re-)certification if they intend to continue bidding for UK Government contracts.

Table 3.1: Cyber Essentials (Plus) Sample

Year of certification	No. of certificates
2014	3
2015	14
2016	25
2017	56
2018	47
Total	145

Standardization (ISO) and the International Electrotechnical Commission (IEC). The standard features 114 controls across 14 clauses and objectives which are intended to mitigate organisational information security risks [433]. The previous (2005) version of the standard required the usage of the controls, whereas currently, organisations can become certified to ISO/IEC 27001:2013 without adhering to all controls. The controls include, inter alia, requirements pertaining to access control, communications security, supplier relationship, incident management, and business continuity management. In order to demonstrate compliance with the standards, a company may announce it meets the requirements following an internal self-assessment. However, in order to fully benefit from potential advantages provided by the management system standard, companies may choose to become certified by an ISO-accredited certification body. To maintain an ISO/IEC 27001 certification, minor annual surveillance audits, as well as major recertification audits three years after the initial award, are required. The ISO/IEC 27001 certificate has by now become a global, widely accepted, standard for security certifications [243]. The global number of organisations certified according to ISE/IEC 27001 standards was 36,362 in 2019 [434].

To create a sample of ISO/IEC 27001 certifications, a copy of the publicly available Certified Organisations Directory of the Joint Accreditation System of Australia and New Zealand (JAS-ANZ)[7] was downloaded in November 2018. The directory includes organisations certified by JAS-ANZ-accredited Certification Bodies[8] and thus features certified companies from multiple countries. All non-public companies were filtered out, which resulted in 84 certification events. For the remaining ones, additional corporate and financial information was downloaded from *S&P Capital IQ*. Excluding companies for which such information could not be found resulted in a usable sample of 77 events, out of which 18 relate to parent/holding companies, and 59 to certifications of subsidiaries, respectively. These events mainly constitute newly awarded certificates. The entire sample is detailed in Table B.1 in Appendix B. An overview of the sample is presented in Table 3.2, which indicates an

[7] `http://www.jas-anz.com.au/our-directory/certified-organisations`
[8] `http://www.jas-anz.com.au/about-the-jas-anz-register`

Table 3.2: ISO/IEC 27001 Sample

Year of certification	No. of certificates
2011	1
2015	4
2016	15
2017	19
2018	38
Total	77

Table 3.3: ISO/IEC 27001 Sample Countries

Country	No. of certificates	Country	No. of certificates
Australia	17	New Zealand	3
Austria	1	Nigeria	1
China	2	Oman	1
Denmark	1	Poland	1
France	1	Qatar	1
Germany	1	Singapore	1
Hong Kong	1	South Africa	2
India	9	Switzerland	2
Ireland	1	UAE	1
Israel	1	UK	2
Japan	14	USA	9
Lebanon	1	Vietnam	2
Netherlands	1		
Total			76

increase in firms' interest in the certification over time, in line with the growth in global demand for ISE/IEC 27001 certifications generally [434]. Table 3.3 shows that most JAS-ANZ (re-)certificates were awarded to companies headquartered in Australia (17) and Japan (14).

3.1.3 Combined Regression Sample

In order to further analyse potential firm and market characteristics influencing whether an investment in security standards is perceived favourably or unfavourably by market participants, a combined sample was constructed. Following the main analysis of Cyber Essentials (Plus) and ISO/IEC 27001 certifications, the two samples including the computed abnormal returns (see Section 3.4 below) were merged. Additionally, the following variables were downloaded from *S&P Capital IQ*: primary industry; total assets in USD million as per the most recent annual report prior to the certification event date; one-year-average daily volume of shares traded in millions of shares; one-year-average price-to-book ratio; and earnings

before interests, tax, depreciation, and amortisation (EBITDA) as per the two most recent annual reports prior to the event date.

3.2 Data Sources and Sample Characteristics: Empirical Dataset Security Breach Costs

In order to analyse the predicted effects of major security incidents on firms' systematic risk, CDS spreads, and information asymmetries, a representative sample of such security breaches in publicly listed companies had to be created. Generally, obtaining a holistic, accurate, and complete database on major security breaches in public companies is difficult (see e.g., [435]). Despite the arguable potential to increase stock market transparency, capital market authorities do not provide official lists of information security breaches in publicly listed companies. In addition, there is no exhaustive government-sponsored database detailing all security breaches in organisations [436]. Analysing publicly listed companies also gives rise to difficulties related to, for example, companies changing names, tickers, and ownership statuses.

Given the absence of any authoritative source of data, a novel dataset was built based on the Privacy Rights Clearinghouse (PRC) database, which is commonly used in similar studies (e.g., [164, 180, 202, 437]). The PRC database is considered to be the most extensive systematic publicly available database on security incidents, and combines security breach data from government and media sources [164, 437].

The PRC database was used as the basis for this dissertation's dataset as US-based companies are commonly subject to extensive data breach notification laws [436], the US stock market is generally considered efficient and highly liquid [438], and public US companies are subject to high equity analyst and media coverage — all of which contributes to a strong information environment [439].

The final sample was constructed as follows. First, the entire PRC database for entries between January 2005 and May 2019, including information on company names, security breach publication dates, number of records breached, and descriptions of incidents was downloaded. This initial list featured 8,921 incidents pertaining to 7,608 unique companies that experienced security breaches. In order to establish which of these companies were public when they experienced a security breach, a global list of all companies with publicly traded equity between 2005 and 2019 was downloaded from *S&P Capital IQ*[9]. Two approximate

[9] `https://www.capitaliq.com/`

string matching techniques[10] were used to merge the list of public companies to the initial PRC database. All organisations identified as publicly listed were validated manually to delete false positive matches (e.g., public companies with similar names, or companies that at the respective privacy breach announcement date were not already, or no longer, publicly listed). Additionally, to verify the accuracy of the aforementioned merging approach, unique companies' public ownership statuses were also examined manually for half of the overall data set of breached organisations (4,460 individual security breach events) by conducting individual manual searches on *S&P Capital IQ*.

PRC-listed privacy breaches in subsidiaries were excluded from the dataset unless the incident pertained to a direct subsidiary (i.e., companies which can intuitively be identified as subsidiaries of publicly listed companies: national subsidiaries and those with names very similar to the publicly listed parent company/that share a similar name with their respective listed parent company)[11]. Similarly, cases in which publicly listed companies' data was affected, but the security breach itself occurred at an (unnamed) vendor or supplier, were excluded.

The aforementioned steps resulted in a preliminary sample of 655 companies that experienced privacy breaches between January 2005 and May 2019. Subsequently, security breaches that were subject to confounding events (e.g., delistings, mergers and acquisitions) shortly before or after the privacy breach announcement were excluded as such confounding events would skew focal events' potential effects on systematic risk, CDS spreads, and information asymmetries.

Crucially, in line with the semi-strong form of the Efficient Market Hypothesis [108, 109], only incidents that provoked media attention were included in the sample[12].

The remaining security incidents were classified into severe and non-severe breaches according to the type, volume, and publicity of the respective privacy breach. A rigorous qualitative case-by-case analysis approach was followed that included reading all case descriptions provided by PRC, publicly available online media reports, and court filings (if

[10]The two approximate string matching techniques used were *Microsoft Excel Fuzzy Lookup* and *Microsoft Excel Wildcard VLOOKUP.*

[11]The rationale here is that market participants are unlikely to expect substantial negative economic impacts on public companies following privacy breaches in one of their indirect or distant subsidiaries. Moreover, it is fair to assume that (lay or retail) investors are unlikely to be aware of ownership structures if these cannot be deducted from company names. This approach is in line with the logic presented in previous studies, in which it was argued that "a breach on [a remote/differently-named subsidiary's] products might have less of an effect on the stock of [the parent company]" [180, p. 8–9].

[12]The existence of at least one relevant and unambiguous news item was verified using a general web search, as well as specialised websites such as `https://www.breachclarity.com`, which is endorsed by the Identity Theft Resource Center, a resource used by the United States Securities and Exchange Commission (see `https://www.sec.gov/files/speech-jackson-cybersecurity-2018-03-15-data-appendix-updated.pdf`), and hence likely used by stock market participants.

available). The analyses described in the following chapters only included incidents that financial market participants without sophisticated technological knowledge were likely to identify as severe high-level security breaches of cash flow-affecting severity for the listed entities. The definition of how typical market participants would define security breaches' severity was based on intuition, own experience, and off-the-record explorative conversations with two professional London-based investors and two Oxford-based retail investors. The definition of severe security breaches applied is thereby in line with Cavusoglu et al.'s [30] sampling process.

To this effect, severe breaches were defined as security incidents that were the result of intentional coordinated or systematic effort to exploit weaknesses in (non-)physical security systems with malicious intent motivated by gaining personal utility. Hence, minor accidents and cases of negligence (e.g., inappropriate disposal of personal information), deliberate privacy breaches (e.g., companies selling customer data), losses (e.g., documents lost in transit), and casual theft/petty theft (e.g., stolen employee laptops) were excluded from the sample. Similarly, small-scale self-contained, isolated, or local incidents, such as the use of card skimmers or an employee using customer data to set up fake accounts, were also excluded.

To ensure robustness and reproducibility of the classification process, a random subset of 100 public companies' security events (i.e., $> 15\%$ of the preliminary sample) was assessed by a second coder with regards to the security events' severity following Lavrakas [440]. At a first meeting, the second coder, a postdoctoral researcher at the University of Oxford with qualitative research experience, was presented with the sample subset and the above definition of severe and non-severe security breaches. The second coder independently categorised the random subsample of security incidents into severe / non-severe security breaches. At a second meeting, the two coding results were compared. The two coders achieved an initial percent agreement score of 89% across all events, indicating a high level of inter-coder reliability. Discrepancies in event classifications were discussed and found to be due to misunderstandings of the categorisation criteria. Eventually, the two coders were in full agreement on all categorised events.

The overall aim of the sampling process delineated above was to mirror the information gathering and decision-making process of equity analysts, investors, and other market participants following security incidents in publicly listed companies. As mentioned above, the sample construction approach was thereby modelled on conversations with professional and retail investors.

Table 3.4 provides an overview of the sampling process described above. The final sample used for this dissertation's studies consisted of 202 severe security breaches, for which an-

Table 3.4: An overview of the sampling process

Filtering step	(Sub-)sample size
PRC database (01/2005–05/2019)	8,921 breach events
Filtering out non-public firms' incidents and non-direct subsidiaries	655 firms
Filtering out confounding events, breaches without media attention, and non-severe breaches	202 breach events

nouncement dates[13], breached entity names, parent company names, market capitalisation at breach announcement, country of primary listing, and other financial information were recorded. Out of 202 security breach events, 181 related to firms with a primary listing on a US stock market. The 164 listed companies in the sample had an average market capitalisation of $52,019.92m at their security breach announcement. Of the 202 incidents, 49, 39, 32, and 28 incidents occurred in the Consumer Discretionary, Information Technology, Financials, and Communication Services industry sectors, respectively. Table C.1 in Appendix C provides an overview of the security breach events included in the sample.

3.3 Other Data and Ethics Approval

All corporate and financial data — including daily share prices to establish abnormal returns following security investments (i.e., changes in equity value), increases in systematic risk (i.e., cost of equity), and insider trading-induced abnormal returns (i.e., information asymmetries), as well as CDS spreads to determine changes in cost of debt — were downloaded using *S&P Capital IQ*.

Insider trading data, used for Contribution **C4** in Chapter 7 to determine changes in information asymmetries, was provided by *2iQ Research GmbH*[14]. The comprehensive database covers insider trades in most listed firms and is well established, having been used in multiple previous academic studies on insider trading (e.g., [39, 399, 441]). 2iQ Research GmbH collects insider trading filings from countries' market authorities (such as the US Securities and Exchange Commission), stock exchanges, financial news, and company websites.

Financial, firm, and insider trading databases were merged via unique firm identifiers with the main samples of security investments and severe security breaches to yield the

[13]In case of conflicting announcement dates or multiple entries for the same security breach, the earlier announcement date was taken into account for the ensuing analyses. Announcement dates were adjusted to the nearest trading day if the actual announcement day fell on a non-trading day.

[14]Access to the *2iQ Research GmbH* database was provided by 2iQ's co-founder Patrick Hable and facilitated by *Altana Wealth Limited*.

overall datasets used in the respective empirical studies.

Research ethics approvals were considered for all four Contributions and underlying research projects. Ethics approvals were not necessary for the studies pertaining to Contributions **C1** to **C3** as no personal data was involved in the respective research projects. The only study which featured human "participation", or rather involvement, to some extent is Contribution **C4**, in which individual executives' trades in financial instruments were analysed. The Computer Science Departmental Research Ethics Committee's review concluded on 11/09/2019 that no CUREC application process was necessary as executives' names were removed and individual transactions were aggregated on firm-level prior to any analysis.

3.4 Empirical Methodology: Investment Value Creation and Destruction / Asset Disposal

In this section the theories, principles, and statistical methods used to analyse the samples of information security standards certifications are described and one example for the analysis of abnormal returns following Cyber Essentials certifications is illustrated. Furthermore, the regression analysis to establish firm characteristics potentially affecting the perception of information security investments and hence abnormal returns is explained. The results obtained from the analytical procedures laid out below are presented in Chapter 4.

3.4.1 Analytical Procedure: Abnormal Returns Analysis

Implied financial gains and losses associated with investments in information security standards can be assessed in terms of value creation indicated by short-term stock price reactions. To establish abnormal stock price reactions following Cyber Essentials (Plus) and ISO/IEC 27001 certification events, standard event study methodology [224–228], which is based on the Efficient Market Hypothesis [108, 109], was applied. Event studies can be considered the standard methodology of quantifying immediate market reactions to news in the context of information security economics [182, 229–231]. As rational market participants in efficient markets swiftly adjust their expectations of future cash flows, immediate market responses upon news reflect an assessment of current corporate activities' effect on future performance.

Daily returns were defined as

$$\frac{price_{i,t}}{price_{i,t-1}} - 1 \tag{3.1}$$

Here, $price_{i,t}$ is the share price of firm i on day t. For each certification event, n, expected

returns were established using a one-factorial market model based on Sharpe's [117] single-index model[15], regressing individual firms' stock returns on the respective country's broad index[16] over the estimation window of 252 trading days. Using the market model, which assumes a linear relationship between stock return and market return, in this way is common within the field of IT and information security investments [231, 233].

Event-specific coefficients were established via ordinary least square (OLS) regression. For each event, daily abnormal returns were defined as

$$\begin{aligned} AR_{i,t} &= R_{i,t} - E\left(R_{i,t}\right) \\ &= R_{i,t} - \left(\alpha_i + \beta_i R_{m,t} + \epsilon_i\right) \end{aligned} \tag{3.2}$$

Here, $AR_{i,t}$ denotes the abnormal return in security i on day t, $R_{i,t}$ the actual return in security i on day t, and $E(R_{i,t})$ the expected return for security i on day t. The coefficient α_i is the average stock return unrelated to market movements, β_i is the stock's sensitivity to returns of the index (defined as the covariance between the return of the stock and the return of the index divided by the variance of the index), $R_{m,t}$ is the daily return on the index, and ϵ_i is an unsystematic prediction error with an expected mean of zero.

Cumulative abnormal returns are defined as

$$CAR_i\left[t_I, t_{II}\right] = \sum_{t=t_I}^{t_{II}} AR_{i,t} \tag{3.3}$$

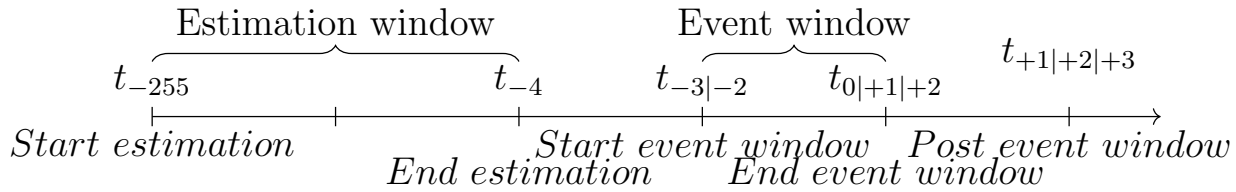
Here, $CAR_i\left[t_I, t_{II}\right]$ denotes the event-specific cumulative abnormal returns and t_I and t_{II} denote the beginning and end of the event window, respectively. To account for differences in Cyber Essentials (Plus) certification dates across the sources, as well as for likely information leakage prior to the public announcement of a corporate event [238,442,443], market reactions of up to three trading days prior to the certification date are included in the analysis. Specifically, t_I — the start of an event window — is either the trading day three (t_{-3}) or two (t_{-2}) days prior to the certification date. Long event windows allow for a delay in market participants' correctly assessing and pricing in a new piece of information and may enable the respective event information to substantiate (e.g., the certified firm might fend off a large-scale cyber-attack more effectively than competitors, or it might win a government contract it would otherwise not have gained). However, as longer event windows increase the risk of including confounding events' share price impacts [442], only short event windows

[15]Sharpe's single-index model is theoretically grounded in fundamental financial theory laid out by Markowitz's Modern Portfolio Theory [57] and the work by Sharpe [118], Lintner [119], Treynor [120], and Mossin [121], respectively, which led to the formulation of the Capital Asset Pricing Model (CAPM).

[16]A list of the indices used can be found in Table D.1 in Appendix D.

of up to two post-event days are analysed.

Hence, to measure short-term market reactions, event window end dates t_{II} were set to include the certification date, one, and two days following the certification date, respectively. The event windows are in line with those used in previous studies [124, 238]. The timeline below illustrates estimation, event, and post-event windows' durations.



The reasoning for centring the study on the certification date, as opposed to the date of the announcement that a certification has been or will be pursued, is as follows. Although there might be stock market value implications stemming from the implementation of security standards prior to the official announcement [238], it is conjectured that the official certification date constitutes the substantiation of actually being compliant with the respective standard. That is to say that only once an official certification body has independently and publicly announced that an organisation is certified according to a particular standard, potential customers can factor the certificate into their purchasing decisions. Consequently, only then may analysts, investors, and other market participants adjust their future cash-flow expectations and stock-price estimations accordingly. Similarly, market participants are likely to recognise breach probability and cost reduction potentials only after certifications have been officially granted by the respective bodies. Hence, it is reasonable to expect reductions in information asymmetries vis-à-vis information security capabilities (and thus positive share price reactions [444]) only after compliance with security standards has been conclusively established.

To mitigate the potential effect of outliers and to increase robustness, an additional measure of abnormal returns was introduced by winsorising cumulative abnormal returns in each of the two samples' event windows at the 0.15 level at each tail. To examine the statistical significance of unexpected share price behaviour following information security certifications, two-sided t-tests on all CARs' and winsorised CARs' means were performed to establish whether the population mean is significantly different from zero. Given the skewed distribution of individual event-specific CARs, non-parametric tests are likely to provide more reliable inferences in addition to parametric tests [228], and are commonly used in related literature (e.g., [30, 231]).

Accordingly, two additional non-parametric tests were conducted. First, sign tests on all event windows' CARs were performed to test whether the actual proportion of positive or

negative cumulative abnormal returns to total number of observations exceeds the expected proportion. In line with MacKinlay [228] and the random walk hypothesis [109], the expected proportions were set at 0.5, which resembles an equal chance of obtaining positive or negative abnormal returns in a given period of time. The test statistics, *positive ratio* and *negative ratio*, were computed by dividing the number of events with positive or negative cumulative abnormal returns by the total number of observations in the respective subsample. Second, two-sided Wilcoxon signed-rank tests under the null hypothesis that the one-sample Hodges-Lehmann-type pseudo-median is equivalent to zero were performed on all samples [445,446]. The parametric t-tests and non-parametric Wilcoxon signed-rank tests are non-directional to account for the fact that ex-ante it is not unambiguous whether the successful certification with an information security standard might be associated with any abnormal returns at all, not to mention the potential direction of such returns. Moreover, two-tailed testing can be considered more prudent and conservative (see, for example, [447]).

3.4.2 Illustration of Abnormal Returns Analysis

To illustrate the methodology of computing cumulative abnormal returns following security certifications, consider the following example. *Capita plc* had a Cyber Essentials re-certification in one of its subsidiaries, *Capita Business Services Ltd (CBSL)*, on 06/12/2017 (the event date). Expected returns were modelled by regressing *Capita plc*'s stock returns on the FTSE 350 during the period of time from 02/12/2016 to 30/11/2017. The event-specific β and α were estimated to be 0.49 and -0.0005, respectively. This implies that *Capita plc*'s stock was substantially less volatile than the market ($\beta < 1$) and that the firm's share price underperformed relative to the market ($\alpha < 0$).

As noted in Section 2.6, we assume that the Efficient Market Hypothesis holds in its semi-strong form. Hence, analysts, investors, and other market participants follow *Capita plc* and become aware of the Cyber Essentials re-certification, for instance, by following the company website, relevant industry news publications, or aggregate databases. The following stock market reaction upon the completion of the security standard certification is due to market participants changing their future cash flow estimations. Consider, for instance, the event day itself. On 06/12/2017, the FTSE 350 returned 0.195%. According to Equation 3.2, the expected return on *Capita plc* is 0.039%. The actual stock return on the day was 0.787%, which leads to an abnormal return of 0.748%. By following this procedure over multiple trading days before and after the event day, and summing the respective daily abnormal returns, a cumulative abnormal return of 4.129% for the event window $[-3, 2]$ was computed.

3.4.3 Analytical Procedure: Regression Analysis

To establish characteristics potentially affecting the perception of information security investments and hence abnormal returns as measured in the study, eight variables were examined in a subsequent regression analysis. In line with previous studies ([124, 231, 238, 241]) the timing of an investment, the industry group in which a firm primarily operates, the type of certification, firm size, and growth potential were considered. These characteristics can carry relevant implications about governance structures, IT maturity, and information asymmetries between the firm and its investors. Additionally, the country in which a firm is located, its stock liquidity, and its EBITDA growth were also considered. The country in which a firm is headquartered defines the legal environment in which it operates. Stock liquidity is an indicator of how efficiently new pieces of information, such as certification news, can be incorporated into the stock price. Investors in a firm with negative EBITDA growth may be inclined to favour other types of capital expenditure over information security investments.

Timing of the investment is a relative measure and defined as the number of days passed since the first event date in the sample (24/06/2014). The 59 industries in which firms primarily operate were clustered into 11 industry groups in line with *S&P Capital IQ's* industry clustering. Certification type was coded as a dummy variable (equal to 1, if the respective event is a Cyber Essentials (Plus) certification). Firm size is the natural logarithm of a firm's total assets in USD million as per the most recent annual report prior to the certification. Growth potential was computed as the natural logarithm of a firm's one-year-average price-to-book ratio (PBV, share price divided by book value per share), whereby a PBV greater than 1 implies that investors are valuing the respective firm higher than its net assets' worth. Liquidity was defined as the natural logarithm of the one-year-average[17] daily volume of shares traded in millions of shares. EBITDA growth is a dummy variable (equal to 1, if the EBITDA reported in the most recent annual report prior to the investment is greater than the EBITDA reported in the previous financial year).

In the first regression model, the effect of timing, industry group, certification type, and firm size on abnormal returns following Cyber Essentials (Plus) and ISO/IEC 27001 certifications was examine. In subsequent models, headquarters country, stock liquidity, growth potential, and EBITDA growth were added to the model. Coefficients were established via linear OLS regression. Across all models, the dependent variable are the post-certification event-specific cumulative abnormal returns in the event window $[-2, 2]$. The full model

[17] One year, starting on the respective event day, ending 365 days before the event date.

including all variables is defined as

$$\begin{aligned} CAR_{[-2,2]} = \beta_0 &+ \beta_1 Time + \beta_2 IndustryGroup + \beta_3 CertificationType \\ &+ \beta_4 FirmSize + \beta_5 StockLiquidity + \beta_6 GrowthPotential \\ &+ \beta_7 EBITDAGrowth + \beta_8 Country + \epsilon \end{aligned} \tag{3.4}$$

3.5 Empirical Methodology: Systematic Risk / Cost of Equity

In this section, the methodology used to establish post-security breach changes in systematic risk, in terms of regular betas and dual-betas, is described. We first cover how pre- and post-announcement betas as well as dual-betas for the sample of severe security breaches were calculated. Then, one exemplifying case is provided and the regression model is explained. The results obtained from the empirical analysis steps laid out below are presented in Chapter 5.

3.5.1 Analytical Procedure: Betas and Dual-Betas

The aim of this analysis is to establish differences in systematic risk in terms of beta prior and subsequent to severe high-level security breaches in publicly listed firms. Beta, a measure of correlated relative volatility, indicates the extent to which a listed firm's stock return volatility is correlated with the relevant index volatility, and thereby functions as an indicator of risk exposure to general market movements [118–121]. The dual-beta model extends the regular beta model by introducing downside and upside betas to measure downside and upside risk, respectively [259,260]. The methodology followed the approach of similar studies (e.g., those of [33, 448]).

For each security breach in the sample ($n = 202$), six sets of betas were computed: pre-breach regular beta, post-breach regular beta, pre-breach upside beta, post-breach upside beta, pre-breach downside beta, and post-breach downside beta[18].

Each set of betas consisted of 60 daily betas, which were calculated as follows. First, daily returns were established as firm i's share price on day t divided by firm i's share price on day $t-1$ (see Equation 3.1). The methodology to obtain regular beta factors is based

[18]Thereby assuming that investors assess each security incident individually. Accordingly, events in companies that repeatedly experienced high-level security breaches were analysed independent of previous incidents, as opposed to assuming autocorrelation or evaluating multiple breaches in aggregation.

on the Capital Asset Pricing Model (CAPM) [118–121][19]. According to the CAPM, a firm's cost of equity can be defined as

$$R_i = r_f + \beta_i \left(R_m - r_f\right) \tag{3.5}$$

Here, R_i denotes the expected return in security i, r_f is the risk-free rate, R_m is the market return, and $beta_i$ is the firm-specific indicator of systematic risk (i.e., correlated relative volatility). The difference between R_m and r_f is referred to as the *market risk premium*.

The value of $beta_i$, the stock's sensitivity to index returns, is estimated via ordinary least square regression of stock returns on index returns, and is defined as

$$\beta_i = \frac{cov(R_i, R_m)}{var(R_m)} \tag{3.6}$$

Here, $cov(R_i, R_m)$ denotes the covariance between an individual stock's returns and the market index and $var(R_m)$ is the variance of index returns. In line with similar previous studies ([33, 231, 233, 448]), an estimation period of one year (i.e., 250 trading days) was used to calculate daily beta factors based on Sharpe's one-factorial market model [117]. The US-oriented sample featured both firms with a primary listing on a US stock exchange as well as firms with a primary listing elsewhere. For this study, only primary listings were considered. Accordingly, for each event, the index used to proxy the market portfolio was the respective country's major multi-industry stock market index[20].

The computation of upside and downside beta factors is similar to the regular beta calculation approach presented above. It followed the Up and Down Markets dual-beta model laid out by Fabozzi and Francis [259] and Kim and Zumwalt [260]. Specifically, Sharpe's [117] single-index model was modified to include upside and downside beta factors to account for days on which a market portfolio's return was ≥ 0 or <0, respectively[21].

$$R_{i,t} = \alpha_i^+ D + \beta_i^+ R_{m,t}^+ D + \alpha_i^- (1 - D) + \beta_i^- R_{m,t}^- (1 - D) + \epsilon_{i,t} \tag{3.7}$$

[19] Alternative methods of estimating cost of capital include Gordon and Shapiro's [106, 107] Dividend Discount Model and Arbitrage Pricing Theory [449]. However, using the CAPM is more common in both academic studies and professional practice. Besides, applying the CAPM in the context of investigating cost of equity changes is coherent with its usage when analysing abnormal returns as a proxy for firm value creation/destruction following security investments (see Section 3.4) and information asymmetries (see Section 3.7)

[20] In line with similar empirical studies (e.g., [30, 231]), as well as financial theory based on Sharpe's single-index model conceptualisation of the CAPM [57, 117–121], market risk was proxied in terms of volatility of the respective country's broad major multi-industry stock market index. A list of the indices used to proxy country-specific market portfolios is provided in Table E.1 in Appendix E.

[21] Up Markets could also be defined differently. For instance, as such days on which market portfolio returns exceeded the average market return or the risk-free rate [260].

Here, $R_{i,t}$, firm i's stock return on day t, is defined as follows. For days t on which the market portfolio return was greater than or equal to zero, α_i^+ is the average stock return idiosyncratic to security i, β_i^+ is the upside beta factor, and $R_{m,t}^+$ is the index return on day t. For days t on which the market portfolio return was negative, the aforementioned logic applies vice versa. D is a binary variable which assumes the value of 1 in Up Markets, that is, when daily market portfolio returns are non-negative, and zero in Down Markets. $\epsilon_{i,t}$ is the residual term with an expected mean of zero.

β_i^+ and β_i^-, the stock's sensitivity to index returns in Up Markets and Down Markets, respectively, are estimated via ordinary least square regression of stock returns on the respective (non-)negative index returns, and are defined as

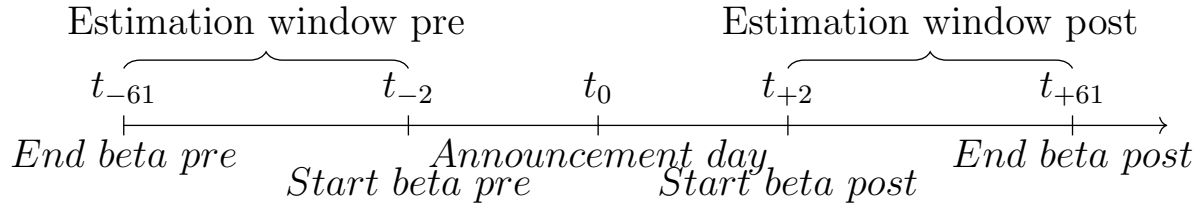
$$\beta_i^+ = \frac{cov(R_i, R_m^+)}{var(R_m^+)} \tag{3.8}$$

and

$$\beta_i^- = \frac{cov(R_i, R_m^-)}{var(R_m^-)} \tag{3.9}$$

Here, $cov(R_i, R_m^+)$ and $cov(R_i, R_m^-)$ denote the covariance between an individual stock's returns and the market index on Up Market days and Down Market days, respectively, and $var(R_m^+)$ and $var(R_m^-)$ are the variances of index returns on Up Market days and Down Market days, respectively. As delineated above, one-year upside and downside betas were calculated using the relevant indices. The number of trading days taken into account to determine dual betas varied contingent upon the number of days in a given year on which market portfolio returns were (non-)negative.

As illustrated below, all three types of daily one-year beta factors (regular, upside, and downside) were computed for periods of 60 trading days prior and subsequent to a security breach announcement, starting two trading days before and after the (potentially adjusted) announcement date, respectively.



As daily beta factors tend to be highly volatile [33], daily one-year beta factors were aggregated over a period of 60 days following graphical and statistical analysis of volatility and outliers of daily one-year betas aggregated between 50 and 90 days[22]. To analyse

[22]Results are qualitatively robust to aggregating over time periods of 50, 60, 70, 75, 80, and 90 days.

changes in systematic risk induced by severe security breaches, each set of 60 daily betas ($\Delta\beta_{i,\bar{t}}, \Delta\beta^{+}_{i,\bar{t}}, \Delta\beta^{-}_{i,\bar{t}}$) was averaged to yield one value, and differences between pre- and post-breach betas for each breach announcement in the sample were established as

$$\begin{aligned}
\Delta\beta_{i,\bar{t}} &= \frac{\sum_{t=t_{+2}}^{t_{+61}} \beta_{i,t}}{60} - \frac{\sum_{t=t_{-2}}^{t_{-61}} \beta_{i,t}}{60} \\
\Delta\beta^{+}_{i,\bar{t}} &= \frac{\sum_{t=t_{+2}}^{t_{+61}} \beta^{+}_{i,t}}{60} - \frac{\sum_{t=t_{-2}}^{t_{-61}} \beta^{+}_{i,t}}{60} \\
\Delta\beta^{-}_{i,\bar{t}} &= \frac{\sum_{t=t_{+2}}^{t_{+61}} \beta^{-}_{i,t}}{60} - \frac{\sum_{t=t_{-2}}^{t_{-61}} \beta^{-}_{i,t}}{60}
\end{aligned} \tag{3.10}$$

In order to account for potentially distorting effects of outliers, all three sets of changes in beta were winsorised at the 0.01 level at both tails[23].

To determine whether changes in regular, upside, and downside beta were of statistical significance, parametric Student t-tests were performed testing the alternative hypothesis that regular and winsorised $\Delta\beta_{i,\bar{t}}, \Delta\beta^{+}_{i,\bar{t}}$, and $\Delta\beta^{-}_{i,\bar{t}}$ scores are significantly greater than zero in the population of severe security breaches. Given the sample size, near-normal distribution could reasonably be assumed, and Student t-tests appeared justified. Graphic analysis of changes in regular, upside, and downside betas, however, revealed that the distributions present heavy tails. Non-parametric testing, which does not require a particular probability distribution, is thus expedient to confirm t-test results [1, 30, 228, 231]. Conducting both parametric and non-parametric statistical tests is in line with similar empirical studies in information security economics (see [30, 231]). Hence, non-parametric one-sided Wilcoxon signed-rank test scores were calculated additionally[24], testing the alternative hypothesis that the one-sample Hodges-Lehmann-type pseudo-median is greater than zero [445, 446]. All statistical tests were directional, as positive changes across all beta types were expected ex-ante (as established in Section 2.7).

3.5.2 Illustration of Beta and Dual-Beta Analysis

In order to illustrate the methodology laid out above, consider the following example.

On 01 October 2018, the PRC database recorded a severe security breach in Chegg Inc., an education technology company with a market capitalisation of $3.1bn at that time. The

[23]Results are qualitatively robust to winsorising at the 0.05 level.

[24]Other non-parametric tests could have been conducted alternatively. For instance, analysing beta changes using sign tests was considered. However, as expected proportions of positive changes in beta cannot be established unambiguously, it was decided not to use this binomial test.

company suffered from an external attack that affected more than 40m customers and filed a statement with the SEC. The incident was widely reported upon in major news outlets[25].

The analysis excluded the announcement day, as well as the two trading days immediately preceding and following the announcement day to avoid capturing volatility induced by the announcement event, following the logic of the semi-strong Efficient Market Hypothesis [108, 109]. Hence, in order to establish the pre-breach regular beta factor, 60 daily one-year betas were calculated between 27 September 2018 and 05 July 2018, and averaged to yield 0.87. Similarly, 60 daily one-year betas were calculated from 03 October 2018 to 28 December 2018 and averaged to establish a post-breach regular beta of 1.16[26]. This increase in beta by 0.29 (i.e., 33%) suggests that following the announcement of the security breach, Chegg Inc.'s systematic risk increased substantially as its stock became more volatile vis-à-vis general market movements.

Pre- and post-breach upside and downside betas are based on the same period of time. However, only trading days with non-negative — or negative, respectively — market returns were taken into account when regressing Chegg Inc.'s stock returns on the S&P 500. Chegg Inc.'s pre-breach upside and downside betas were 0.57 and 0.61, respectively. Following the severe security breach announcement, these figures increased to 0.94 and 1.00, respectively. These results for Chegg therefore suggest that in both Up and Down Markets (i.e., during periods of time featuring positive and negative market returns, respectively), Chegg Inc.'s upside and downside risks increased due to the security breach, as its stock became more volatile vis-à-vis general market movements during both bull and bear markets.

3.5.3 Analytical Procedure: Regression Analysis

To further explore the dataset, and to establish firm features that exacerbate the impact of severe security breaches on systematic regular and downside risk, further baseline regression analyses were conducted. Specifically, the following aspects which characterise a firm's information environment and might impact its susceptibility to shocks posed by security breaches were examined: announcement year, industry, firm size, and primary listing country. The announcement year is the calendar year in which a firm announced the focal security breach. Ex-ante, it was expected that the impact of security breaches on risk increases over time

[25]See, for example, `https://www.techcrunch.com/2018/09/26/chegg-resets-40-million-user-passwords-after-data-breach/`, `https://www.cnbc.com/2018/09/26/ed-tech-company-chegg-plunges-after-disclosing-data-breach.html`, and `https://www.zdnet.com/article/chegg-to-reset-passwords-for-40-million-users-after-april-2018-hack/`.

[26]Using 250 trading days to establish daily betas, the first daily pre-breach beta in the set of 60 daily pre-breach betas, for instance, was calculated using returns data between 27 September 2018 and 02 October 2017.

due to advances in media reporting and data breach notification laws. The industry was defined with respect to the *S&P Capital IQ* industry sector[27]. Differences across industries can stem from divergent regulations, the amount of media coverage an industry is subject to, and investors' assessment of security breaches' relevance for firms in the respective industry.

As noted in Section 3.5.1, the analysis approach attempted to model an 'average' market participant's decision-making process. Accordingly, firms with market capitalisations at breach announcement exceeding $10bn or $2bn were defined as large- or medium-sized firms, respectively. Primary listing country is a dummy variable, which takes the value of unity for firms with a primary listing on a US stock exchange and zero otherwise. The regression model included all the independent variables mentioned above. The dependent variables were the changes in systematic regular and downside risk.

3.6 Empirical Methodology: Credit Default Swap Spreads / Cost of Debt

In this section, the methodology to demonstrate the empirical relationship between security breaches and cost of debt in terms of credit default swap (CDS) spreads is explained. The section first covers how abnormal, or unexpected, changes in CDS spreads following security breach events were computed and assessed with regards to their statistical significance following an event study framework. Afterwards, the regression-based factor model to examine movements of CDS spreads around security breaches is introduced. The results obtained from the analytical procedures laid out below are presented in Chapter 6.

3.6.1 Analytical Procedure: Changes in CDS Spreads

The aim of Contribution **C3** was to establish whether severe security breaches in publicly listed firms are associated with increases in firms' cost of debt in terms of changes in CDS spreads. The rationale for using CDS spreads as a measure of credit risk to provide a near real-time proxy of cost of debt is explained in Section 2.8.

Credit default swaps, highly liquid credit derivative contracts quoted daily on OTC markets, provide a market-based measure of firms' default risk and hence function as a direct proxy for default spreads which are added onto risk-free rates by debt issuers, resulting in firms' effective cost of debt (see Equation 2.5 and the associated explanations in Section 2.8 for reference).

[27]Communication Services, Consumer Discretionary, Financials, Health Care, Industrials, Information Technology, or Other.

For each severe security breach in the initial sample ($n = 202$, see Section 3.2) available daily 5-year CDS Mid closing prices (i.e., CDS spreads) were retrieved from Intercontinental Exchange Credit Market Analysis (ICE CMA) via *S&P Capital IQ*. ICE CMA CDS Mid spreads are quarterly par spreads[28] based on Bid and Ask quotes that are directly sourced from executable transactions processed by multiple independent traders (i.e., buy-side market participants). Comparing major providers of CDS prices, Mayordomo et al. [450] found that quotes provided by ICE CMA lead the price discovery process, which makes the database particularly suitable for event study-like analyses [451].

Five-year CDS spreads are generally considered the most liquidly traded CDS contracts featuring the lowest bid-ask spreads [295, 452, 453], and were hence most commonly used in previous empirical studies of (changes in) CDS spreads [285, 290, 299, 310]. In line with these studies, both analytical approaches in Contribution **C3** used CDS contracts with 5-year maturities.

Out of 202 initial events in the PRC-based dataset used throughout Contribution **C2**'s analysis of cost of equity, CDS spreads were only available for 75 security breach events (56 reference entities). This lack of observations is mainly due to the fact that CDS credit derivatives are still relatively new financial instruments (see [288, 290]), which were hence not traded at the time of some firms' security breaches. For the same reason, the factor analysis only took into account 73 security events (55 reference entities) due to the absence of CDS spreads for sufficient amounts of time prior to the breach events.

There are two major ways in which the impact of events on CDS spreads is typically studied in empirical literature — factor models and matching-portfolio models. Using matching-portfolios, an analytical framework similar to standard event studies and difference-in-difference quasi experiment methods, has been the most commonly applied approach in previous studies [451], and there are some advantages of using said approach. Using factor models can result in biased samples overrepresenting firms with lower CDS spreads, whereas matching-portfolio models are less subject to such sample bias [451]. Additionally, factor models necessitate the availability of CDS and other financial data for longer time periods to establish unexpected or abnormal behaviour of CDS spreads relative to the chosen variables, which can result in even fewer events in the ultimately usable sample and hence reduces generalisability. However, factor models offer the advantage of effectively controlling for other potential influences on changes in CDS spread during the considered period of time. They thereby allow for singling out the impact of breaches on CDS premia and conducting

[28]ICE CMA CDS quarterly par spreads indicate, in basis points, the annual premium on the secured notional amount due to the seller of the CDS per annum, paid quarterly by the buyer of the insurance. Par spreads are coupons that set the NPV of the two CDS contract legs, the fixed premium payments one and the default payment one, at inception to zero.

predictive analyses. Accordingly, both a matching-portfolio approach following Bertoni and Lugo [451], Hull et al. [290], and Norden and Weber [310] as well as a factor model approach similar to Shivakumar et al. [295], Yang et al. [454], Du [308], Jenkins et al. [455], and Callen et al. [288] were used in this present study to assess changes in CDS spreads.

For both approaches, daily changes in 5-year CDS spreads ($\Delta CDS_{i,t}$) pertaining to firm i on two consecutive trading days (t and $t-1$) were defined in absolute terms as follows.

$$\Delta CDS_{i,t} = CDS_{i,t} - CDS_{i,t-1} \tag{3.11}$$

The **matching-portfolio approach** study set-up is akin to that of standard event study methodology following MacKinlay [228], Brown and Warner [226, 227], Banz [224], and Benninga [225] laid out in Section 3.4. Event studies are the most common methodology to quantify market reactions to information security news items [182, 229–231]. The process of calculating daily and cumulative abnormal changes in CDS prices via adjusting actual changes in CDS spreads by changes in the spreads of a relevant index or a portfolio of comparable companies is similar to computing abnormal stock market returns as per the market-adjusted model in the traditional event study framework[29].

A firm's $\Delta CDS_{i,t}$ is subject to both idiosyncratic changes in the underlying firm's default risk and changes in macroeconomic credit risk [451]. This study investigates the effect of severe security breaches on firms' CDS spreads. Accordingly, any market-wide effects had to be adjusted for in order to isolate the firm-specific component of spread changes. In order to do so, portfolios (or baskets) of CDS contracts that matched fundamental characteristics of the focal firms' CDS, but did not experience the same event, were constructed as a proxy for the level of CDS spread change expected under regular, or non-event-presence, circumstances. Two different matching-portfolio techniques were used in this study to construct benchmark portfolios to adjust actual, or observed, breached firms' CDS spreads controlling for market-wide and industry-wide macroeconomic effects, respectively.

First, in order to control for economy-wide effects inducing changes in CDS spreads, a rating-matched method — the most common matching-portfolio technique in similar previous studies [451] — was applied, using cross-industry index portfolios based on firms' credit rating. Specifically, for each security breach event firm in the sample, the prevailing credit rating at or around the time of the respective security breach announcement was established based on information published by *Moody's Investors Service*, *S&P Global Ratings*,

[29] Generally, considering the traditional event study framework, even though the market-adjusted model is a simplification of the market model assuming similar systematic risk for all securities ($\beta_i = 1$, $\alpha_i = 0$), differences between the market model and the market-adjusted model can reasonably be expected to be economically and empirically insignificant [226, 227, 456, 457].

Fitch Ratings, *Rating and Investment Information Inc.*, and company websites. For each event observation, the appropriate CDS index was then chosen on the basis of the breached firm's country of incorporation and whether the underlying firm's debt was of investment or non-investment grade at the time of the breach[30]. Applying a rating-matched method that distinguishes only between investment grade and non-investment grade classes, as opposed to using individual letter rating codes, is thereby in line with previous studies [460]. *Markit iTraxx Europe Main*, *CDX North America Investment Grade*, *CDX North America High Yield*, and *Asia Japan* indices were used to proxy CDS market returns for firms incorporated in Europe, the United States, and Japan, respectively. Markit's iTraxx Europe Main and CDX North American Investment Grade indices are thereby considered the two main corporate credit derivative indices globally [309]. Both indices are equally-weighted and reference the 125 most liquidly traded European and North American investment grade firms, respectively. The iTraxx Asia Japan index features 50 equally-weighted Japanese entities' CDS contracts. All indices are rolled over, updated, and re-launched as new series every six months, including or excluding underlying constituents as appropriate. The frequent re-launch and the changes in underlying constituents thereby also affect the pricing level every six months. Accordingly, in the analysis only the most recent, or highest, series available for the required dates were used. For each firm and event in the sample of 75 severe security breaches, daily spread changes in the relevant CDS index ($\Delta I_{i,t}$) were calculated on an absolute basis as follows.

$$\Delta I_{i,t} = CDSI_{i,t} - CDSI_{i,t-1} \tag{3.12}$$

Here, $CDSI$ is the relevant CDS index price on two consecutive trading days t and $t-1$. Table J.1 in Appendix J summarises the CDS indices used to proxy market-wide rating-matched CDS spread changes around the time of a breach for each affected firms.

Second, observed CDS spread changes were adjusted using industry-matched portfolios. Specifically, portfolios of competitors' CDS contracts were created for each event firm by looking up all available 5-year CDS contracts of competitors named by the breached firm, competitors named by competitors, and firms operating primarily within the same industry[31]. For each competitor CDS contract, daily changes in spreads were calculated in the same way as those calculated for event firms above (see Equation 3.11). For each security breach

[30]Note that although different credit rating agencies were used to determine the rating of different issuers at their respective breach event date, credit ratings are similar across rating agencies as they are subject to similar analysis processes and incentives (see e.g., [458, 459]).

[31]Industry definitions, competitors named by the focal company and competitors named by competitors were based on the respective *S&P Capital IQ* data fields.

event, the daily CDS spread changes of all competitors (C) to the focal firm (i) were then averaged to yield one daily spread change value ($\Delta C_{i,t}$)[32]. See Table J.1 in Appendix J for the number of CDS contracts used to proxy firm-specific industry-matched CDS portfolio baskets for each event and Table K.1 in Appendix K for a detailed list of all CDS contracts used per event-firm combination.

Abnormal CDS spread changes, which were analysed with regards to their statistical significance, were computed as

$$ASC_{i,t} = \Delta CDS_{i,t} - \Delta I_{i,t} \tag{3.13}$$

and

$$ASC_{i,t} = \Delta CDS_{i,t} - \Delta C_{i,t} \tag{3.14}$$

Here, $ASC_{i,t}$ is the daily abnormal CDS spread change, and $\Delta CDS_{i,t}$, $\Delta I_{i,t}$ and $\Delta C_{i,t}$ are the daily changes in CDS spreads for the focal breached firm, the CDS index, and the averaged basket of competitors, respectively. In line with the logic presented by Jenkins et al. [455] and Lok and Richardson [461], the study used "raw" or absolute CDS spread changes as opposed to relative or percental ones.

For further analyses, daily $ASC_{i,t}$ were aggregated over several multi-day event windows centred on the (adjusted) security breach announcement date. In line with the observation that information leakage can occur prior to public announcements of security breaches (see [442, 443]), the Efficient Market Hypothesis [108, 109], and prior related studies (see e.g., [295, 451]), cumulative abnormal CDS spread event windows covered up to three t_{-3} trading days prior to the (adjusted) security breach announcement date and up to two t_2 trading days after it. Even though it would have been interesting to analyse the long-term effect of security breaches on cost of debt, event windows were kept short to mitigate the presence of any confounding events (see [442]). Analysing short event windows around the (adjusted) security breach announcement date implies the assumption that there is no major information leakage prior to the announcement.

As common in the statistical analysis of abnormal changes in CDS spreads, the statistical significance of cumulative abnormal CDS spread changes ($CASC_{[-3,1]}$, $CASC_{[-2,0]}$, $CASC_{[-2,2]}$, and $CASC_{[-1,0]}$) following information security breaches was examined using

[32]Note that this method of analysis implicitly assumes that security breaches are indeed idiosyncratic to the focal firm in the time period under consideration and do not affect the portfolio of matched firms. Whilst some studies have demonstrated that negative firm value spillovers to other non-breached firms can occur [30, 179], it is reasonable to assume that given both the short event windows considered in this study and the broad portfolios used to establish expected, or normal, CDS spread movements, any spillover effect that could potentially distort other firms' CDS spreads and hence $\Delta C_{i,t}$ is negligible.

one-sided t-tests, sign tests, and Wilcoxon signed-rank tests (see [325,451]). Non-parametric tests are thereby expected to be substantially more powerful than the t-test [451]. The analytical procedure for the three sets of tests was similar to the one presented in Section 3.4.1. Specifically, in the present analysis, both t-tests and Wilcoxon signed-rank tests were one-sided directional tests following the initial hypothesis that severe security breaches are associated with *increases* in CDS spreads. In line with the random walk hypothesis [109], sign test expected proportions were set at 0.5, resembling an equal chance of obtaining positive or negative abnormal changes in CDS spreads in a given period of time.

In line with previous similar studies (e.g., [295]), all sets of cumulative market- and competitor-adjusted CDS spread changes were winsorised at the top and bottom one-percentile of their distributions to mitigate potentially distorting effects of outliers.

The **factor model study set-up** used regression models to investigate whether severe security breach announcements are associated with short-term changes in CDS spreads, controlling for other variables that can influence such price changes. The methodology was based on the ones applied in related studies [295,453,454], following the notion that changes in CDS spreads are associated with CDS spread volatility, equity returns, equity volatility, general market returns, implied market volatility, and risk-neutral borrowing rates.

The present study followed a quasi-experiment methodology, in which for each severe security breach event ($n = 73$, treatment group), a subsample featuring all available competitor firms that did not suffer from a security breach during the same period of time (control group) was generated. The control group firms in the subsamples for each event are the same ones as those used in the matching-portfolio analysis approach above, i.e., competitors named by the breached firm, competitors named by competitors, and firms operating primarily within the same industry[33]. Accordingly, in addition to the 73 security events (55 reference entities) of interest, the overall regression-based analysis sample additionally consisted of 1,651 control observations of 546 competitor firms that did not suffer from a security breach in the respective period of time. The 1,724 complete observations were used to estimate the following regression:

[33]Note that the number of matched control group firms for each breach event differs from the number of five-year CDS contracts used for the same respective event in the matching-portfolio approach. This is due to the fact that one unique firm might be associated with multiple credit default swaps resulting, for instance, from mergers and acquisitions and other corporate restructuring activities.

$$\begin{aligned}\Delta CDS\ Spread = \beta_0 &+ \beta_1 Breached\ Firm + \beta_2 \sigma(CDS\ spread) \\ &+ \beta_3 \sigma(Stock\ Return) + \beta_4 Residual\ Stock\ Return \\ &+ \beta_5 Market\ Return + \beta_6 Risk\text{-}Neutral\ Rate \\ &+ \beta_7 Implied\ Market\ Volatility + Year\text{-}fixed\ effects + \epsilon\end{aligned} \tag{3.15}$$

The dependent variable $\Delta CDS\,Spread$ is defined as the cumulative absolute daily change in CDS spreads in firm i, calculated as per 3.11, over multiple event windows, spanning the time periods t_{-2} or t_{-1} to t_1 or t_2 relative to the (adjusted) breach announcement date[34]. In line with the logic presented by Jenkins et al. [455] and Lok and Richardson [461], the dependent variable was defined in absolute ("raw") terms as opposed to relative or percental ones.

For each security breach event, a matched basket of non-breached competitors was created, and $\Delta CDS\ Spread$ for such firms was estimated during the same respective event windows. The main independent variable of interest is *Breached Firm*, which is a binary variable assuming the value of 1 for event observations, i.e., those related to firms that experienced a security breach, and zero for matched competitor observations[35]. To control for other variables potentially associated with changes in CDS spreads (see [288, 295, 453, 462, 463]), the following firm- and event-specific independent variables were included additionally. Intrinsic daily CDS spread volatility ($\sigma(CDS\ spread)$) and daily stock return volatility ($\sigma(Stock\ Return)$) were defined as the standard deviations of CDS spreads and stock returns during the time frame $[t_{-80}, t_{-6}]$ relative to the (adjusted) breach announcement day. *Residual Stock Return* is the contemporaneous (i.e., during the same period of time during which the dependent variable was measured) market-adjusted stock return. Residual stock returns were orthogonalised with respect to all other independent variables to mitigate potential multi-collinearity concerns. *Market Return* is the contemporaneous cumulative country-specific index return (based on the respective firm's country of incorporation). *Risk-Neutral Rate* is the contemporaneous cumulative proportional change in the country-specific risk-free rate, defined as either the three-month country-/region-specific

[34]Note that these are the same event windows as those considered in the matching-portfolio analysis approach above (as well as those analysed in Contribution **C1**). The nature of cumulative daily absolute changes implies that the period of time under consideration includes the spread data point on the day prior to the start of the specified "changes event window". For instance, the $[-2, 1]$ cumulative absolute daily change in CDS spreads in firm i is equal to the difference between the five-year CDS spread three days prior to the (adjusted) security breach announcement date and the five-year CDS spread on the trading day after that day (i.e., $CDS_{i,1} - CDS_{i,-3}$).

[35]See Table K.1 in Appendix K indicating the matched observations (i.e., firms) used for each of the 73 event observation.

interbank lending rate or the short-term government debt rate. *Implied Market Volatility* is the contemporaneous cumulative proportional change in the relevant implied volatility index. *Year-fixed effects* is a set of dummy variables indicating the year in which a breach occurred and event-group and control-group firms were observed. The year-fixed effects control for characteristics not explicitly included as a separate variable that are constant on firm-level, but varying over time [464]. ϵ is the residual term with an expected mean of zero.

Following Cameron et al. [465], White [466], and Petersen [467], regressors' t-statistics were computed based on heteroskedasticity-consistent standard errors adjusted for clustering at firm level to account for potential violations of homoskedasticity assumptions, as some firms feature multiple observations in the dataset[36]. In line with previous similar studies (e.g., [295]), all non-indicator variables, including cumulative CDS spread changes, were winsorised at the top and bottom one-percentile of their distributions to mitigate potentially distorting effects of outliers. As an additional robustness check, firm-fixed effects were included in a further set of OLS regression-based models by including dummy variables for each firm.

All data to construct the regression-based models was downloaded via *S&P Capital IQ*, apart from three-month Canadian Treasury Bill Yields which were downloaded from the Bank of Canada website. Due to data availability issues some country-specific data points were used to proxy the returns and rates for more than one country. For instance, for companies headquartered in Jersey, the UK's FTSE 100 Index was used. Unavailable interbank lending rates or treasury bills were substituted with World Bank Discount Rates. Equally, the United States CBOE S&P 500 Volatility Index (VIX), one of the oldest and most widely followed volatility indices globally, was used when similar country-specific indices were not available. Please see Tables L.1 and L.2 in Appendix L for details on the particular indices, risk-free rates, and implied market volatility indices used for each country and observation in the sample.

3.7 Empirical Methodology: Insider Trading Abnormal Returns / Information Asymmetries

In this section, the methodology to assess the empirical association between severe information security breaches and information asymmetry in terms of insider trading abnormal

[36]Heteroskedasticity-consistent standard errors adjusted for clustering at firm level were computed using package *multiwaycov* V1.2.3 in *R*. Standard errors were not adjusted for potential autocorrelation assumption violations given the absence of first-order autocorrelation as indicated by Durbin-Watson test statistics [468, 469].

returns is delineated. The section thereby covers how the sample of insider transaction filings around security breaches was constructed and how cumulative abnormal returns ($CARs$) following such insider trades were computed. Afterwards, the regression-based model to examine the effect of security breaches on $CARs$ is explained. The results obtained from the empirical research design laid out below are presented in Chapter 7.

3.7.1 Analytical Procedure: Changes in Insider Trading Abnormal Returns

Contribution **C4** aimed to establish to what extent severe security breaches in publicly listed firms are empirically associated with increases in information asymmetries as proxied by insider trading abnormal returns. As delineated in Section 2.9.3, (cumulative) abnormal returns following upon insider trading filings provide a suitable proxy for long-term analyses of changes in ex-ante information asymmetries.

In order to compare insider trading abnormal returns in breached firms before and after a security breach, a sample based on *2iQ Research*'s 2005–2019 database of 8,118,700 individual insider transaction filings was constructed. First, only transactions that pertained to firms in the sample of severe security breaches ($n = 202$, see Section 3.2) were included. Then, in line with previous studies on insider trading and information asymmetries (see [390, 391, 394, 396, 399, 404, 441]), all non-regular equity purchase and sale transactions were omitted from the sample, and remaining transactions were aggregated on a daily level. Specifically, transaction filings arising from the award of stock-based remuneration; announcements of plans to conduct transactions; transfers of shares to spouses and other family members; and OTC, private, forced (such as margin calls), and automated transactions (such as Rule 10b5-1 transactions) were excluded as they are not based on insiders' perceptions of stock mispricings and hence do not inherently carry informational value. All transaction filings pertaining to derivatives and non-ordinary equity trades such as options, bonds, and share rights were also omitted from the sample. Additionally, all transactions related to potentially confounding events, i.e., corporate restructurings, mergers, reverse mergers, spin-offs, and IPOs were filtered out.

The remaining insider transaction filings were then net-aggregated on a daily basis by adding the number of shares purchased and subtracting the number of shares sold on each filing day[37] for every firm in the sample. Days on which the firm-level aggregate number of shares traded by insiders was greater than zero, or less than zero, were designated Net Buy, or Net Sell, transactions, respectively. Net-neutral observations (i.e., the aggregate number

[37] A filing day is the day on which a transaction was reported to the relevant market authority.

of shares bought and sold by insiders in a given firm on a given day was zero) were omitted.

Subsequently, for each security breach, the daily net-aggregated insider transactions in breached firms during the 24-months period centred on security breaches were selected. Filings during the ten days surrounding a particular security breach itself were thereby excluded to avoid unduly biasing information asymmetry figures by measuring uncertainty immediately around the security breach announcement. Security breach events were dropped from the analysis if the insider trading sample did not feature at least one trade before *and* after a particular breach.

In efficient markets, rational stock market participants are expected to swiftly adjust their expectations of future cash flows, and hence pricing, as a response to insider trading news. The greater the ex-ante information asymmetries between outside investors and corporate insiders are, the greater the informational content of aggregated insider trades is, and in turn, the more substantial the abnormal returns following the filing of insider trades become.

For all daily net-aggregated insider trades, short-term three-day cumulative abnormal returns were calculated in an event study framework following similar previous studies on insider trading abnormal returns proxying for information asymmetries [390, 391, 394, 396, 470, 471]. The abnormal return calculations were thereby done in a similar manner to the analysis conducted in the context of Contribution **C1**, as explained in Section 3.4 above.

Specifically, for every net-aggregated insider trade, expected returns were established using one-factorial Sharpe [117] single-index models grounded in the CAPM [118–121], which are commonly used in similar information security economics studies [1, 2, 231, 233]. Individual insider-traded stocks' returns were regressed on the respective countries' broad indices[38] over estimation windows of 250 trading days (i.e., one year)[39].

Insider trade filing-specific coefficients were estimated via ordinary least square regressions. Daily abnormal returns were calculated as per Equation 3.2. Cumulative abnormal returns between t_0 and t_2 ($CAR\ [0, 2]$), comprising market reactions on the (adjusted) filing day and the following two trading days, were computed following Equation 3.3[40].

To examine whether information asymmetries as proxied by insider trading abnormal returns increase after security breaches, the following regression-based models were set up

[38] A list of the indices used to proxy country-specific market portfolios is provided in Table E.1 in Appendix E.

[39] If a particular filing day was a non-trading day, the filing date was adjusted to reflect the closest following trading day. Regression windows started at trading day t_{-2} and ended at trading day t_{-251} relative to (adjusted) filing dates. The abnormal returns analysis was based on filing dates as these mark the dates on which insider trades become public knowledge and market participants could act upon the new information accordingly.

[40] In order to ensure results' robustness to different abnormal return specifications, cumulative abnormal returns were also computed over multiple other time periods, i.e., $CARs$ $[-1, 0]$, $[-1, 1]$, $[-1, 2]$, $[0, 0]$, and $[0, 1]$.

controlling for other firm characteristics that are known to affect firms' information asymmetries[41]. The cross-sectional regression model is thereby similar to Brochet [470], who assessed changes in the information content of insider trades before and after the introduction of the Sarbanes-Oxley Act, and Bhabra and Hossain [471], who analysed levels of insider trades' informational value after extreme market downturns. All financial data to compute control variables was downloaded from *S&P Capital IQ*. The full explanatory model is defined as follows:

$$\begin{aligned} CAR\,[0,2] = \beta_0 &+ \beta_1 Post\ Breach + \beta_2 Firm\ Size + \beta_3 R\&D + \beta_4 Loss \\ &+ \beta_5 Book\text{-}to\text{-}Market + \beta_6 Reporting\ Lag + \beta_7 Trade\ Size \\ &+ \beta_8 Post\ Breach\ X\ Trade\ Size + \beta_9 Insider\ Rank \\ &+ Firm\text{-}fixed\ effects + Year\text{-}fixed\ effects + \epsilon \end{aligned} \tag{3.16}$$

The dependent variable is the insider trade-induced three-day cumulative abnormal return $CAR\ [0,2]$[42]. The main variable of interest, *Post Breach*, is a dummy variable that takes the value of 0 for aggregate insider trades filed in the 12 months before a security breach, and 1 for aggregate insider trades recorded in the 12 months after said security breach. Based on the main hypothesis **C4-H1** (see Section 2.9), positive regression coefficients were expected for Net Buy transactions, and negative regression coefficients for Net Sales transactions, indicating that on average post-breach insider transactions induce greater abnormal returns. Net Buy transactions are generally expected to convey greater informational value and therefore generate greater abnormal returns [391, 396, 410]. Accordingly, in **C4-H1a**, it was hypothesised that the effect of security breaches on information asymmetries is more reflected by Net Buy transactions, resulting in more significant coefficient estimates.

On firm level, the model controls for *Firm Size*, *R&D*, *Loss*, and *Book-to-Market*. *Firm Size* is the natural logarithm of the underlying firm's market capitalisation on the filing day in millions of Euro. Firm size is a typical indicator of information asymmetries. Previous research demonstrated that firm size is negatively associated with information asymmetries as larger firms publish information more frequently and attract greater analyst and media coverage [372,396,397,408,472]. The regression coefficients for *Firm Size* are hence expected

[41] A potential alternative to estimating regression-based models would have been to estimate simple within-subject differences between average firm-level information asymmetries as proxied by insider trading abnormal returns before and after a security breach. However, given the lengthy periods of time considering up to 24 months, it is pertinent to control explicitly for other variables that are known to influence information asymmetries and insider trading abnormal returns. A within-subject study design could also have led to reduced sample sizes.

[42] $CAR\ [0,2]$ is the time period commonly used in previous literature (see e.g., [470]). In order to ensure results' robustness to different abnormal return specifications, models were also run with $CARs\ [-1,0]$, $[-1,1]$, $[-1,2]$, $[0,0]$, and $[0,1]$ as the dependent variable.

to be negative for purchases and positive for sales.

R&D is a dummy variable taking the value of one for firms that reported greater-than-zero research and development expenses for the fiscal year in which the trade was filed, and zero otherwise. Aboody and Lev [408] found greater information asymmetries in terms of insider trading abnormal returns in firms with R&D-intensive strategies. *Loss* is another dummy variable taking the value of one for firms that reported a negative net income for the fiscal year in which the trade was filed, and zero otherwise. Subpar financial performance can be associated with more positive abnormal returns in the case of net purchases and more negative abnormal returns in the case of net sales [470].

The *Book-to-Market* ratio is defined as the book value per share in Euro divided by the closing price in Euro on the filing date. A firm's book-to-market ratio is a classical proxy for information asymmetry and indicates whether a firm's stock can be classified as value or growth stock, whereby insiders' purchases are concentrated more in value stocks (i.e., those with a low book-to-market ratio) and vice versa [372, 383, 396, 470, 471, 473]. Insider purchases in firms with higher book-to-market ratios are expected to signal undervaluation and should hence be associated with positive regression coefficients. Insider sales in such firms are expected to signal overvaluation and should hence be associated with negative regression coefficients.

On aggregate transaction level, the model controls for *Reporting Lag*, *Trade Size*, and *Insider Rank*. *Reporting Lag* is the natural logarithm of one plus the difference between the insider trade and the filing of said trade in days ($log\,[1 + (filingdate - tradingdate)]$). If multiple insider transactions were filed on the same day, the reporting lag is based on the maximum filing delay. An increase in reporting lag is considered to be associated with more substantial profits but also greater increases in information leakage prior to the filing and hence lower information content of the eventual filing [405, 470, 471, 474].

If the net-aggregated number of shares on the filing date was positive, *Trade Size* was defined as the natural logarithm of said net-aggregated number. If the net-aggregated number of shares on a given filing date was negative, *Trade Size* was defined as the natural logarithm of the absolute net-aggregated figure multiplied by minus one. The informational value of insider transactions was expected to increase in line with the size of the transaction [384, 391, 471], resulting in positive regression coefficients for Net Buy transactions and negative ones for Net Sell transactions. *Post Breach X Trade Size* is the interaction term of the two variables indicating the potential impact of *Trade Size* for post-breach insider filings. It was thereby assumed that larger trades carry greater informational value following a security breach.

Insider Rank is a dummy variable taking the value of one if at least one of the insiders

who traded on a given filing day was a "Top 20" insider (i.e., a member of the upper level management or executive board/committee). Prior research established that executives' roles inside the firm determine their ability to access information and hence the information content of their insider trades [471, 475–477]. Trades by "Top 20" insiders were expected to be associated with greater information content and hence more positive abnormal returns following insider purchases and more negative abnormal returns following insider sales.

Firm-fixed effects is a set of dummy variables indicating the firm in which a net-aggregated insider trade was filed. The firm-fixed effects control for characteristics time invariant within firms, such as industry and country of incorporation. *Year-fixed effects* is a set of dummy variables indicating the year in which an insider trade was filed and insider trading abnormal returns were measured. The year-fixed effects control for characteristics not explicitly included as separate variables that are constant on firm-level, but varying over time [464]. ϵ is the residual term with an expected mean of zero. All non-categorical variables were winsorised at the 0.05 level at both tails of their respective distributions to mitigate the potential effect of outliers.

As a robustness check, and to verify that the hypothesised empirical relationship holds over multiple periods of time, a subset of the main sample, which contained insider trades during the 12 months before and after a security breach, was created by selecting only trades in the 18-months period centred on security breaches, again excluding the immediate ten days surrounding the respective security breach. Concluding the process of filtering, aggregating, and omitting transactions with missing data points led to final samples of 2,409 (830 Net Buy and 1,579 Net Sell) and 3,256 (1,168 Net Buy and 2,088 Net Sell) aggregated insider trades for the ± 9 and ± 12 months' time frames, respectively. These insider trades related to up to 129 security breach events[43].

After establishing all variables and samples for two time periods, the two final datasets were split into, and the regression model specified above was run separately for, Net Buy and Net Sell transactions as most variables were ex-ante expected to have diametrically opposed effects on $CARs\ [0, 2]$ following purchases and sales, respectively. OLS regression standard errors were clustered on firm level and adjusted to be heteroskedasticity-consistent based on Cameron et al. [465], White [466], and Petersen [467][44] due to repeated firm-level observations.

[43] See Table 7.2 for details on how many security breach events the particular subsamples are based on.

[44] Heteroskedasticity-consistent standard errors adjusted for clustering at firm level were computed using package *multiwaycov* V1.2.3 in *R*.

Chapter 4
Security Investment Costs: Firm Value

An analysis of abnormal stock returns following investments in Cyber Essentials and ISO/IEC 27001

This chapter is based on the WEIS 2019 publication [1] (**MP1**) (adjusted to conduce to the more general dissertation narrative). It gives rise to Contribution **C1** by demonstrating the extent to which investments in security certificates can have underlying / consequential negative economic consequences (in the case of the ISO/IEC 27001 certificate) or positive economic consequences and secondary benefits (in the case of the Cyber Essentials certificate).

4.1 Overview

In this chapter the results of the empirical analysis of stock market reactions following security certifications are presented. Specifically, we discuss the results of three statistical tests pertaining to the research question whether cumulative abnormal returns following security standards certifications are significantly different from zero. Subsequently, firm and market characteristics potentially affecting the direction and magnitude of abnormal returns are examined. The sampling process and methodology applied to obtain the results discussed herein are presented in Sections 3.1 and 3.4.

The three statistical tests' results for both security standards and both outlier treatment approaches are presented in the following order: Cyber Essentials (Plus) untransformed cumulative abnormal returns, Cyber Essentials (Plus) winsorised cumulative abnormal returns, ISO/IEC 27001 untransformed cumulative abnormal returns, and ISO/IEC 27001 winsorised cumulative abnormal returns. In each table, two-sided t-test, one-sided sign test, and two-

sided Wilcoxon signed-rank test results are shown for four event windows, which cover the event day, as well as up to three trading days prior to and up to two trading days following a certification date. Within each table, from left to right, the columns indicate the event window under consideration, the number of certification events in the respective event window, the sample mean and median, and test statistics and associated p-values for t-tests, sign tests, and Wilcoxon signed-rank tests. Statistical significance is accepted at p-values below 0.05; statistical trends at p-values of less than 0.1 are also discussed.

In Section 4.4, the results obtained from the regression analysis are presented. Abnormal returns in the event window $CAR[-2, 2]$ are defined as the outcome variable across all models. Each regression model includes different sets of regressors. Model (1) examines timing, industry group, certification type, and firm size. Model (2) also includes the country in which a firm is headquartered. Model (3) additionally considers stock liquidity and growth potential. In the full model (4), EBITDA growth is also added. For each model and regressor, the estimated coefficients are shown, with standard errors in parentheses.

145 Cyber Essentials events between 2014 and 2018, and 76 ISO/IEC 27001 certifications between 2001 and 2018, were analysed. Overall, the award of Cyber Essentials (Plus) certificates is found to be associated with economically and statistically significant *positive* abnormal returns. In contrast, ISO/IEC 27001 certificate awards are coherently associated with economically and statistically significant *negative* abnormal returns. The regression analysis demonstrates limited positive relations between abnormal returns and time, Cyber Essentials certificates, firm size, and firms headquartered in Nigeria, respectively. The models also reveal limited negative associations between abnormal returns and Financial Services, Industrials, and IT firms, respectively. These results show that well-intended information security investments may have unexpected underlying / consequential economic repercussions.

4.2 Empirical Results Cyber Essentials (Plus)

Table 4.1 presents the analysis of untransformed abnormal returns following Cyber Essentials (Plus) certifications. The t-test results almost unanimously show that CAR scores are statistically significantly different from zero with positive mean CARs across all four event windows. For instance, the mean $CAR[-3, 2]$ is 1.06% ($n = 145, p = 0.012$), which is also economically significant. Only the mean CAR of the four-day event window $[-2, 1]$ suggests merely a statistical trend of CARs being statistically significantly different from zero. It can also be observed that mean CARs become more positive over time, i.e., the longer event windows $[-3, 2]$ and $[-2, 2]$ are associated with greater abnormal returns than the event

Table 4.1: Cyber Essentials (Plus) — Untransformed

Event window	n	M	Mdn	t	p_t	$PosRat$	p_{Sign}	$Pseudo\ Mdn$	$p_{Wilcoxon}$
$[-3, 0]$	145	0.751	0.091	2.138	0.034^{**}	0.545	0.159	0.257	0.152
$[-3, 2]$	145	1.056	0.201	2.545	0.012^{**}	0.545	0.159	0.351	0.110
$[-2, 1]$	145	0.591	0.087	1.938	0.055^{*}	0.531	0.253	0.141	0.439
$[-2, 2]$	145	0.749	0.346	2.084	0.039^{**}	0.545	0.159	0.262	0.224

Note: *** $p < 0.01$; ** $p < 0.05$; * $p < 0.1$; n = sample size; M = sample mean; Mdn = sample median; t = test statistics t-test; p_t = p-value t-test; $PosRat$ = positive ratio sign test; p_{Sign} = p-value sign test; $PseudoMdn$ = pseudo-median Wilcoxon test; $p_{Wilcoxon}$ = p-value Wilcoxon test. Mean and median cumulative abnormal returns are in percentage. t-tests and Wilcoxon signed-rank tests are two-sided, testing the alternative hypothesis that the population mean is different from zero and that the population pseudo-median is different from zero, respectively. Sign tests are one-sided, testing the alternative hypothesis that the positive ratio is greater than chance (0.5).

Table 4.2: Cyber Essentials (Plus) — Winsorised

Event window	n	M	Mdn	t	p_t	$PosRat$	p_{Sign}	$Pseudo\ Mdn$	$p_{Wilcoxon}$
$[-3, 0]$	145	0.298	0.091	2.334	0.021^{**}	0.545	0.159	0.337	0.023^{**}
$[-3, 2]$	145	0.304	0.201	2.023	0.045^{**}	0.545	0.159	0.312	0.046^{**}
$[-2, 1]$	145	0.063	0.087	0.499	0.619	0.531	0.253	-0.007	0.976
$[-2, 2]$	145	0.198	0.346	1.285	0.201	0.545	0.159	0.146	0.128

Note: See Table 4.1.

windows $[-3, 0]$ and $[-2, 1]$ are.

The non-parametric tests do not support initial indications as provided by the parametric t-test. In absolute terms, all sign tests' positive ratios are greater than 50%, which means that more than half of all Cyber Essentials (Plus) certification events are associated with positive cumulative abnormal returns. However, no sign test provides sufficient evidence to reject the null hypothesis that the actual proportion of positive CARs statistically significantly exceeds chance. Interestingly, there is almost no change in positive ratios and associated p-values across the event windows, indicating that abnormal returns in a given firm are coherently positive or negative over time.

Similarly, non-parametric Wilcoxon signed-rank tests on untransformed values do not provide further evidence for the presence of positive abnormal returns following Cyber Essentials (Plus) certifications. For untransformed CARs, the two-sided test results indicate that CARs are not statistically significantly different from zero during the four considered event windows, although all (pseudo-)medians are substantially positive.

The analysis of winsorised abnormal returns following Cyber Essentials (Plus) certifi-

cations is shown in Table 4.2. Mean and median winsorised CARs are positive across all event windows. For a given event window time frame, winsorised mean CARs tend to be lower than untransformed mean CARs, which can suggest the presence of outliers featuring strong positive market reactions subsequent to security certification events. Notwithstanding the lower magnitude of winsorised mean CARs scores, their t-tests corroborate initial observations for untransformed scores. After reducing the impact of outliers, the four- and six-day event windows starting at $[-3]$ continue to exhibit statistically significant positive mean CARs. For instance, the winsorised mean $CAR[-3, 2]$ is 0.30% ($n = 145, p = 0.045$). The aforementioned observation that abnormal returns increase over time also holds in the case of winsorised scores.

As winsorising does not alter the number of positive event-specific CARs, the positive ratio and sign test results remain unchanged relative to the untransformed figures.

The non-parametric Wilcoxon signed-rank test for winsorised CARs provides evidence in support of the hypothesis that certification events are followed by significant abnormal returns. Following the outlier treatment, CARs in the event windows $[-3, 0]$ and $[-3, 2]$ appear to be statistically significantly different from zero and positive. For instance, the winsorised median $CAR[-3, 2]$ is 0.20% ($n = 145, p = 0.046$).

4.3 Empirical Results ISO/IEC 27001

Test results concerning abnormal returns following ISO 27001 certifications presented in Tables 4.3 and 4.4 provide a more unified picture as both untransformed and winsorised CARs are significantly negative.

Table 4.3 displays test results for untransformed abnormal returns. All mean CARs are negative across all four event windows. t-test results indicate that mean CARs in all but one event window are statistically significantly different from zero. For instance, the mean $CAR[-3, 2]$ is -1.17% ($n = 74, p = 0.02$), which is also economically material. Mean CARs following ISO 27001 certifications become more negative with increasing event window lengths, i.e., mean CARs in event windows $[-3, 2]$ and $[-2, 2]$ are more negative than the CARs in event windows $[-3, 0]$ and $[-2, 1]$, respectively.

Sign test results confirm the t-test results. Negative ratios range from 0.67 $[-2, 1]$ to 0.70 $[-3, 2]$, with p-values indicating that in every considered event window, negative CARs are statistically significantly more likely to occur than by mere chance.

Median CARs are also negative for all event windows and range between -0.37% $[-3, 0]$ and -0.92% $[-3, 2]$. Wilcoxon signed-rank test results for untransformed CAR scores indicate that the true median CAR in the event windows $[-3, 2]$ is indeed different

Table 4.3: ISO/IEC 27001 — Untransformed

Event window	n	M	Mdn	t	p_t	$NegRat$	p_{Sign}	$Pseudo\ Mdn$	$p_{Wilcoxon}$
$[-3,0]$	76	-0.875	-0.374	-2.077	0.041^{**}	0.671	0.002^{***}	-0.643	0.056^{*}
$[-3,2]$	74	-1.165	-0.921	-2.324	0.023^{**}	0.703	$<0.001^{***}$	-0.901	0.020^{**}
$[-2,1]$	75	-0.449	-0.440	-1.562	0.123	0.667	0.003^{***}	-0.377	0.186
$[-2,2]$	75	-0.795	-0.704	-2.064	0.043^{**}	0.693	0.001^{***}	-0.640	0.054^{*}

Note: *** $p<0.01$; ** $p<0.05$; * $p<0.1$; n = sample size; M = sample mean; Mdn = sample median; t = test statistics t-test; p_t = p-value t-test; $NegRat$ = negative ratio sign test; p_{Sign} = p-value sign test; $PseudoMdn$ = pseudo-median Wilcoxon test; $p_{Wilcoxon}$ = p-value Wilcoxon test.
Mean and median cumulative abnormal returns are in percentage. t-tests and Wilcoxon signed-rank tests are two-sided, testing the alternative hypothesis that the population mean is different from zero and that the population pseudo-median is different from zero, respectively. Sign tests are one-sided, testing the alternative hypothesis that the negative ratio is greater than chance (0.5). Different sample sizes across event windows are due to missing financial data points.

Table 4.4: ISO/IEC 27001 — Winsorised

Event window	n	M	Mdn	t	p_t	$NegRat$	p_{Sign}	$Pseudo\ Mdn$	$p_{Wilcoxon}$
$[-3,0]$	76	-0.687	-0.374	-3.069	0.003^{***}	0.671	0.002^{***}	-0.748	0.012^{**}
$[-3,2]$	74	-0.935	-0.921	-3.475	0.001^{***}	0.703	$<0.001^{***}$	-1.043	0.002^{***}
$[-2,1]$	75	-0.438	-0.440	-2.385	0.020^{**}	0.667	0.003^{***}	-0.517	0.066^{*}
$[-2,2]$	75	-0.653	-0.704	-2.857	0.006^{***}	0.693	0.001^{***}	-0.678	0.011^{**}

Note: See Table 4.3.

from zero ($n = 74, p = 0.02$). For the event windows $[-3,0]$ and $[-2,2]$, we find strong statistical trends suggesting that the true median CAR is materially negative in these event windows as well.

Statistical test results for winsorised abnormal returns following ISO 27001 certifications are shown in Table 4.4 and strongly support inferences drawn from the prior analysis of untransformed abnormal returns.

All winsorised mean CARs are negative across event windows. In each event window, winsorised mean CARs are slightly less negative than untransformed CARs. t-tests on winsorised CARs uniformly support the notion that the population mean is negative and statistically significantly different from zero. For instance, the winsorised mean $CAR[-3,2]$ is -1.17% ($n = 74, p = 0.001$), which is also economically significant. Again, negative abnormal returns become more substantial over time.

Mitigating outliers through winsorising does not alter the number of negative event-specific CARs, hence the negative ratio and sign test results remain unchanged relative to

the untransformed figures.

Winsorised median CAR scores also remain unchanged relative to the untransformed figures and are hence negative across all event windows. After mitigating the effect of outliers, the Wilcoxon sign-ranked test results indicate that winsorised CAR scores reveal an even greater tendency to be statistically significantly different from zero than their untransformed counterparts. Specifically, the true median CARs in the event windows $[-3, 0]$, $[-3, 2]$, and $[-2, 2]$ appear to be statistically significantly different from zero. For the event window $[-2, 1]$, a strong statistical trend suggesting that the true median CAR is materially negative in this event window can be found as well.

4.4 Empirical Results Regression Analysis

Table 4.5 shows descriptive statistics of the combined sample used in the combined regression analysis. Note that the sample size decreases when including EBITDA growth due to data unavailability. Banks do not report EBITDA as their business model renders the figure meaningless.

Table 4.6 presents the regression analysis results. Only Model (1) is overall-significant as per the F-Test of Overall Significance. The model reveals a statistically significant and negative association between abnormal returns in the event window $CAR[-2, 2]$ and the Financial Services, Industrials, and IT industries. There is also limited statistical evidence suggesting a positive relation between the abnormal returns and time, Cyber Essentials certificates, and firm size. In Models (2) to (4), the empirical effect of the three aforementioned industries persists, although less pronounced. In these models, the negative effect of firms primarily operating in the IT industry merely becomes a statistical trend. The same holds for Model (4) and the Financial Services industry's effect. Surprisingly, none of the countries apart from Nigeria (in Models (2) and (3)) display a statistically significant effect on abnormal returns. According to these models, firms headquartered in Nigeria are associated with more positive abnormal returns following investments in security standards.

4.5 Summary of Empirical Results

Overall, the evidence regarding Cyber Essentials (Plus) certifications is mixed. t-tests of untransformed CARs suggest the presence of positive abnormal returns significantly different from zero across all event windows. However, these results are not supported by non-parametric tests. When mitigating the influence of outliers, significant and positive ab-

Table 4.5: Combined Regression Sample

Model		Model 1			Model 2			Model 3			Model 4	
Variable	Min	Mean	Max	Min	Mean	Max	Min	Mean	Max	Min	Mean	Max
Number of observations		219.00			219.00			217.00			198.00	
CAR [-2, 2]	-13.32	0.25	27.76	-13.32	0.25	27.76	-13.32	0.24	27.76	-13.32	0.27	27.76
Time (days)	0.00	1,110.20	1,613.00	0.00	1,110.20	1,613.00	0.00	1,108.00	1,611.00	20.00	1,114.00	1,611.00
Commercial and Prof. Services (n)		50.00			50.00			50.00			50.00	
Consumer Services (n)		7.00			7.00			6.00			6.00	
Distributors (n)		6.00			6.00			6.00			6.00	
Financial services (n)		31.00			31.00			31.00			13.00	
Healthcare (n)		2.00			2.00			2.00			2.00	
Industrials (n)		46.00			46.00			46.00			46.00	
IT (n)		48.00			48.00			47.00			47.00	
Real Estate (n)		9.00			9.00			9.00			9.00	
Transportation (n)		12.00			12.00			12.00			12.00	
Utilities (n)		8.00			8.00			8.00			7.00	
Cyber Essentials (n)		145.00			145.00			144.00			130.00	
Log (total assets USDm)	1.97	8.58	14.70	1.97	8.58	14.70	1.97	8.58	14.70	1.97	8.42	13.90
Log (avg. daily volume)							-5.16	0.10	5.04	-5.16	0.04	4.14
Log (avg. PBV)							-1.11	1.15	3.22	-0.41	1.26	3.22
Positive EBITDA Growth (n)											97.00	
Australia (n)					16.00			16.00			15.00	
Austria (n)					1.00			1.00			1.00	
China (n)					2.00			2.00			2.00	
Denmark (n)					1.00			1.00			1.00	
France (n)					1.00			1.00			1.00	
Germany (n)					1.00			1.00			1.00	
Hong Kong (n)					1.00			1.00			1.00	
India (n)					9.00			9.00			9.00	
Ireland (n)					4.00			4.00			4.00	
Israel (n)					1.00			1.00			1.00	
Japan (n)					14.00			14.00			14.00	
Lebanon (n)					1.00			1.00				
Netherlands (n)					1.00			1.00			1.00	
Nigeria (n)					1.00			1.00				
New Zealand (n)					2.00			2.00			2.00	
Oman (n)					1.00			1.00				
Poland (n)					1.00			1.00			1.00	
Qatar (n)					1.00			1.00			1.00	
Singapore (n)					1.00			1.00			1.00	
South Africa (n)					2.00			2.00			1.00	
Switzerland (n)					2.00			2.00			2.00	
UAE (n)					1.00			1.00			1.00	
UK (n)					143.00			142.00			128.00	
USA (n)					9.00			8.00			8.00	
Vietnam (n)					2.00			2.00			2.00	

normal returns appear to be present in the event windows $[-3, 0]$ and $[-3, 2]$ as per t-tests and Wilcoxon signed-rank tests. This leads us to consider, in this case, that the main hypothesis **C1-H1** — the completion of security standards is associated with significant abnormal returns — is partially supported. We deduce that Cyber Essentials (Plus) certifications can be associated with significant positive abnormal returns.

In contrast, strong evidence suggesting a negative association between ISO/IEC 27001 certifications and short-term stock market returns was found. Negative untransformed and winsorised mean CARs can be observed across all event windows. Together with t-tests suggesting statistically significant deviance from zero, this demonstrates that, on average, ISO/IEC 27001 awards are followed by negative market reactions. Both non-parametric tests corroborate these t-test results substantially. Consequently, we consider, in this case, that the main hypothesis **C1-H1** — the completion of security standards is associated with

Table 4.6: Regression Results

	Dependent variable:			
	CAR[-2,2]			
	(1)	(2)	(3)	(4)
Time	0.001*	0.001	0.001	0.001
	(0.001)	(0.001)	(0.001)	(0.001)
Industry dummies included Selected coefficients shown	Yes	Yes	Yes	Yes
Financial services	−2.359**	−2.718***	−2.894**	−2.845*
	(0.937)	(1.036)	(1.195)	(1.492)
Industrials	−2.414***	−2.656***	−2.727***	−2.791***
	(0.812)	(0.851)	(0.923)	(0.972)
IT	−1.978**	−1.958*	−2.025*	−1.963*
	(0.882)	(0.994)	(1.049)	(1.093)
Certification Type	1.149*	4.377	4.314	4.353
	(0.650)	(3.241)	(3.302)	(3.434)
Firm Size	0.267*	0.189	0.408	0.432
	(0.145)	(0.166)	(0.295)	(0.329)
Stock Liquidity			−0.272	−0.307
			(0.318)	(0.352)
Growth Potential			0.161	0.102
			(0.454)	(0.514)
EBITDA Growth				−0.090
				(0.663)
Country dummies included Selected coefficient shown	No	Yes	Yes	Yes
Nigeria		8.693**	9.476**	
		(4.264)	(4.425)	
Constant	−2.864	−2.616	−4.256	−4.155
	(1.803)	(2.088)	(2.918)	(3.193)
Observations	219	219	217	198
R^2	0.103	0.166	0.170	0.160
Adjusted R^2	0.051	0.001	-0.007	-0.027
Residual Std. Error	3.964 (df = 206)	4.068 (df = 182)	4.101 (df = 178)	4.226 (df = 161)
F Statistic	1.978** (df = 12; 206)	1.006 (df = 36; 182)	0.962 (df = 38; 178)	0.854 (df = 36; 161)
Note:				*p<0.1; **p<0.05; ***p<0.01

significant abnormal returns — is fully supported.

In summary, it was shown that completed investments in information assurance standards elicit statistically significant stock market reactions. Surprisingly, the results for the two types of certificates point in diametrically opposed directions: the completion of Cyber Essentials (Plus) certifications can increase a firm's share price, whereas becoming compliant with the ISO/IEC 27001 standard is likely to diminish a firm's market value. The subsequent regression analysis only contributes a limited amount of additional insights to the counter-intuitive results. We saw that Financial Services, Industrials, and IT firms are negatively associated with abnormal returns, whilst Cyber Essentials certificates, time, and firm size have a positive impact on $CARs[-2, 2]$.

4.6 Discussion of Empirical Results

Previous empirical literature on the economics of information security investments, particularly with regards to indirect underlying / consequential costs, is scarce. The literature review revealed an absence of a consensus as to whether security investments create value as indicated by significant positive abnormal returns, which can be perceived as an additional benefit or negative cost c as per the ENBIS equation (Equation 2.2). Moreover, the literature features antithetic evidence suggesting that security investments might indeed be associated with negative future cash flows and thus negative abnormal returns, which can be interpreted as additional indirect underlying / consequential costs c.

In both cases, investors, analysts, and other market participants can be expected to alter their future cash flow expectations following investments in holistic security standards. If these economic agents expect future economic benefits stemming from the investment to be greater than the associated costs, share prices will increase following successful security certifications. On the other hand, if stock market participants anticipate initial and follow-on costs associated with the investment to be greater than future benefits, share prices will decrease following successful security certifications. Accordingly, in **C1-H1** it was hypothesised that the certification of a firm with an information security standard is associated with significant abnormal returns. To investigate the hypothesis, data on two different types of information security standards was gathered and an event study to examine the immediate impact of a security investment on stock prices and thereby the respective firm's market value was conducted. The empirical results and their implications for firms, executives, and the overarching research question are discussed below.

4.6.1 Cyber Essentials (Plus) Certificates

The empirical analysis showed that investing in Cyber Essentials (Plus) certifications results in average abnormal returns of up to 1.06% over the six-day period starting three trading days prior to the certification date and ending two trading days afterwards. Positive abnormal returns following these certifications are statistically significant according to parametric tests. Winsorised abnormal returns corroborate the finding and also indicate statistical significance according to the non-parametric Wilcoxon signed-rank test. Market reactions following Cyber Essentials investments are thus in line with previous studies [124, 231, 240]. The effect size of untransformed abnormal CARs, particularly in the $[-3, 0]$ and $[-2, 2]$ event windows, is similar to the 0.72% presented in Deane et al.'s [238] study of security certifications.

The significant positive abnormal returns following Cyber Essentials certifications indicate that investors expect economic benefits of the investment to outweigh associated costs (i.e., more positive cash flows). Potential reasons for stock market participants' positive re-valuation of firms may include their belief that becoming Cyber Essentials-compliant can reduce financial penalties and losses associated with data breaches, enhance reputation, elicit greater revenues, and facilitate business process improvements.

It is worth reiterating that compliance with the Cyber Essentials programme is necessary to bid for "government contracts which involve handling of sensitive and personal information and provision of certain technical products and services" [478]. It is plausible to assume that investors pay particular attention to the fact that only certified firms are allowed to bid for particular UK Government contracts, and that there is thus a direct positive cash flow component to becoming Cyber Essentials-compliant. This conjecture is echoed by the finding that security investments with commercial exploitability are associated with greater abnormal returns than those exclusively intended for security improvements [124, 239]. In fact, the types of industries predominantly present in the sample (Human Resources and Employment Services and Aerospace and Defence) suggest that firms aspiring to comply with the Cyber Essentials programme mainly do so to become or remain UK Government suppliers. The sample might hence be biased due to this self-selection process.

Firms operating within the Human Resources and Employment Services industry by definition handle personal information, whilst those active in the Aerospace and Defence industry naturally provide technical products and services of high relevance to government customers. Whilst it is difficult to link changes in financial performance directly to security standards certifications — as such strategic decisions do not take place in isolation and cannot be analysed ceteris paribus — it is unambiguous that absence of Cyber Essentials certifications prohibits firms from bidding for certain government contracts, and some firms

might find it difficult to operate profitably without winning these contracts.

Consider, for example, the British company *G4S plc*. The company, inter alia, provides prison and airport security services, and engages in other high-level security tasks for the UK Government. As a public services outsourcing company, it is highly dependent on government contracts (see [479]). Being compliant with a security standard required to bid for government contracts is a necessity for such firms, which are thus highly incentivised to pursue the respective certification. Once a firm such as G4S becomes (re-)certified according to Cyber Essentials standards, it can expect greater future revenues relative to hypothetical future revenues without being compliant to the information security standard. Market participants are likely to expect that additional revenues generated by firms known to be government suppliers/contractors exceed associated security certificate investment expenses. It can thus reasonably be assumed that investors in turn highly appreciate firms pursuing Cyber Essentials certifications, and hence acknowledge security standards certifications with greater share prices, resulting in positive abnormal returns. Anecdotally, this can indeed be observed for *G4S plc*. The firm's Cyber Essentials certification events, elicit an average $CAR[-2, 1]$ of 2.08%.

Separately, the Cyber Essentials (Plus) sample constructed for this study does not differentiate between new certifications, initial subsidiary certifications, follow-on certifications of the entire organisation, and mandatory later re-certifications. Positive mean abnormal returns found in the sample might thus stem from the fact that market participants deem follow-on company-level certifications and re-certifications economically reasonable as they allow for a (continuous) ability to bid for UK Government contracts without necessitating substantial new investments in IT controls.

Havakhor et al. [270] recently presented evidence that can partially explain the value-creative effect of information security investments. The authors showed that disclosing security investments leads to a reduction in information asymmetries and cost of capital. Such a reduction in investor uncertainty and perceived risk can in turn result in greater share prices.

Market participants expecting firms to generate additional positive cash flows subsequent to a Cyber Essentials (Plus) certification expect the reputational gain, the revenue stemming from UK Government contracts, and reductions in ALE to outweigh expenses associated with pursuing the certificate. Put differently, stock investors outside the firm expect the investment-specific ENBIS (see Equation 2.2) to be greater than zero. As delineated in Chapter 2, stakeholder value-maximising security executives using ENBIS to assess different investment opportunities are interested in gaining a holistic understanding of costs and benefits associated with an investment. For such executives, the market value creation in

terms of positive CARs constitutes an additional benefit beyond the reduction in Annual Loss Expectancy. Such a benefit constitutes a negative cost element ($c_{fincosts_{CAR}} < 0$) within the c_{CE} vector of the ENBIS equation on Cyber Essentials (Plus) certificates. Accordingly, in light of the security and firm value benefits, from a security executive's perspective, ceteris paribus, it makes economic sense to invest in becoming Cyber Essentials (Plus) certified.

4.6.2 ISO/IEC 27001

In contrast, the ISO/IEC 27001 analysis revealed that the certification is coherently associated with significant negative abnormal returns of up to -1.16% over the six-day period starting three trading days prior to the certification date and ending two trading days afterwards. Negative mean abnormal returns persist across all event windows and are statistically significant according to both parametric and non-parametric tests in both outlier treatment approaches. These statistically significant negative returns following ISO/IEC 27001 certifications suggest that market participants expect negative returns on investment as the security standard entails substantial initial and follow-on costs which are not exceeded by savings stemming from reduced security breach probabilities and costs. Anticipating follow-on costs to be greater than those associated with the Cyber Essentials programme is reasonable. Whilst both security standards function as platforms for further investments, the ISO/IEC 27001 standard features 114 controls, which may necessitate greater costs to maintain and advance existing systems and processes.

Multiple additional potential reasons for the negative stock market reaction can be identified. First, Jeong et al. [241] argued that the absence of positive market reactions following security investments can be due to market participants already expecting firms to invest in security. Investors do not consider news of substantial investments a differentiator, but, rather, a pure cost factor born out of necessity. Accordingly, an investment in ISO/IEC 27001 controls might merely be deemed a compulsory exercise, and it might constitute a negative surprise to investors that a particular firm has not already made necessary investments before.

Another likely explanation is that market participants do not appreciate the necessity to invest in information security generally. Szubartowicz and Schryen [196] contend that prior to a security breach, market participants might consider security investments not worth pursuing and therefore react negatively upon intended and completed security investments. Therefore, investors might consider an ISO/IEC 27001 certification — a major long-term investment endeavour — unnecessary for companies which have not yet experienced severe security incidents.

Another important difference to note vis-à-vis the analysis of the Cyber Essentials programme is that the sampling process of ISO/IEC 27001 events centred on newly issued certificates, whereas the Cyber Essentials (Plus) sample contains multiple re-certificates. Negative market reactions should therefore be viewed as associated with the substantial initial investment. Accordingly, investors might perceive later re-certifications more positively, as these convey a positive signalling effect regarding the firm's information security capabilities without necessitating substantial new investments in IT controls.

As these study's results contradict those established by an earlier study on market value implications of ISO/IEC 27001 completions [238], it can be conjectured that there are significant regional differences in market participants' assessments of security investments. Deane et al. [238] demonstrated statistically significant positive abnormal returns on the US stock market following ISO/IEC 27001 certifications, but noted the importance of replicating their study of abnormal returns following ISO/IEC 27001 awards with other security certifications and on other stock exchanges. This divergence between the results presented above and Deane et al. [238] might be caused by different levels of market sophistication and liquidity. The US stock market can be considered fairly developed and efficient, whereas, for instance, emerging and developing markets included in this present study might behave differently[1]. This notion is in line with the finding that, in the United States, stock market participants reacted with even greater positive abnormal returns to security investments after the introduction of the Sarbanes-Oxley Act, a major accounting and transparency reform, than before the legislation was introduced [124]. Moreover, differences between the results obtained for the Cyber Essentials programme relative to the ISO/IEC 27001 standard can be due to asset liquidity. FTSE 350 stocks can be considered highly liquid, whereas markets in developing countries may be too illiquid to react to security investments in a similar manner.

Notwithstanding potential explanations, these results are interesting and potentially discouraging for a security executive contemplating an investment in ISO/IEC 27001 controls. Market participants expecting firms to generate additional negative cash flows subsequent to an ISO/IEC 27001 certification expect the expenses associated with pursuing and maintaining the certificate to outweigh the reputational gain, improved processes, and reductions in ALE. Put differently, stock investors outside the firm expect the investment-specific ENBIS (see Equation 2.2) to be less than zero. As delineated in Chapter 2, stakeholder value-maximising security executives using ENBIS to assess different investment opportunities are interested in gaining a holistic understanding of costs and benefits associated with

[1]Given that the sample used in this study features security certifications in, for instance, India, Vietnam and Nigeria, the differences in abnormal returns may be due to lower levels of market regulation and sophistication compared to the US market.

an investment. For such executives, the market value destruction in terms of negative CARs constitutes an additional cost element ($c_{fincosts_{CAR}} > 0$) within the c_{ISO} vector of the ENBIS equation on ISO/IEC 27001 certifications. The study's results neither implicate that (investors believe that) ISO/IEC 27001 security controls are ineffective, nor do they necessarily convey information about long-term firm value implications. However, the negative short-term abnormal returns render pursuing investments in ISO/IEC 27001 certificates less economically reasonable.

4.6.3 Factors Influencing Security Certification Abnormal Returns

The regression analysis only yields limited additional insights into the contradictory results. Only one regression model can be considered overall-significant. Regression Models (2) to (4) are not statistically significant overall due to the introduction of country-dummy variables. Country-level (and to a limited extend also industry-level) subsamples are too small to yield substantial insights.

Across all models, a persistent negative association between Financial Services, Industrials, and IT industries and abnormal returns following security standard certifications can be found. In the overall-significant model, time and firm size appear to have a small positive impact on abnormal returns. Additionally, in Models (2) and (3), out of all countries, only Nigeria is significantly and positively associated with post-certification abnormal returns.

The persistent negative association between the three industries and post-certification abnormal returns merits particular discussion. From the regression results, it appears as though investors in Financial Services, Industrials, and IT firms do not expect reductions in breach costs ($ALE_0 - ALE_s$) to outweigh initial and follow-on investment expenses (c). In the case of Financial Services and Industrials firms, investors might deem security standards investments to be ineffective and to require substantial follow-on expenses given the complexity of the firms' operations, their large attack surface, and the value of their data. In the case of the IT industry, market participants might consider firms inherently experienced in information security matters and do thus not appreciate (seemingly redundant) investments in the protection of information confidentiality, integrity, and availability.

The positive impact of time on abnormal returns elicited by investments in security certificates suggests that over the course of time, market participants react more favourably to firms pursuing security standards investments. This might be due to investors, for instance, by increasing media coverage, becoming more knowledgeable about security threats, associated costs, and the necessity to mitigate them.

The positive coefficient for the variable certification type corroborates earlier findings

discussed above. Cyber Essentials (Plus) certifications tend to be associated with more positive abnormal returns than ISO/IEC 27001 certifications.

Firm size's positive impact on abnormal returns somewhat contradicts previous findings by Deane et al. [238], and may be due to market participants expecting economic benefits from security standards to exceed associated costs at larger firms. The positive impact of size might also stem from reduced ex-ante information asymmetries. Larger firms tend to be followed more extensively by analysts and the media [396, 397, 408, 472], and it is thus likely that larger firms' security certification news are disseminated more efficiently.

Nigeria's positive association with abnormal returns can potentially be interpreted as an indicator that external certifications carry an even higher relevance in less-mature markets than they do in highly-developed markets.

4.6.4 Limitations

Despite the thorough set up of the study and using parametric and non-parametric statistical analyses and outlier treatment methods to analyse two types of security investments, there remain some limitations.

First, the major constraints stem from the methodology used (see [229]). Event studies can only reliably generate evidence of *short-term* stock market reactions. Given that security investments may only prove appropriate in the long-run, the immediate nature of market reactions might not prove a helpful metric to inform decision-making processes. Moreover, given the constant stream of new information to be factored in by stock market participants, there is an abundance of confounding events that may affect organisations' market value but are impossible to control for.

Additionally, abnormal returns upon the listing of compliance may only represent a proportion of the overall stock market reaction associated with investments in security standards. It is indeed likely that the notification of a decision to pursue an investment, the announcement of having completed an investment, and the actual official listing in a database all generate discrete changes in a firm's market value. Accordingly, a negative market reaction on the certification day may merely offset an initial positive overreaction on the day of the announcement that a security certificate investment will be pursued. Relatedly, abnormal returns across studies are difficult to compare given that other studies (e.g., [231, 238]) centre their event studies on announcement dates, whereas in this study actual certification dates were utilised.

Finally, abnormal returns following Cyber Essentials (Plus) and ISO/IEC 27001 certifications are difficult to compare on a like-for-like basis as, for example, the sample of Cyber

Essentials events contains re-certifications, whereas the ISO/IEC 27001 analysis focuses on newly issued certificates.

4.7 Conclusion on Security Investment-Induced Firm Value Implications

This chapter provides novel empirical evidence on underlying / consequential costs and benefits associated with information security investments.

Analysing 145 Cyber Essentials and 76 ISO/IEC 27001 certification events revealed that Cyber Essentials (Plus) certifications are systematically associated with significant positive market reactions, whereas the international sample of ISO/IEC 27001 certifications reveals that becoming ISO/IEC 27001-compliant elicits significant negative abnormal stock returns. The results imply that market participants expect increased discounted net cash flows to follow from Cyber Essentials certifications and diminished discounted net cash flows as a consequence of ISO/IEC 27001 investments. Put simply, this study provides insights into how financial market participants perceive firms' security investment activities. There are, however, extensive implications and major consequences stemming from these empirical results.

As delineated in Chapters 1 and 2, stakeholder value-maximising security executives inherently aspire to, and are due to their fiduciary duty also legally obligated to, increase their firms' share prices [17, 18, 76]. Using ENBIS as a framework to assess investment opportunities as to their economic suitability, such executives need to be aware of all potential costs ($c > 0$) and secondary benefits ($c < 0$) associated with investments. The occurrence of significant abnormal returns provides corporate decision makers with an indication as to how market participants perceive this type of security investment. It is in the best personal and professional interest of a rational executive to factor such potential costs and benefits into the investment decision-making process. If a security investment generates negative underlying / consequential costs (i.e., positive economic benefits) in the form of increased equity value ($c_{fincosts_{CAR}} < 0$), a decision to pursue the respective investment becomes more economically reasonable, and vice versa[2]. Consequently, the results of the investigation above can inform and influence organisational security budget allocation.

By extension, the described non-obvious losses and gains in share prices also pertain to individual investors (inside and outside the organisation), and holistically also to society at

[2]If a security investment generates positive underlying / consequential costs (i.e., negative economic benefits) in the form of reduced equity value ($c_{fincosts_{CAR}} > 0$), a decision to pursue the respective investment becomes less economically reasonable.

large (e.g., due to institutional investors such as insurances holding equity of firms investing in information security).

Given that the majority of British security executives predominantly base their information security investment decisions on the need to protect customer data and business continuity, as opposed to economic considerations of improved efficiency and reduced costs [133,134], this study is particularly insightful for British security officers. Specifically, they might be encouraged to incorporate the potential firm value-creative benefits into their ENBIS considerations to mitigate their investment dilemmas.

UK-based policy makers might also find this study's results helpful to reduce negative externalities caused to society by companies not securing their data. Firms which can externalise breach costs to society are not incentivised to invest in attack deterrence and hence invest more in damage control than in breach avoidance [125]. Policy makers such as the NCSC might want to encourage more companies to actively manage cyber risk by investing in Cyber Essentials (Plus) controls. Demonstrating positive equity value implications ($c_{fincosts_{CAR}} < 0$) in addition to reduced breach probability and costs (ALE_s) might support such endeavours.

For security executives contemplating investments in ISO/IEC 27001 certificates, the purpose of this study is not to discourage them from doing so, despite demonstrating the existence of negative stock market reactions following completed certifications in the sample. The Information Security Management Systems standard is comprehensive and guided by security experts and academics. Such holistic improvements of information security are supposed to reduce future breach probability and costs [238, 243]. The empirical findings should rather be perceived as an encouragement to companies to improve their security communication processes, for instance, by informing investors about the advantages of the certification for their firms. Moreover, given the additional cost element ($c_{fincosts_{CAR}}$), firms investing in ISO/IEC 27001 certificates should pay particular attention to actively managing initial and follow-on costs associated with the certification.

Amongst multiple other negative economic implications, a stock price decrease following ISO/IEC 27001 certifications suggests a reduction in the value of treasury shares and hence the value of an internal financing instrument. This implies an increase in financing costs due to the necessity to obtain alternative sources of capital to maintain a set level of available capital. Obtaining additional capital leads to increased financing costs. The same logic applies vice versa for Cyber Essentials (Plus) certificates that elicit positive stock market reactions. The additional cost of investing in ISO/IEC 27001, and secondary benefit of investing in Cyber Essentials (Plus), should be recognised as elements $c_{fincosts_{CAR}} > 0$ and $c_{fincosts_{CAR}} < 0$ in ENBIS calculations.

Chapter 5
Security Breach Costs:
Cost of Equity

An analysis of changes in asymmetric beta following information security breaches

This chapter is based on the WEIS 2020 publication [2] (**MP2**) (adjusted to conduce to the more general dissertation narrative). It provides Contribution **C2**, the provision of novel empirical evidence on security breach-induced underlying and consequential costs in the form of increases in regular, upside, and downside beta that indicate rises in cost of equity.

5.1 Overview

The aim of this study was to establish whether severe security breaches are associated with an increase in firms' cost of equity by elevating systematic risk, and whether systematic risk is affected differently in bearish and bullish markets. To this end, three hypotheses as outlined in Section 2.7 were tested, conjecturing positive associations between security breaches and changes in systematic risk. Analysing a US-centric sample of 202 severe security breaches between 2005 and 2019 revealed that severe security breaches are associated with significantly positive increases of systematic risk and systematic downside risk in terms of regular and downside beta, respectively, which contribute to increases in cost of equity. Given the absence of similar effects for systematic upside risk in terms of upside beta, the analysis also demonstrated the unsymmetrical nature of security breaches' effect on systematic risk. The implications of these findings and their relevance for firms' cost of capital are also discussed in this chapter. Cost of equity is an underlying or consequential cost factor particularly prone to be overlooked in economic assessments of information security investments.

In this chapter, all relevant empirical results are presented. Based on the methodology presented in Section 3.5, changes in systematic risk induced by severe security breaches in publicly listed companies were determined in terms of differences in regular beta, upside beta, and downside beta. This chapter demonstrates the empirical results obtained by the analysis and provides a discussion as to the relevance and implications of the empirical findings.

First, Student t-test and Wilcoxon signed-rank results for untransformed and winsorised scores of changes in regular beta, upside beta, and downside beta are examined. Tables 5.1 and 5.2 indicate, from left to right, the type of beta examined, sample size, mean, median, one-sided Student t-test statistics, and one-sided Wilcoxon signed-rank test statistics. As common, statistical significance is accepted as indicated by p-values of less than 0.05, and statistical trends as indicated by p-values of less than 0.1, respectively.

Second, it was investigated whether time, industry classification, firm size in terms of market capitalisation, or featuring a primary listing on a US stock exchange have a significant impact on changes in systematic risk. As above, the models' independent variables were considered to be statistically significant at p-values of less than 0.05, and to exhibit statistical trends at p-values of less than 0.1, respectively. The regression analysis results are presented in Section 5.5.

Overall, based on Student t-tests and Wilcoxon signed-rank test analyses, the study found support in favour of hypotheses **C2-H1** and **C2-H3**. This establishes that severe security breaches are associated with statistically significant changes in firms' systematic risk and downside risk as measured by differences in regular and downside betas. However, there is not sufficient evidence to support hypothesis **C2-H2**: upside beta is not statistically significantly affected by severe security breaches in publicly listed firms. Preliminary regression analysis results do not provide additional insights into factors influencing changes in systematic and downside risk.

5.2 Empirical Results Regular Beta

We started the analysis by posing the initial research question: *Do severe security breaches increase firms' cost of equity by elevating systematic risk?* It was hypothesised that severe security breaches in publicly listed companies are associated with positive changes in systematic risk (i.e., regular beta).

As noted earlier, regular beta is a measure of systematic risk indicating to what extent aggregate changes in the market affect individual firms' stock returns. Generally, a higher regular beta indicates that the focal asset's volatility is more correlated with index volatility, and hence more exposed to general market risk.

Table 5.1: Changes in Systematic Risk — Untransformed

Beta Type	n	M	Mdn	t	p_t	$Pseudo\ Mdn$	$p_{Wilcoxon}$
$\Delta\beta_{i,\bar{t}}$	202	0.022	0.010	1.682	0.047^{**}	0.015	0.032^{**}
$\Delta\beta^{+}_{i,\bar{t}}$	202	0.004	0.004	0.204	0.419	0.001	0.481
$\Delta\beta^{-}_{i,\bar{t}}$	202	0.031	0.009	1.720	0.043^{**}	0.015	0.089^{*}

Note: $^{***}\ p < 0.01$; $^{**}\ p < 0.05$; $^{*}\ p < 0.1$; n = sample size; M = sample mean; Mdn = sample median; t = test statistics t-test; p_t = p-value t-test; $PseudoMdn$ = pseudo-median Wilcoxon test; $p_{Wilcoxon}$ = p-value Wilcoxon test. Mean and median figures are changes in regular, upside, and downside beta, respectively. t-tests and Wilcoxon signed-rank tests are one-sided, testing the alternative hypothesis that the population mean is greater than zero and that the population pseudo-median is greater than zero, respectively.

Table 5.2: Changes in Systematic Risk — Winsorised

Beta Type	n	M	Mdn	t	p_t	$Pseudo\ Mdn$	$p_{Wilcoxon}$
$\Delta\beta_{i,\bar{t}}$	202	0.014	0.010	1.767	0.039^{**}	0.014	0.026^{**}
$\Delta\beta^{+}_{i,\bar{t}}$	202	-0.007	0.004	-0.507	0.694	-0.001	0.535
$\Delta\beta^{-}_{i,\bar{t}}$	202	0.020	0.009	1.504	0.067^{*}	0.016	0.077^{*}

Note: See Table 5.1.

Graphically (see Figure 5.1), some periodicity and volatility in beta across time can be observed. Additionally, a trend of increasing one-year regular beta figures over the relevant period of time can be seen. Specifically, approximately twenty days after the breach announcement, the average regular beta figure increases substantially.

Statistical analysis supports the initial graphical analysis of results. The top rows in Tables 5.1 and 5.2 present the analysis results for untransformed changes in regular beta and winsorised changes in regular beta, respectively. Further statistics on security breach-induced changes in regular beta per event are reported in Appendix F. Apart from winsorised upside beta scores, all mean and (pseudo-)median figures are of the expected sign. First, consider untransformed differences between pre- and post-breach betas. According to t-test results, the mean change in regular beta of 0.022 can be considered statistically significant ($n = 202, p_t = 0.047$). The non-parametric Wilcoxon signed-rank test provides further evidence in support of this statistical significance ($Mdn = 0.010, p_{Wilcoxon} = 0.032$).

For winsorised differences between pre- and post-breach betas, we find equally strong evidence that severe security breaches in public companies are followed by changes in regular beta. Both statistical tests demonstrate that the population mean and (pseudo-)median are

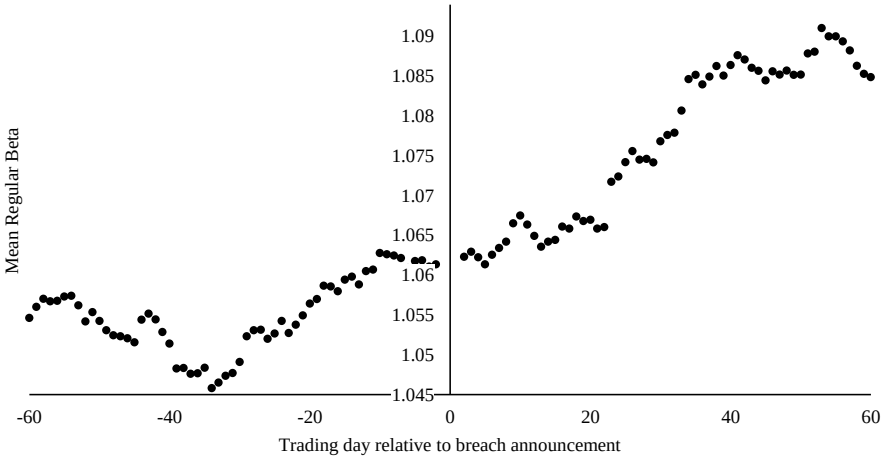


Figure 5.1: Daily Mean One-Year Regular Beta

indeed significantly greater than zero ($p_t = 0.039, p_{Wilcoxon} = 0.026$). The winsorised mean ($M = 0.014$) is slightly smaller than the non-winsorised figure ($M = 0.022$), suggesting the presence of some outliers.

Differences between pre- and post-breach regular betas are qualitatively robust to changing the aggregation time period of daily one-year betas. Specifically, across 50, 60, 65, 70, 75, and 80 aggregation days, untransformed and winsorised[1] differences in regular beta always exhibit at least a positive statistical trend ($p < 0.1$) or are statistically significantly positive ($p < 0.05$) as per t-tests and Wilcoxon signed-rank tests.

Overall, we find sufficient evidence in support of hypothesis **C2-H1**. Severe security breaches in publicly listed companies are indeed associated with an increase in systematic risk, as indicated by an increase in regular beta, leading to an increase in cost of equity.

5.3 Empirical Results Upside Beta

At the beginning of the analysis the research question of whether severe security breaches affect firms' cost of equity differently in bearish and bullish markets by affecting downside and upside risk was raised. To this end, it was hypothesised (**C2-H2** and **C2-H3**): Severe security breaches in publicly listed companies are associated with positive changes in upside risk (i.e., upside beta) and downside risk (i.e., downside beta).

As described above, upside betas signify to what extent aggregate changes in bullish

[1] As delineated in Section 3.5, winsorised scores in beta changes were winsorised at the 0.05 level at both tails. Results are also qualitatively robust to winsorising at the 0.10 level.

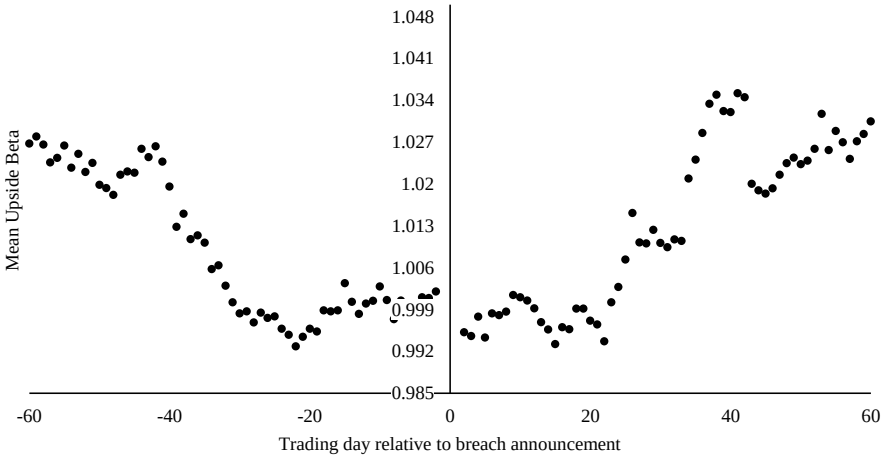


Figure 5.2: Daily Mean One-Year Upside Beta

markets (i.e., positive index returns) affect individual firms' stock returns. Generally, a greater upside beta suggests that the focal asset's volatility is more correlated with index volatility, and hence is more exposed to general market risk, during bullish periods of time.

Figure 5.2 does not reveal a clearly discernible trend with regards to increases in average upside beta over time. Instead we mainly observe periodicity and volatility in beta across time. On average, upside beta factors seem to be greater in the 60 days prior to and following a security breach announcement, but not in the immediate time period around the breach.

In the middle rows of Tables 5.1 and 5.2 the statistical analysis results for untransformed changes in upside beta and winsorised changes in upside beta are presented. Further statistics on security breach-induced changes in upside beta per event are reported in Appendix G. According to t-test results, the mean untransformed difference between pre- and post-breach upside betas of 0.004 cannot be considered meaningfully greater than zero ($n = 202, p_t = 0.419$). Similarly, Wilcoxon signed-rank test results suggest that the population median is not significantly greater than zero ($Mdn = 0.004, p_{Wilcoxon} = 0.481$).

After controlling for the effect of outliers on changes between pre- and post-breach upside betas, we find even stronger evidence that severe security breaches in publicly listed companies are not followed by changes in upside beta. Instead, the winsorised mean change is actually slightly negative at -0.007 ($n = 202, p_t = 0.694$). Additionally, the Wilcoxon signed-rank test results for winsorised differences in upside beta do also confirm that the population median cannot be expected to be greater than zero ($Mdn = 0.004, p_{Wilcoxon} = 0.535$). Considering the difference between the mean change in untransformed upside beta and the mean change in winsorised upside beta of 0.01, outliers do not seem to substantially influence the

analysis.

Differences between pre- and post-breach upside betas are qualitatively robust to changing the aggregation time period of daily one-year betas. Specifically, across 50, 60, 65, 70, 75, 80, and 90 aggregation days, untransformed and winsorised[2] differences in upside beta never exhibit positive statistical trends ($p < 0.1$) or statistical significance as per t-tests and Wilcoxon signed-rank tests.

Overall, we do not find evidence to reject the null hypothesis in connection with **C2-H2**. In contrast, the results unanimously suggest that major security breaches in publicly listed companies are not associated with an increase in systematic upside risk, as indicated by no significant increase in upside beta, not leading to an increase in cost of equity.

5.4 Empirical Results Downside Beta

It was hypothesised (**C2-H2** and **C2-H3**) that severe security breaches in publicly listed companies are associated with positive changes in upside risk (i.e., upside beta) and downside risk (i.e., downside beta). Additionally, security breach-induced changes in downside beta were expected to exceed those in upside beta.

As noted earlier, downside beta is an indicator for the extent to which general market changes in bearish markets (i.e., negative index returns) affect individual firms' stock returns. Generally, a greater downside beta indicates that the focal asset's volatility is more correlated with index volatility, and hence more exposed to general market risk, during bearish periods of time.

Figure 5.3 depicts a distinct increase of downside beta over the considered period of time. There seems to be some periodic volatility in downside beta prior to the security breach. Following a security breach announcement, downside beta on average increases, featuring a particularly pointed rise approximately 20 days subsequent to a security breach.

Indicative graphical evidence is supported by the statistical analysis. The analysis results for untransformed changes in downside beta and winsorised changes in downside beta are presented in the bottom rows of Tables 5.1 and 5.2, respectively. Further statistics on security breach-induced changes in downside beta per event are reported in Appendix H. First, consider untransformed differences between pre- and post-breach downside betas. The untransformed mean change in downside beta of 0.031 can be considered statistically significant ($n = 202, p_t = 0.043$). The median of 0.009 can be considered a statistical trend ($n = 202, p_{Wilcoxon} = 0.089$).

[2]As delineated in Section 3.5, winsorised scores in beta changes were winsorised at the 0.05 level at both tails. Results are also qualitatively robust to winsorising at the 0.10 level.

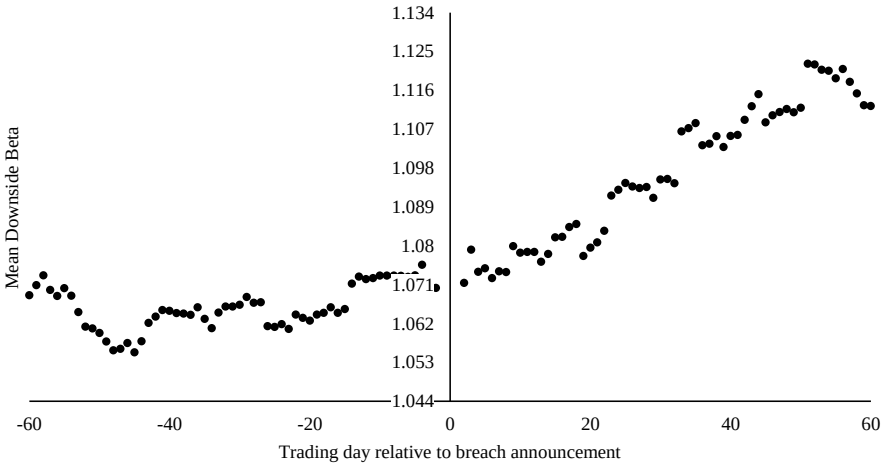


Figure 5.3: Daily Mean One-Year Upside Beta

Controlling for outliers in the analysis of downside beta changes also yields results in favour of the hypothesised relationship between security breaches and downside systematic risk. The t-test of winsorised mean changes suggests a positive statistical trend ($M = 0.020, p_t = 0.067$). The non-parametric Wilcoxon signed-rank test corroborates the t-test results. Testing median winsorised differences in downside beta shows a statistical trend indicating that the population median can be expected to be greater than zero ($p_{Wilcoxon} = 0.077$). The minor divergence between untransformed and winsorised mean changes in downside beta of 0.01 suggest the presence of some minor outliers in the sample.

Differences between pre- and post-breach downside betas are qualitatively robust to changing the aggregation time period of daily one-year betas. Specifically, across 50, 60, 65, 70, 75, and 80 aggregation days, untransformed and winsorised[3] differences in upside beta always exhibit at least positive statistical trends ($p < 0.1$) or are statistically significantly positive as per t-tests and Wilcoxon signed-rank tests.

Overall, we find some evidence in support of hypothesis **C2-H3**. Severe security breaches in publicly listed companies are associated with an increase in systematic downside risk, as evidenced by a significant increase in downside beta, causing an increase in cost of equity.

[3]As delineated in Chapter 3, winsorised scores in beta changes were winsorised at the 0.05 level at both tails. Results are also qualitatively robust to winsorising at the 0.10 level.

5.5 Empirical Results Regression Analysis

Regression analysis results are reported in Table 5.3[4]. Given the results presented in Sections 5.2–5.4, only security breach-related changes in regular and downside systematic risk were considered. Accordingly, the outcome variables across the analysed regression Models (1)–(4) are the differences between pre- and post-breach betas.

For the two types of beta factors and outlier treatment approaches, the full models including all variables specified above are presented. Specifically, Models (1) and (2) examine untransformed changes in regular beta and winsorised changes in regular beta, respectively. Models (3) and (4) consider unadjusted changes in downside beta and winsorised changes in downside beta, respectively. For each model, regressors' estimated coefficients as well as standard errors in parentheses are reported. According to the models' F-statistics, none are overall-significant and thus only yield limited insights into firm characteristics affecting the extent to which security breaches induce changes in systematic risk and systematic downside risk, respectively.

Models (1) and (2) suggest the presence of a weak negative statistical association that exists between security breach-related changes in regular beta and Industrial companies ($\beta_{Industrials,\, untransformed} = -0.110$, $se_{Industrials,\, untransformed} = 0.062$; $\beta_{Industrials,\, winsorised} = -0.066$, $se_{Industrials,\, winsorised} = 0.037$). Surprisingly, no other industry-based differences are observable.

Considering skewness-reduced regular beta differences in Model (2) also reveals a statistically significant and negative association between winsorised changes in regular beta and primary listings on US stock exchanges ($\beta_{Primary\ Listing\ US,\, winsorised} = -0.053$; $se_{Primary\ Listing\ US,\, winsorised} = 0.026$).

Analysing the effect of firm characteristics on security breach-associated changes in systematic downside risk, Models (3) and (4) suggest firm size effects. Specifically, both models indicate the presence of weak negative statistical associations between firms of high market capitalisations and shifts in systematic downside risk ($\beta_{Large\ firms,\, untransformed} = -0.085$, $se_{Large\ firms,\, untransformed} = 0.049$; $\beta_{Large\ firms,\, winsorised} = -0.070$, $se_{Large\ firms,\, winsorised} = 0.035$). In addition, both models indicate the existence of a similar trend for medium-sized firms ($\beta_{Medium\ firms,\, untransformed} = -0.088$, $se_{Medium\ firms,\, untransformed} = 0.053$; $\beta_{Medium\ firms,\, winsorised} = -0.065$, $se_{Medium\ firms,\, winsorised} = 0.038$).

[4]Note that as the dependent variable is a parameter established from a previous first stage regression, the correct critical value for the t-statistics might be biased upwards. However, this limitation does not have a material impact on the results and the ensuing analysis of implications.

Table 5.3: Changes in Systematic Risk Regression Analysis

	Dependent variable:			
	$\Delta\beta_{i,\bar{t}}$	$\Delta\beta_{i,\bar{t}}, winsorised$	$\Delta\beta^{-}_{i,\bar{t}}$	$\Delta\beta^{-}_{i,\bar{t}}, winsorised$
	(1)	(2)	(3)	(4)
Year	−0.002	−0.001	−0.008	−0.004
	(0.004)	(0.002)	(0.006)	(0.004)
Communication Services	−0.044	0.008	−0.058	−0.045
	(0.062)	(0.036)	(0.086)	(0.061)
Consumer Discretionary	−0.047	−0.006	−0.031	−0.041
	(0.057)	(0.034)	(0.079)	(0.057)
Financials	0.002	0.002	−0.004	−0.034
	(0.061)	(0.036)	(0.085)	(0.061)
Health Care	0.006	0.025	0.082	0.053
	(0.069)	(0.041)	(0.097)	(0.069)
Industrials	−0.110*	−0.066*	−0.085	−0.081
	(0.062)	(0.037)	(0.087)	(0.062)
Information Technology	−0.048	−0.004	−0.031	−0.022
	(0.058)	(0.034)	(0.081)	(0.058)
Firm Size: Large	−0.026	−0.017	−0.085*	−0.070*
	(0.036)	(0.021)	(0.049)	(0.035)
Firm Size: Medium	−0.025	−0.024	−0.088*	−0.065*
	(0.038)	(0.023)	(0.053)	(0.038)
Primary Listing US	−0.047	−0.053**	−0.004	−0.015
	(0.044)	(0.026)	(0.061)	(0.044)
Constant	4.959	2.644	15.932	8.684
	(8.383)	(4.940)	(11.658)	(8.356)
Observations	202	202	202	202
R^2	0.041	0.066	0.046	0.049
Adjusted R^2	-0.009	0.017	-0.004	-0.0003
Residual Std. Error	0.186 (df = 191)	0.109 (df = 191)	0.258 (df = 191)	0.185 (df = 191)
F Statistic	0.818 (df = 10; 191)	1.350 (df = 10; 191)	0.916 (df = 10; 191)	0.994 (df = 10; 191)

Note: *p<0.1; **p<0.05; ***p<0.01

5.6 Summary of Empirical Results

Overall, we find substantial evidence in support of the predicted empirical relationships. Severe security breaches in publicly listed firms are associated with changes in systematic risk as indicated by beta factors. However, there are differences across the three types of

beta assessed[5].

For regular betas, untransformed scores are associated with statistically significant positive changes. These results are supported by tests on winsorised figures which also indicate that changes in regular beta are statistically significantly greater than zero. This leads us to accept hypothesis **C2-H1**. Severe security breaches in publicly listed companies are indeed associated with significant positive changes in systematic risk as indicated by positive post-breach differences in regular beta.

Considering upside betas, all statistical tests unambiguously suggest that security breach-induced changes in upside beta are not statistically significantly greater than zero. We can hence not accept hypothesis **C2-H2**. Severe security breaches in publicly listed companies are not associated with significant increases in systematic positive risk as indicated by an absence of significantly positive post-breach differences in upside beta.

Results for downside betas are less unequivocal. Nevertheless, evidence in support of hypothesis **C2-H3** outweighs antithetical evidence. All four statistical tests demonstrate that there is at least a strong statistical trend towards an increase in downside betas following security breaches. The t-tests of untransformed differences in downside beta reveal the presence of a statistically significant change. Accordingly, we accept hypothesis **C2-H3**. Severe security breaches in publicly listed companies are associated with significant increases in systematic negative risk as indicated by significantly positive post-breach differences in downside beta.

The initial regression analysis does not yield substantial insights into firm characteristics aggravating or alleviating the impact of severe security breaches on systematic regular and negative risk. There are statistical trends indicating that industrial firms and those with a primary listing on a US stock exchange are less prone to increases in systematic risk following security breaches. Similarly, we found statistical trends suggesting a negative association between large to medium-sized firms and increases in systematic downside risk.

5.7 Discussion of Empirical Results

Contribution **C2** was motivated by the absence of comprehensive large-sample contemporary analyses on costs of equity implications of security breaches. Moreover, as downside beta is a more appropriate measure for financial risk [36], and investors are likely to be more wary and aware of a firm's negative news history when markets yield negative returns, the effect of security breaches on cost of equity in Up and Down Markets was considered. In this

[5]An overview of absolute and relative changes in regular, upside, and downside beta for each event is provided in Appendix I.

section, the empirical results presented above are discussed with regards to their academic and professional relevance. First, building upon the example illustrating the methodology presented in Section 3.5.2, one case study that underlines the severity of increases in systematic risk for publicly listed firms is provided. Then, we discuss changes in regular, downside, and upside beta generally. Moreover, we review the indicative regression analysis findings on factors influencing changes in beta as well as limitations to the study.

5.7.1 Illustration of Changes in Cost of Equity

In order to demonstrate the relevance of beta for a breached firm's cost of equity, consider the following, which builds upon the example of Section 3.5.2.

Chegg's pre- and post-breach betas were in line with the industry. In 2018, US Business & Consumer Services and Retail companies typically featured a beta of around 1.17 and 1.05, respectively [480]. To illustrate breach-induced changes in cost of equity, we apply Equation 3.5 using a risk-free rate (r_f), as proxied by US Treasury Bonds, of 2.68%, and an implied equity risk premium ($R_m - r_f$) of 5.96% [481].

Chegg's regression-based averaged pre-breach regular, upside, and downside betas were 0.87, 0.57, and 0.61, respectively. Following the security breach, these figures increased to 1.16, 0.94, and 1.00. Considering regular beta, Chegg's cost of equity hence increased by 1.73 percent points from 7.87% to 9.59%. The increase in downside cost of equity is even more pronounced with an increase of 2.32 percentage points from 6.36% to 8.64%. Chegg's cost of equity have thereby increased beyond industry average figures [480].

According to Chegg's Q4-2018 annual report, common equity made up 59.14% of its total capital. Hence, an increase in cost of equity by 1.73 or 2.32 percentage points would ceteris paribus result in a positive cost of capital change by 1.02 or 1.37 percentage points, respectively, which is economically significant.

5.7.2 Changes in Regular, Downside, and Upside Beta

Beta is a measure of systematic risk indicating to what extent aggregate changes in the market affect individual firms' stock returns. Generally, a higher beta indicates that the focal asset's volatility is more correlated with index volatility, and hence more exposed to general market risk. It is thereby necessary to distinguish between regular beta calculated irrespective of market returns' directions, upside beta taking into account firms' returns during Up Markets, and downside beta, the most appropriate measure of financial risk [259, 260], focusing on firms' risk exposure when markets yield negative returns.

First, we posed the question *Do severe security breaches increase firms' cost of equity by elevating systematic risk?* We found strong evidence in support of hypothesis **C2-H1**. Severe security breaches in publicly listed companies are associated with increased cost of equity as indicated by positive changes systematic risk. Second, it was explored whether severe security breaches affect firms' cost of equity differently in bearish and bullish markets by affecting downside and upside risk differently. We did not find evidence in support of hypothesis **C2-H2**. Severe security breaches in publicly listed companies are not systematically associated with increased cost of equity in a bull market as indicated by positive changes in systematic upside risk. However, there was sufficient evidence supporting hypothesis **C2-H3**, conjecturing that severe security breaches in publicly listed companies are associated with increased cost of equity in a bear market as indicated by positive changes in systematic downside risk.

Accordingly, it can be conjectured that severe security breaches induce increases in firms' cost of equity by elevating systematic risk. However, the effect on systematic risk is not of symmetrical nature. Firms' cost of equity are more severely affected when stock market indices yield negative returns.

The finding that severe security breaches are associated with significant increases in regular beta is difficult to compare with prior small-scale studies conducted by Hinz et al. [33], Cardenas et al. [34], and Nicholas-Donald et al. [35]. In this present study, an average increase in regular beta of 0.022 was established, which corresponds to an average percentage increase of 2.07%. Analysing security breaches in US companies, Nicholas-Donald et al. [35] reported a mean increase in regular beta of 0.034. However, the study only made use of a small sample of 29 events, and did not aggregate beta factors over multiple days, which, given high daily volatility [33], poses methodological issues and hinders comparison. Hinz et al. [33] correctly accounted for daily beta volatility. In their small-sample ($n = 6$) study, the authors established an unadjusted average beta increase of 0.022, which corresponds to the increase in regular beta present in the sample used in this dissertation's analysis.

The effect size of severe security breaches-induced changes in regular beta of 0.022 is broadly in conformity with similar studies on different types of events. Analysing the effect of firm-specific earnings announcements, which have an immediate impact on investors' firm valuation processes and hence share prices, Patton and Verardo [267] showed that regular betas increase by 0.16 on average, whereas Ball and Kothari [268] demonstrated that beta increases by an average of 0.04 in the 10 days after earnings announcements relative to the 10 days before the announcements. Grammatikos and Vermeulen [269], who analysed changes in systematic risk following the 2007–2009 financial crisis, established changes in beta factors between -1.20 and 0.97, averaging at -0.14. Using daily measures, Chatterjee and Lubatkin

found that unrelated corporate mergers reduce acquiring firms' beta by 0.058 [482]. In summary, breach-induced changes in regular beta are of smaller magnitude than changes in systematic risk elicited by other types of firm- or market-related events. Given the long-lasting fundamental changes associated with the aforementioned types of events, it is not surprising that beta changes caused by security breach are statistically and economically significant, but overall of lower magnitude.

The average increase in downside beta of 0.031 (i.e., 2.92%) can be considered significant, whereas the small average increase in upside beta of 0.004 (i.e., 0.38%) is not statistically meaningful at conventional levels. The observation that breach-induced changes in downside beta are more severe than changes in upside beta is in line with intuition. Downside beta is considered to be a more appropriate measure of risk than the CAPM's regular symmetric single beta [36, 260–266], and investors are more wary and aware of a firm's negative news history during Down Markets[6]. It is fair to assume that changes in regular beta hence mainly stem from greater exposure to market fluctuations in bearish markets.

Generally, the significant positive changes in regular and downside beta suggest that market participants alter their estimates of breached firms' operational risk. The announcement of a severe security breach appears to remind investors of the negative economic repercussions associated with such events. Moreover, the short- and long-term direct costs of recovering from security breaches (e.g., forensics and audit fees, legal and regulatory expenditures, revenue losses, and customer re-acquisition and retention costs) reduce breached firms' ability to react flexibly to changing market conditions and consumer demand.

The finding that systematic risk in terms of beta and downside beta increases following a security breaches carries multiple material implications for breached firms. As laid out in Equation 3.5, according to the CAPM [118–121], $beta_i$ is the focal element of a firm's cost of equity as this firm-specific indicator of systematic risk (i.e., correlated relative volatility) is multiplied by the difference between R_m and r_f, the market risk premium. Shifts in beta imply variations in a stock's sensitivity to market risk and indicate changes in investors' assessment of a firm's systematic risk (i.e., the proportion of overall investment risk that is specific to the focal firm and cannot be eliminated by portfolio diversification).

Market cyclicality also affects high-beta firms' stock more strongly than it does low-beta firms [110, 483]. With increased exposure to aggregate market risk ($beta_i$), investors expect a greater proportion of risk premium ($R_m - r_f$). Put differently, investors expect to be compensated for taking on greater individual risk incurred by investing in a firm subject to greater market risk. Accordingly, a firm's cost of equity increases. This major

[6]The argument that investors overly pay attention to negative firm news is in line with Kahneman and Tversky's Prospect Theory and Utility Theory [272–274].

implication of the study is in line with Florackis et al. [484], who demonstrated that firms with greater exposure to information security risk, as measured by cybersecurity-risk disclosures in corporate filings, are associated with higher expected stock returns.

A firm's weighted average cost of capital (WACC) consists of its proportionately weighted cost of equity and debt factors. Accordingly, all other things being equal, with increases in beta, a firm's cost of equity increases, which in turn results in an increase in WACC. An increase in beta, cost of equity, and consequentially cost of capital, leads to an increase in risk factors[7], heightened cost of funding a firm's operations, elevated discount factors applied in valuation scenarios, and reduced share prices [58, 82, 105, 110, 111, 216].

Following a value-based planning (or shareholder value) approach, value creation on project-level is commonly defined in financial terms, as the project's net present value (NPV) [110], which decreases with greater discount factors [157]. As mentioned in Section 2.2, in the context of information security investments, an NPV calculation may be used when intending to summarise the net benefit gained from investments in security controls into one single value [22, 110, 157]. The discount factor applied in NPV-based project valuations is typically based on WACC. Discounted future economic benefits thereby decrease with greater WACCs, resulting in lower NPVs. A low NPV might render an otherwise sound project economically unviable. Accordingly, greater systematic risk (β_i and β_i^-) factors following security breaches, causing greater WACCs and discount factors, can induce executives to shy away from pursuing investments in information security.

Moreover, on firm-level, discounted cash flow-based company valuations also decrease with greater discount factors (i.e., WACC) [58]. As discounted cash flows are highly correlated with stock prices [105], greater WACC coefficients cause lower market values. In the context of security breaches, this implies that one of the factors influencing share price drops following security breaches (see [26, 30, 171–174, 176–182]) can be due to investors expecting increases in systematic risk, and hence applying greater discount factors to future cash flows.

In summary, financial valuations of projects, investments, and firms are based on the time value of money concept, which incorporates a discount factor reflecting risk. In corporate scenarios, this discount factor is usually based on the weighted average cost of capital (WACC) principle, which partially depends on a firm's systematic risk, measured as the firm-and-time-specific beta. All other things being equal, a firm with a relatively low beta features lower cost of capital, and thus the ability to invest in lower-return projects and to command higher company valuations [105, 157, 255]. Following this line of argumentation, a security breach causing increases in regular and downside beta can render investments economically unfavourable and depress stock prices.

[7] Investors tend to use the terms risk factor and discount factor synonymously.

Greater cost of capital also introduce additional costs to society at large: breached firms might increase prices for consumers to offset increasing costs, reduce capital expenditures, and delay investments. Moreover, capital markets become less efficient given that investors' fair price discovery process is impeded by security breaches inducing changes to firms' cost of capital structure.

5.7.3 Factors Influencing Changes in Beta

The regression models presented above indicate a weak negative statistical association between security breach-related changes in regular beta and Industrial companies. This finding suggests that firms operating in said sector are less susceptible to changes in systematic beta than firms in other industries are. The reason for this observation might be the fact that Industrial companies supply goods and services used to produce other goods as opposed to selling directly to customers. Investors might expect that buyers of industrial goods pay less attention to security breaches than retail customers do. Following that logic, business-to-business firms might be expected to be less subject to increased scrutiny and increased costs than business-to-consumer firms.

Generally, differences between industries are not distinctively pronounced, which might be due to small subsample sizes. Interestingly, obvious direct costs and increases in underlying / consequential cost of equity are not necessarily interlinked. Direct costs of security breaches tend to be the highest in Healthcare [163]. However, Healthcare companies are not associated with significantly greater changes in beta or downside beta than companies in other industries.

The impact of security breach announcements on regular beta is more severe in firms that do not feature a primary listing on a US stock exchange. This might be due to the more advanced information environment and higher market liquidity present in the United States.

Firm-size effects with regards to the impact of security breaches on downside beta were also established. A statistical trend indicates that breached medium- and large-sized firms are less prone to suffer from increases in downside beta. Firm size is generally negatively associated with information asymmetries [408, 472], as larger firms attract greater analyst and media coverage. Hence, as smaller firms are already subject to greater ex-ante information asymmetries, it is likely that small firms' security breach announcements carry greater relative informational value to investors whose changes in breached firms' risk assessments are hence more pronounced.

5.7.4 Limitations

There are some limitations to the study's design and results. First, as mentioned above, Up and Down Markets can be defined in various ways [260]. It is hence debatable whether average market participants define upside and downside risk as presented here (i.e., on a daily basis, benchmarking actual returns against zero).

As common in related studies, market risk was proxied in terms of volatility of the respective country's broad major multi-industry stock market index. To verify robustness of the results, the analysis could be repeated using industry-based indices instead of country-based ones. For instance, for the exemplifying case study used in Sections 3.5.2 and 5.7.1, the relevant stock market could be proxied by using Business & Consumer Services or Retail indices.

The difference between untransformed and winsorised changes in beta suggest the presence of outliers in the sample. Such outliers may be due to small samples of daily downside betas, as daily beta factors are highly volatile [33]. Small daily downside beta samples are due to markets yielding predominantly non-negative returns around a particular security breach.

As none of the regression models' F-statistics indicated overall-significance, insights into firm characteristics affecting the extent to which security breaches induce changes in systematic risk and systematic downside risk were rather limited. Accordingly, the variables chosen to explain changes in beta could be reconsidered in further studies.

5.8 Conclusion on Breach-Induced Changes in Cost of Equity

This chapter contributes novel insights to the literature on underlying / consequential economic effects of security breaches generally and changes in financial systematic risk exposure specifically. It describes the results of the first study in this area to consider post-breach changes in both upside and downside risk as well as firm characteristics mitigating changes in systematic risk.

Analysing 202 security breaches between 2005 and 2019 revealed that severe security breaches are associated with statistically and economically significant positive increases of financial systematic risk and financial systematic downside risk in terms of regular and downside beta. On average, breached firms experience a rise in regular and downside beta of 0.022 and 0.031, respectively. Security breaches do not appear to be systematically linked to increases in systematic upside risk in terms of upside beta.

As cost of equity are a reflection of how risky investors deem an investment in a company to be, these findings imply that market participants consider breached firms a greater investment risk. Consequently, investors' return expectations increase, resulting in elevated costs of equity and by implication cost of capital. In summary, ceteris paribus security breaches hence raise cost of capital.

Stakeholder value-maximising security executives are inherently interested in, and due to their fiduciary duty also legally obligated to, mitigating negative cash flows and invest monetary resources in the most economically efficient way [17,18,76][8]. When considering information security investments, executives strive to quantify negative economic impacts (λ) that potential investments shall mitigate. Using ENBIS as a metric to decide on the cost effectiveness of investments requires information security decision makers to estimate the Annual Loss Expectancies with (ALE_s) and without (ALE_0) security investment. The expected costs stemming from a security breach (λ) is thereby of particular relevance and estimation difficulty. Focusing exclusively on obvious costs neglects an entire subset of relevant economic considerations.

To this end, this study represents an important step towards a more holistic concept of security breaches' economic impact and can thus aid corporate information security investment and policy makers. In terms of the ENBIS equation, the study demonstrated the existence of an additional underlying / consequential cost element in the expected costs vector in the form of increases in financial systematic risk and hence cost of equity ($\lambda_{fincosts_{CoE}} > 0$)[9].

In fact, increases in cost of equity are of dyadic relevance for calculating the economic benefit of security investments. On the one hand, greater cost of equity — as evidenced by increased beta factors — can lead to project cancellations if NPV requirements are not met, lower valuations in corporate transactions (e.g., mergers and acquisitions), and lower share prices [58,82,105,110,111,157,216]. This $\lambda_{fincosts_{CoE}}$ cost element is of *consequential* nature as it only substantiates indirectly and consequent to a security breach event over time. Naturally, for each firm, the particular $\lambda_{fincosts_{CoE}}$ figure, resulting from aggregating the related negative economic impacts, is different and subject to, for instance, capital structures and intentions to sell all or part of the firm's equity. Nevertheless, for any firm, with an increase in the cost vector λ (and accordingly ALE_0), the expected benefit of information security (i.e., the difference between ALE_0 and ALE_s) increases. The rational security executive strives to include all potential costs and benefits into the information security investment decision-making process. If greater total cost ($\lambda_\Sigma = \lambda_{ab\ initio} + \lambda_{fincosts_{CoE}}$) can

[8]See Section 2.1 for further explanations on executives' duties and motivation as part of principal-agent arrangements which imply fiduciary responsibilities to shareholders.

[9]Note that none of the parameters including ALE_s, ALE_0, and λ are explicitly estimated here.

be mitigated via an information security investment, the decision to pursue said investment becomes more economically reasonable. It is hence in the best personal and professional interest of rational security executives to factor negative economic impacts arising from increases in cost of equity into their investment decision-making process.

On the other hand, greater cost of equity — as evidenced by increased beta factors — leads to an increase in WACC [58, 82, 105, 110, 111, 157, 216], the underlying discount rate r applied to determine the net present value of potential information security investments. A low project-based NPV might induce firms not to pursue an investment in otherwise economically sound net cash flow positive projects. Accordingly, increases in cost of equity can constitute a cost element of *underlying* nature. All else being equal, for a firm that suffered from a security breach, the net present value (NPV) of the expected net benefit of an information security investment ($ENBIS$) is lower. Paradoxically, in isolation, the underlying cost element $\lambda_{fincosts_{CoE}}$ in the form of greater WACC might hence render a breached firm less likely to invest in information security.

The results of this study also imply that corporate decision makers in breached firms need to pay particular attention to their cost of capital to mitigate potential increases. As costs of capital are systematically associated with a firm's leverage [485], breached firms are likely to adjust their capital structure and leverage following a breach. Prior research indicated that breached firms indeed increase their cash holdings and decrease external financing [486].

Overall, this chapter introduced a novel perspective on non-obvious underlying and consequential costs associated with (breaches of) information security and thereby added to nascent theories on information security investments and management generally. The contribution to the information security economics literature is twofold. First, previous work that used small and now-outdated samples [33–35] was extended by using a new hand-picked dataset, which allows for presenting more holistic, useful, and updated empirical insights into the effect of security breaches on firms' systematic risk. Second, this contribution constituted the first analysis of "a more appropriate measure of portfolio risk" [36, p. 265], namely dual-beta models, in addition to regular betas. Additionally, new indicative insights into firm characteristics potentially mitigating changes in systematic risk were contributed.

An improved understanding of changes in systematic risk is of relevance to information security economics researchers and practitioners alike. For researchers, an increase in cost of equity following changes in the underlying exposure to financial systematic risk (i.e., beta) might inform frameworks and models on information security investments based on cost-benefit analyses. Increases in systematic risk and cost of equity might also help to explain a multitude of corporate phenomena following security breaches. From a practitioner's perspective, a holistic understanding of potential impacts of security breaches is essential to

facilitate economic decision making. Changes in cost of equity resulting from increases in financial systematic risk are also of concern to corporate executives, as the measurement relates to all major corporate finance activities including capital raising, share issues and buybacks, as well as shareholder value management. Similarly, for investors, an increase in cost of equity, and consequentially an increase in cost of capital, implies an increase in a firm's (investment) risk [111].

Chapter 6
Security Breach Costs: Cost of Debt

An analysis of changes in CDS spreads following information security breaches

This chapter presents the results and discussions of the analysis on credit default swap (CDS) spread changes following severe security breaches. By providing novel empirical evidence on security breach-induced underlying and consequential costs in the form of widening short-term CDS spreads indicating increasing default spreads, and eventually cost of debt, the chapter constitutes Contribution **C3**.

6.1 Overview

The ideation and ensuing analysis for Contribution **C3** began by posing the research question: *Do severe security breaches increase firms' cost of debt by elevating perceived default risk?* It was hypothesised that severe security breaches in publicly listed firms are systematically associated with significant positive changes in default risk as proxied by CDS spreads. Accordingly, the aim of Contribution **C3** was to assess whether severe security breaches are associated with rises in default premiums, which would eventually result in an increase in firms' cost of debt. Employing the methodology laid out in Section 3.6 to test the hypothesis outlined in Section 2.8 suggests that on average severe security breaches are not associated with statistically significant increases in CDS spreads.

Out of the initial sample of 202 severe security breaches between 2005 and 2019, 75 events pertained to firms for which quoted CDS spreads were available via *S&P Capital IQ*. This sample was further reduced to 73 complete event observations for the regression-based quasi-experiment analysis. Overall, neither of the two analyses finds sufficient empirical evidence

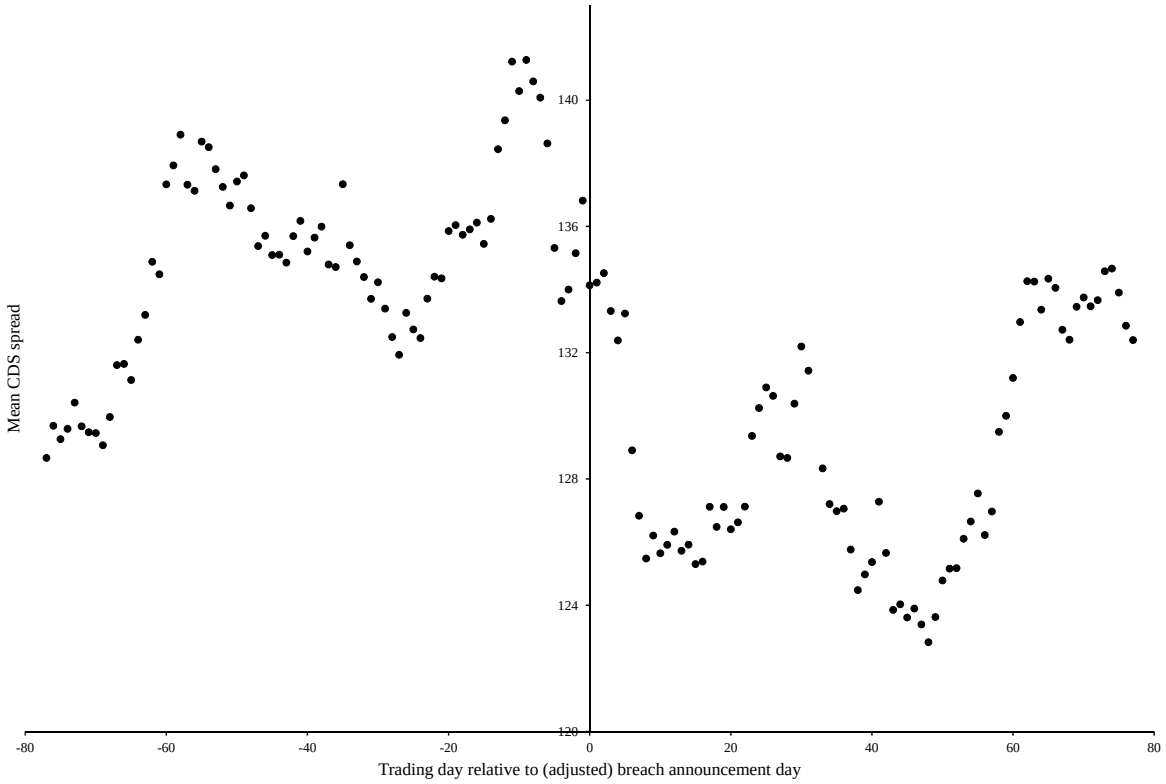


Figure 6.1: Mean CDS Spreads Around Security Breach

in support of the ex-ante hypothesised relationship between severe security breaches and changes in CDS spreads. Particularly, controlling for changes in CDS spreads of competitors, the rating-matched index, as well as antecedent factors known to be associated with changes in CDS premia suggests that the short-term effect of security breaches on CDS spreads is negligibly small. The findings indicate that potential increases in firms' cost of debt do not occur in the short-term around the security breach or that they are not exclusively driven by objective default risk considerations.

Figure 6.1 shows daily CDS spreads [bp] averaged across the sample of 75 severe security breach events during the 155 days surrounding a breach event, centred on the (adjusted) breach announcement date. Generally, average CDS spreads exhibit notable volatility, indicating the presence of periodicity effects as well as market participants who frequently price in new pieces of information. Initial indicative graphical analysis suggests that on average CDS spreads widen in the time period leading up to a security breach event announcement, peaking at t_{-9}, i.e., nine trading days prior to the (adjusted) breach announcement day. CDS premia then seem to drop, until exhibiting another marked increase during the three

trading days (t_{-3} to t_{-1}) immediately prior to the event date. Interestingly, there appears to be a distinct fall in average CDS premia during the three weeks (15 trading days) following security breach announcements, before eventually returning to an overall higher level in the long run ($\overline{CDS\ Spread_{t_{60}}} >> \overline{CDS\ Spread_{t_{-60}}}$).

This contribution's empirical analysis focused exclusively on the short-term impact of security breaches on CDS spreads. Assessing the short-term effect of corporate events on CDS premia is in line with previous literature [295] and fundamental financial economics considerations culminating in Fama's seminal paper on the Efficient Market Hypothesis (EMH) [108]. Extending the logic of the semi-strong form of the EMH to the market for CDS contracts, current CDS premia are expected to adjust almost instantaneously to newly issued public information and provide a time value-adjusted (i.e., appropriately discounted) reflection of expectations on future developments. Put differently, even if market participants expected security breaches to result exclusively in negative repercussions in the long run, such considerations would be reflected in their pricing models immediately around the time of the security breach publication.

Applying a matching-portfolio approach study set-up to the sample of 75 events revealed that competitor- and index-adjusted changes in CDS spreads are not statistically positively different from zero. Introducing a quasi-experiment factor model controlling for a multitude of variables known to be associated with changes in CDS spreads similarly confirmed that breached firms do not exhibit statistically significantly greater increases in CDS spreads than their non-breached competitors do.

This chapter presents all relevant empirical results based on the methodology laid out in Section 3.6 and discusses the economic relevance and limitations of these findings. On a high level, it is established that — relative to cost of equity — cost of debt, an underlying or consequential cost item prone to be overlooked in assessments of the economic viability of information security investments, might be of lower relevance to information security investment decision makers assessing immediate negative economic impacts of security breaches. Contribution **C3** also corroborates the notion that there are asymmetric reactions in the private and public debt markets[1].

First, Section 6.2 reveals the results of t-tests, sign tests, and Wilcoxon signed-rank tests on winsorised changes in CDS spreads stemming from the two matching-portfolio analytical approaches. Second, regression models controlling for multiple influencing factors simultaneously including volatility, market movements, and risk-free rates were set up. The results

[1]In the context of this study, private debt refers to unsecuritised corporate debt arranged privately between a lender and a borrower and not traded on bond markets. Public debt refers to corporate debt securities and their derivatives traded on public bond markets and CDS OTC markets.

of this regression analysis are presented in Section 6.3. Overall, there is insufficient support in favour of rejecting the null-hypothesis in connection with **C3-H1**, establishing that severe security breaches are not associated with statistically significant increases in default risk as measured by changes in CDS spreads. The evidence is robust to changes in the considered time periods, but limited to a short-term perspective and a small sample, and might hence lack generalisability qualities and explanatory power.

6.2 Empirical Results Matching-Portfolio Approach

The aim of Contribution **C3** was to assess whether severe security breaches are associated with an increase in firms' cost of debt as indicated by rises in default premiums. As laid out in Sections 2.8 and 3.6, CDS spreads provide an ideal "pure" and standardised market-oriented proxy to measure changes in default risk in a near-real time manner. An *unexpected* increase in CDS spreads, i.e., one that is greater than either the contemporaneous change in competitors' CDS prices or the change in the overall market for CDS, thereby indicates that the focal firm's CDS spread is indeed subject to greater default risk exposure and the firm hence attracts greater return requirements leading to elevated cost of debt.

Tables 6.1 and 6.2 present the results of the two matching-portfolio studies. Table 6.1 features the results of the rating-matched portfolio approach; Table 6.2 exhibits results based on industry-matched portfolio adjustments. The tables show the results of the event study-like analysis of cumulative abnormal CDS spread changes during the event windows $[-3, 1]$, $[-2, 0]$, $[-2, 2]$, and $[-1, 0]$ relative to the (adjusted) breach announcement date. Both tables present from left to right, the short-term event window considered, sample size, mean, median, one-sided Student t-test statistics, sign test statistics, and one-sided Wilcoxon signed rank test statistics.

First, consider winsorised unexpected changes in CDS spreads based on the similar rating-portfolio adjustment approach in Table 6.1. Only the event windows $[-3, 1]$ and $[-2, 2]$ exhibit a mean change of the expected direction. Similarly, in the event windows $[-3, 1]$ and $[-2, 0]$, the median scores of abnormal cumulative CDS spread changes are negative. The median scores pertaining to the event windows $[-2, 2]$ and $[-1, 0]$ are positive, and positive ratio scores are marginally greater than 50%, however, none of these figures are statistically meaningful at conventional significance levels.

Second, consider winsorised unexpected changes in CDS spreads based on the competitors portfolio adjustment approach in Table 6.2. Mean winsorised cumulative abnormal CDS spread changes across all considered periods of time are of the expected sign. However, none of the positive mean abnormal changes can be considered statistically meaningful according

Table 6.1: CDS Spread Changes — Rating-Matched Portfolio Adjusted

Event window	n	M	Mdn	t	p_t	$PosRat$	p_{Sign}	$Pseudo\ Mdn$	$p_{Wilcoxon}$
$[-3,1]$	75	0.317	-0.350	0.253	0.400	0.453	0.822	-0.408	0.775
$[-2,0]$	75	-0.167	-0.235	-0.174	0.569	0.493	0.591	-0.218	0.693
$[-2,2]$	75	0.740	0.080	0.515	0.304	0.520	0.409	-0.127	0.578
$[-1,0]$	75	-0.528	0.090	-0.530	0.701	0.520	0.409	0.103	0.383

Note: *** $p < 0.01$; ** $p < 0.05$; * $p < 0.1$; n = sample size; M = sample mean; Mdn = sample median; t = test statistics t-test; p_t = p-value t-test; $PosRat$ = positive ratio sign test; p_{Sign} = p-value sign test; $PseudoMdn$ = pseudo-median Wilcoxon test; $p_{Wilcoxon}$ = p-value Wilcoxon test. Mean and median cumulative abnormal CDS spread changes are in absolute terms. t-tests and Wilcoxon signed-rank tests are one-sided, testing the alternative hypothesis that the population mean is greater than zero and that the population pseudo-median is greater than zero, respectively. Sign tests are one-sided, testing the alternative hypothesis that the positive ratio is greater than chance (0.5). Cumulative abnormal CDS spread changes are winsorised at the 0.01 level at both tails.

Table 6.2: CDS Spread Changes — Industry-Matched Portfolio Adjusted

Event window	n	M	Mdn	t	p_t	$PosRat$	p_{Sign}	$Pseudo\ Mdn$	$p_{Wilcoxon}$
$[-3,1]$	75	2.012	0.100	0.652	0.258	0.547	0.244	0.273	0.303
$[-2,0]$	75	2.909	-0.282	1.247	0.108	0.480	0.678	-0.059	0.549
$[-2,2]$	75	2.058	-0.293	0.790	0.216	0.467	0.756	-0.149	0.578
$[-1,0]$	75	1.137	0.400	0.713	0.239	0.587	0.083^{*}	0.532	0.065^{*}

Note: See Table 6.1.

to t-test results. The event windows $[-3,1]$ and $[-1,0]$ also exhibit positive median scores and positive ratios of greater than 50%. For the shortest event window ($[-1,0]$) these median and positive ratio scores can be considered statistical trends according to Wilcoxon signed-rank test ($p_{Wilcoxon} = 0.065$) and sign test results ($p_{Sign} = 0.083$). The results suggest that the true population mean and median are not significantly greater than zero and that positive differences are unlikely to occur with greater likelihood than chance.

The overall results for both CDS spread changes adjustment approaches are qualitatively robust to changing the outlier treatment approach, that is, analysing untransformed cumulative abnormal CDS spread changes, and those winsorised at the 0.05 level at both tails of their respective distribution, yields substantially similar results. In summary, the study of competitor- and rating-adjusted CDS spread changes does not find sufficient evidence to reject the null hypothesis in connection with hypothesis **C3-H1**. Severe security breaches in publicly listed companies do not seem to be associated with short-term increases in CDS spreads that systematically exceed those contemporaneously present in competitor firms or

in those with similar credit ratings.

6.3 Empirical Results Regression Model Approach

The starting point for the quasi-experiment factor model analysis was the same as in Section 6.2. Due to the small event sample size, the cross-country and multi-year nature of the sample, and the myriad of other factors influencing changes in CDS spreads, further analysis controlling for such variables was merited.

Similar to the previous event study-like analysis, it was hypothesised again that severe security breaches in publicly listed companies are associated with widening CDS spreads, which indicate increases in credit default risk and ultimately rises in cost of debt. However, in this particular analytical approach, controlling for micro- and macroeconomic factors as well as time-varying firm-level constant effects known to influence changes in CDS spreads, the study explored the hypothesis that successfully attacked firms feature greater changes in spreads than comparable non-breached firms did over the same periods of time.

The regression-based analytical approach provides not only a different empirical perspective on CDS premia changes, but also possesses greater ability to make claims as to the direct relationship between security breaches and default spreads as proxied by short-term changes in CDS prices controlling for confounding factors. The quasi-experiment-like analytical framework is explained in Section 3.6. Intuition and previous research suggested that CDS spreads — indicating default risk, and therefore by implication debt investors' return requirements and firms' cost of debt — widen following severe security breaches (**C3-H1**). The models presented herein effectively control for intrinsic CDS ($\sigma(CDS\ spread)$) and equity volatility ($\sigma(Stock\ Return)$), other firm-specific information that became available at the same time (*Residual Stock Return*), contemporaneous macroeconomic changes (*Market Return*, *Risk-Neutral Rate*, and *Implied Market Volatility*), as well as time-varying market developments non-idiosyncratic to a firm ($Year\text{-}fixed\ effects$).

Table 6.3 presents descriptive statistics for the pooled overall sample of 1,724 observations, the 1,651 observations in non-breached competitors, and the 73 observations of firms that suffered from a security breach. The average CDS spread change for breached firms is only greater than the contemporaneous one in non-breached firms in the [-2,0] event window. Specifically, the average CDS spread change in breached firms over the three-day event window ending on the (adjusted) breach announcement day was 0.037bp, whereas the average non-breached firms' CDS spread change was -0.242bp. The absence of systematically greater increases in breached firms' spreads relative to competitor firms' spreads suggests that breached firms are not perceived to be subject to greater credit default risk.

Table 6.3: CDS Spread Changes — Factor Model Descriptives

Variable	n	Min	$Mean$	Max	SD
ΔCDS Spread					
t_{-3}, t_1 breached	73	-39.979	0.374	49.861	12.858
t_{-3}, t_1 non-breached	1,651	-98.108	0.449	68.633	17.521
t_{-2}, t_0 breached	73	-28.106	0.037	37.276	8.890
t_{-2}, t_0 non-breached	1,651	-80.458	-0.242	46.613	13.681
t_{-2}, t_2 breached	73	-33.426	0.424	52.062	13.198
t_{-2}, t_2 non-breached	1,651	-72.655	0.424	69.615	15.876
t_{-1}, t_0 breached	73	-56.361	-0.407	30.125	9.391
t_{-1}, t_0 non-breached	1,651	-55.905	-0.217	36.558	9.700
σ(CDS Spread)	1,724	0.445	7.947	101.652	14.412
σ(Stock Return)	1,724	0.022	4.629	182.358	19.502
Residual Stock Return					
t_{-3}, t_1	1,724	-10.190	-0.240	13.248	3.568
t_{-2}, t_0	1,724	-8.018	-0.111	10.947	2.706
t_{-2}, t_2	1,724	-11.239	-0.158	11.071	3.548
t_{-1}, t_0	1,724	-7.083	-0.176	6.703	2.159
Market Return					
t_{-3}, t_1	1,724	-5.628	-0.099	6.663	2.290
t_{-2}, t_0	1,724	-4.390	-0.041	4.496	1.652
t_{-2}, t_2	1,724	-5.770	0.059	6.406	2.171
t_{-1}, t_0	1,724	-3.324	-0.082	2.906	1.187
Risk-Neutral Rate					
t_{-3}, t_1	1,724	-29.960	-0.653	14.383	5.615
t_{-2}, t_0	1,724	-22.002	-0.431	11.048	3.993
t_{-2}, t_2	1,724	-22.190	-0.040	22.235	5.988
t_{-1}, t_0	1,724	-14.286	-0.250	7.984	2.497
Implied Market Volatility					
t_{-3}, t_1	1,724	-31.562	1.828	39.859	12.442
t_{-2}, t_0	1,724	-32.291	0.969	25.232	9.546
t_{-2}, t_2	1,724	-34.568	0.517	47.190	12.346
t_{-1}, t_0	1,724	-24.894	0.809	24.034	7.462
Market Capitalisation at t_0					
breached [m$]	73	1,287.5	86,641.5	613,756.4	116,294.7

Note: n = (sub-)sample size; Min = Minimum; Max = Maximum; SD = Standard Deviation
t_I, t_{II} = Time period relative to (adjusted) breach announcement date for which daily cumulative (absolute / proportional) changes in the respective variables were computed. Breached and non-breached refers to event firms that suffered from a severe security breach and control-group competitor firms, respectively. All values apart from firm size (which is not included in the regression models, but shown for information) were winsorised at the 0.01 level at both tails.

Table 6.4: CDS Spread Changes — Factor Model

	Dependent variable:			
	$\Delta CDS\ Spread_{[-3,1]}$	$\Delta CDS\ Spread_{[-2,0]}$	$\Delta CDS\ Spread_{[-2,2]}$	$\Delta CDS\ Spread_{[-1,0]}$
	(1)	(2)	(3)	(4)
Breached Firm	1.834	2.550*	2.257	1.194
	(1.556)	(1.409)	(1.612)	(1.217)
$\sigma(CDS\ spread)$	−0.149*	−0.264***	−0.167**	−0.170***
	(0.077)	(0.054)	(0.073)	(0.044)
$\sigma(Stock\ Return)$	0.076***	0.065***	0.094***	0.036***
	(0.024)	(0.017)	(0.030)	(0.011)
Residual Stock Return	−0.898***	−0.607***	−0.831***	−0.444***
	(0.167)	(0.166)	(0.155)	(0.170)
Market Return	−2.029***	−1.325***	−1.618***	−1.223***
	(0.317)	(0.294)	(0.303)	(0.273)
Risk-Neutral Rate	0.074	0.138***	0.099**	0.046
	(0.050)	(0.049)	(0.043)	(0.057)
Implied Market Volatility	−0.014	0.054	0.037	0.020
	(0.043)	(0.041)	(0.040)	(0.041)
Year-fixed effects	Yes	Yes	Yes	Yes
Constant	0.848	2.118*	0.792	0.728
	(1.370)	(1.196)	(1.504)	(1.060)
Observations	1,724	1,724	1,724	1,724
R^2	0.250	0.286	0.249	0.209
Adjusted R^2	0.242	0.279	0.241	0.201
Residual Std. Error (df = 1,705)	14.427	11.341	13.535	8.842
F Statistic (df = 18; 1,705)	31.521***	37.975***	31.359***	25.008***
Note:				*p<0.1; **p<0.05; ***p<0.01

The large range and standard deviations of changes in CDS spreads might imply that there is no clearly discernible trend observable, particularly in the small subsample of 73 breach events.

Table 6.3 further shows that on average CDS spreads are approximately as volatile as stock returns, which is in line with the notion that both equity and credit markets feature knowledgeable investors who adjust their pricings based on new information. Recall that seemingly large minimum, mean, and maximum *Risk-Neutral Rate* and $ImpliedMarketVolatility$ values are not absolute values but cumulative proportional changes in the underlying figures.

In Table 6.4, results of the regressions of changes in CDS spreads on the main indica-

tor variable (*Breached Firm*) and relevant control variables are presented with clustered standard errors in parentheses. As common, statistically relevant trends and statistical significance are accepted and discussed at p-values of less than 0.1 and less than 0.05, respectively. Positive coefficients thereby signify that the dependent variable, CDS spread changes, increases (i.e., becomes more positive).

All models are overall-significant as per the F-Test of Overall Significance. The R^2 is in line with previous similar studies (e.g., [319]). The main coefficient of interest, *Breached Firm*, is positive across all time periods considered. However, none of these coefficients are statistically significantly different from zero. Only the coefficient for the three-day event window starting two days prior and ending on the (adjusted) event day (2.550, $se = 1.409$) suggests the presence of a statistical trend of severe security breaches being indeed positively associated with widening CDS spreads.

The control variables' coefficients are of expected direction. For instance, the statistically significant negative coefficients for *Market Return*, and the statistically significant positive coefficients for *Risk-Neutral Rate*, are in line with intuition. There is a natural inverse relationship between the CDS spread and the equity price of a firm; here, the portfolios of CDS spreads under analysis and the market return constitute measurements akin to aggregations of CDS spreads and equity prices. Similarly, surges in the risk-neutral rate indicate that investors can expect greater returns on non-risky investments, in turn leading to greater return requirements on riskier debt investments as well. The presented analyses include year-fixed effects to control for variance that is constant across firms but varying over time.

The four models presented in Table 6.4 demonstrate that the absence of security breach-induced spread increases holds over varied short-term event windows. The regression results are also qualitatively robust to introducing firm-fixed effects in addition to year-fixed effects and winsorising variables at the 0.05 level at both tails.

Overall, firms that experienced severe security breaches are on average not associated with additional increases in CDS spreads relative to their non-breached counterparts. Put differently, the occurrence of severe security breaches is not systematically associated with widening CDS spreads.

6.4 Discussion of Empirical Results

Contribution **C3** aimed to close the gap in the literature pertaining to post-breach empirical evidence on changes in firms' cost of debt. By analysing changes in CDS spreads, a market-near proxy for default spreads which constitute a key part of cost of debt estima-

tions, the study demonstrates how (public) debt market participants evaluate the short-term impact of severe security breaches. In summary, both the two event study-like analyses and the regression-based model, examining abnormal changes in CDS spreads adjusted for co-movements in competitors, the rating-matched index, and multiple control variables, did not establish a statistically significant impact of security breaches on short-term CDS spreads. The evidence can generally be considered strong, given that it is not sensitive to changes in the empirical set-up, particular event-window time periods, and outlier treatment approaches.

The absence of a significant association between severe security breach announcements and short-term CDS spread changes indicates that breached firms are not associated with statistically significant increases in default risk as measured by changes in CDS spreads, and that post-breach increases in firms' cost of debt do not pertain to public debt, are not exclusively driven by objective default risk considerations, or do not occur in the short-term around the security breach.

Accordingly, the multitude of potential explanations as to why the two analytical approaches did not reveal the hypothesised association between security breaches and CDS spreads can be subsumed into three categories:

1. CDS spreads are not affected, as public debt investors do not expect security breaches to negatively affect breached firms' earnings and cash flow (stability).

2. CDS spreads might actually be affected by security breaches, but premia changes substantiate after the analysed period of time.

3. CDS spreads might actually be affected by security breaches, but premia changes substantiate before the analysed period of time.

There are also some limitations regarding the empirical set-up. This section provides a discussion of the three aforementioned sets of potential explanations, possible limitations, and implications of this study's results.

6.4.1 Irrelevance to Public Debt Investors

First and foremost, it is worth noting that at initial glance, the findings of this study appear unexpected given the hypothesised positive relationship between costs of debt (in terms of default spreads as proxied by CDS spreads) and security breaches. However, the finding that public credit market participants do not seem to change their risk assessments and pricing levels is actually in line with previous studies. Iyer et al. [307] established that bond prices (i.e., indications for debt traded on public markets) do not exhibit statistically significant changes in the three-day, eleven-day, and even 31-day event windows surrounding a security

breach announcement. Relatedly, Binfarè [201] demonstrated that security breaches are only associated with increases in at-issue rates charged by private lenders such as banks, whereas there is no statistically significant effect of security breaches on public debt rates (i.e., newly issued public corporate bonds' yield spread). Apparently, private debt issuers react differently to security breaches than institutional public debt investors do.

The CDS market merely provides a different, one might argue complementary but diametric, perspective on public debt markets. Given the strong inherent theoretical and empirical connection between the bond market and the CDS market [290, 305], the absence of statistically significant abnormal changes in the CDS market shown in this present study can therefore be seen as being in line with Binfarè's [201] and Iyer et al.'s [307] findings. Combining the three studies' results on new bond issues, existing bond price changes, and CDS spread changes suggests that firms' risk assessments conducted by institutional (public debt) investors, who are the main investor group partaking in new bond issues and engaging in CDS contracting activities, are less affected by security breaches than those done by private debt investors. This notion is consistent with public debt market participants, who tend to be professional investors, being less prone to overreaction and having greater access to a multitude of information sources and hence better informed views, particularly with regards to information predictive of future period earnings (see e.g., [295, 487–492]).

Stock markets, which feature larger numbers of less sophisticated investors, are known to react more spontaneously, and may often overreact, to security breach announcements [307]. In fact, there is some evidence that breach-induced negative stock price shocks may only be of short-term nature and do not necessarily impact firms in the long run [184–187]. There is an inherent inverse relationship between share prices and CDS spreads (see e.g., [310]). However, CDS markets are dominated by institutional public debt investors and hence deemed to be even more sophisticated and efficient than equity markets [323]. In practice, CDS traders have even been shown to focus on different content within the same news items relative to equity traders [493]. One can therefore intuitively assume that a short-lived overreaction on equity markets causing share prices to drop does not necessarily manifest on CDS markets at all. It is also worth recalling that debt is senior to equity and often secured against assets. The observation that debt holders are less affected by a security breach than equity holders hence seems natural.

Moreover, banks (i.e., private debt investors) are subject to different sets of incentives and dynamics. When deciding on their loan portfolios, banks can be inclined to engage in lending activities to breached firms not exclusively based on their risk assessments. Instead, they are likely to grant loans based on relationship banking considerations and follow-on (advisory) fee-generating opportunities (see e.g., [494–496]). To compensate for the increased

risk incurred when granting a loan, and to facilitate offloading loans from their balance sheet later on, banks might decide to charge higher interest rates. In contrast, (institutional) public debt holders are more flexible and unconstrained in their decision-making process on whether they want to hold debt, and debt derivatives, of a particular (breached) firm at a given point in time.

Relatedly, as delineated in Section 2.8, CDS spreads are a direct proxy for firms' default risk, which is in turn the major driver behind cost of debt. In theory, the default spreads estimated on the (public) market for CDS should apply to all debt holders, public and private. However, besides the theoretical default risk and macroeconomic conditions, private lenders also consider other factors such as costs of intermediation including screening and monitoring costs — which banks might anticipate to increase following a security breach — when computing interest rates charged on a loan [497].

It was hypothesised that security breaches, which can introduce a plethora of obvious and underlying / consequential economic consequences on earnings quality, affect CDS spreads in the same way as events that are arguably more fundamental to firms' default risk, such as earnings announcements, do. However, the results presented in this chapter add further evidence to the notion that public debt investors deem the impact of security breaches on default risk to be rather minor.

The conjecture that public debt investors are less susceptible to security breach announcements than private debt investors are, as suggested by the results of Binfarè [201], Iyer et al. [307], and this study, carries an important implication for breached firms' capital structures. Firms that experienced severe security breaches might be inclined to reduce the proportion of private debt in their debt capital mix and rather favour greater public debt proportions.

6.4.2 Cost of Debt Impact Substantiates Subsequently

Section 6.4.1 explained that the absence of significant abnormal increases in CDS spreads around security breach announcements signifies that investors' default spread expectations remain unaltered after a severe security breach. Despite the plethora of obvious and underlying / consequential negative economic consequences of security breaches, debt holders appear to assign no major relevance to successful attacks with regards to their abilities to hamper firms' ability to service debt interest and principle payments. It was further elaborated that there are potential differences between costs of public and private debt, and that the latter's post-breach interest rates may not be exclusively driven by default spread considerations (as indicated by CDS spreads).

However, there are two alternative explanations for the absence of significant default spread changes during the assessed event windows around severe security breaches. In this subsection, the possibilities that negative impacts only substantiate over the course of time and that the CDS market is not fully efficient as debt market participants underreact are discussed.

First, this study of abnormal CDS spreads only reveals explicit evidence pertaining to short-term changes; it does not necessarily contradict the hypotheses that (a) default spreads as indicated by CDS premia may rise in the subsequent long-run, or that (b) long-term consequences in terms of cost of debt may accordingly substantiate only later on. It is possible that some negative economic consequences only manifest themselves in the weeks after the initial security breach announcement, or that the severity of attacks' impact might not be fully obvious at the time of the event announcement.

Relatedly, although most studies find that CDS markets react to new information fully, efficiently, and immediately (e.g., [498–500]), analysing CDS market reactions to fundamental earnings news, Jenkins and colleagues [455] revealed evidence consistent with the notion that — despite the overwhelming presence of professional investors — the CDS market is not immune to initial underreaction to information announcements. There is also evidence suggesting that CDS markets can to a certain extent lag equity markets' reactions to events [501–503], and that information dissemination on the CDS market is subject to delay even in the case of highly fundamental financial information [504]. Following the logic of the Efficient Market Hypothesis [108, 109], markets adjusting to new information should be observable in the immediate days surrounding the announcement events. Accordingly, this study examined CDS spread changes over a total of six days centred on the (adjusted) breach announcement date. However, based on previous studies [455, 501, 504], there is also the possibility that CDS markets underreact initially and only properly price in new information learned from a breach announcement in the days and weeks following such a news event.

Anecdotally, Figure 6.1 shows that average CDS spreads of breached firms exhibit substantial rises during the time periods ranging from t_{15} and t_{30} as well as during t_{48} to t_{63} relative to the (adjusted) breach announcement day.

The suspicion that security breaches' effect on default spreads and ultimately cost of debt exclusively manifests during a remote financial period, and that public debt markets are not fully efficient, would be in line with the findings of Huang and Wang [306] and Binfarè [201] who only demonstrated the existence of said effect over the three or four years subsequently to a security breach.

6.4.3 Cost of Debt Impact Substantiates Priorly

In Section 6.4.1, it was established that insignificant CDS spread changes around security breaches indicate that investors do not expect security breaches to have significant impacts on credit quality and default risk. Differences between public and private debt holders were also discussed. Section 6.4.2 then provided an alternative explanation for the absence of hypothesised default spread changes, namely the possibility that negative impacts only substantiate significantly later.

Another possible angle explaining the insignificant change in CDS premia surrounding breach announcements is that CDS premia price the breach impact not subsequently to, but in fact *before* the official announcement date.

The graph presented in Figure 6.1 provides anecdotal evidence in support of the notion that informed market participants trade on the CDS market prior to the release of information as indicated in the PRC database. Specifically, the graph shows that average CDS spreads of breached firms increase substantially in the days and weeks prior to the (adjusted) breach announcement day, and peak nine trading days prior to the event date.

The presence of informed traders in the market would hint at information leakage and "insider trading". Generally, information leakage is a common issue in event study-type analyses on corporate events (see [442, 443]), which is why the analysis for Contribution **C3** included up to three trading days prior to the breach announcement in the examined event windows. However, informed trading might have already occurred in the time period leading up to those three days.

There is a noteworthy body of evidence positing that the CDS market anticipates negative news announcements (e.g., [290,310]). Analysing unfavourable earnings announcements, Greatrex [322] found statistically significant increases in CDS spreads in the [-20,-2] time period prior to bad news announcements indicating that the market anticipated them. Similar conclusions were drawn by Finnerty et al. [314], who documented that the CDS market anticipates positive as well as negative credit rating change announcements, whereby the phenomenon is particularly pronounced for downgrades. Relatedly, Zhang and Zhang [323] showed that the CDS market anticipates negative earnings surprises in the 30 days prior to the announcement day, but on the announcement day only speculative-grade firms are associated with abnormal CDS spread changes. Batta et al. [319] and To et al. [505] go even further, providing evidence that strongly suggests the presence of informed insiders operating in the CDS market, which provides an easier and less regulated platform to make informed trades due to its OTC nature.

Insider trading, that is, corporate insiders buying and selling financial instruments re-

lated to their own firms, is generally considered legal in most jurisdictions, as long as such trades are not based on material non-public information and appropriately reported to the relevant authorities [39, 337]. There is a nascent but growing body of anecdotal and empirical evidence establishing that informed market participants trade on private knowledge of security breaches prior to their public announcement [337, 413–419]. Given the apparent presence of informed traders on equity and derivatives markets, the observation that CDS spreads peak prior to the announcement of severe security breaches might be due to informed market participants trading on their knowledge of imminent attack announcements.

6.4.4 Limitations

For the main finding of this study — there is no statistically significant association between severe security breach announcements and short-term CDS spread changes — to hold, the underlying data has to be considered appropriate, without unaccounted-for biases and of sufficient explanatory power for the analyses to be correctly specified. However, there are some limitations to this study that might have hampered the ability to demonstrate the non-existent effect of security breaches on short-term default spread changes.

First, there are some empirical issues concerning the sample of $n = 75$ (or $n = 73$) severe security breaches. As outlined in Chapter 2, data availability is a major area of concern for information security researchers and practitioners. For instance, when using the PRC database — as many previous studies have (e.g., [164, 180, 202, 437]) — one is faced with the option to either apply a naïve approach by analysing the entire unadjusted database, or to restrict the ensuing analyses to cases that are of high significance in terms of their levels of criminality and intention involved, volume, and publicity. As explained in Section 3.2, in this dissertation we chose to do the latter.

Whilst the overall sample of severe security breaches ($n = 202$) was of sufficient size for analyses in the context of Contribution **C2** (see Chapter 5), the low availability of CDS spread data for Contribution **C3** resulted in a significantly smaller useable sample. A post-hoc analysis of the reported results showed that the small sample size rendered all t-tests to be associated with very low statistical power as per Cohen [506, 507]. Specifically, at a significance level (Type I error probability) of 0.05, the small sample size in combination with low Cohen's d values resulted in the power of these tests (i.e., the probability of avoiding a Type II error) to be far below the usual threshold of 0.80. To mitigate the small sample size issue and to strengthen the analytical approach, quasi-experiment regression-based models controlling for contemporaneous factors influencing changes in CDS premia were established as well. Although these factor models unanimously supported the null results obtained from

the matching-portfolio approach, the small sample and low power is still of relevance as it reduces the generalisability of the results presented in this chapter.

Relatedly, the sample is biased towards medium- and large-sized firms[2]. Specifically, Table 6.3 shows that the average breached firm featured in the sample had a market capitalisation of $86,641.5m, whilst the smallest firm present in the sample featured a market capitalisation of $1,287.5m. In fact, only two observations in the sample of 73 breach events featured a market capitalisation of below $2bn and could accordingly be classified as small firms. Larger firms tend to be associated with lower ex-ante CDS spreads [508, 509]. Additionally, most breached firms in the sample featured investment grade credit ratings[3], whereas CDS premia of firms with non-investment grade credit ratings are more susceptible to the impact of corporate events than those with an investment grade rating are [295, 322]. Accordingly, due to the aforementioned sample biases, the study's results might be of limited generalisability to smaller firms with speculative credit ratings and rather mainly apply to large firms with low ex-ante CDS spreads and those with investment grade credit ratings.

6.5 Conclusion on Breach-Induced Changes in Cost of Debt

This chapter presented Contribution **C3**, which provided novel empirical evidence on a potentially overlook underlying / consequential cost item elevated by security breaches via an examination of credit market reactions following large-scale security breaches.

This study constitutes the first empirical analysis to document the immediate impact of severe security breaches on CDS spreads following the exposure of a breach. Making use of this more accurate, cleaner, market-near measurement of firms' default risk, it establishes whether successful severe attacks induce (public) debt market participants to alter their credit risk assessments. Positive changes in default risk as proxied by CDS spreads indicate that debt investors require greater returns to compensate them for (perceived) increases in risk, eventually resulting in elevated cost of debt for breached firms.

The results of two analytical approaches examining CDS spread changes around security breach announcements were presented above. First, CDS premia changes adjusted by competitor- and rating category-based portfolios of firms were assessed. The analysis of 75 severe security breaches between 2005 and 2019 revealed the absence of statistically significant abnormal CDS premia increases around security breach announcements. Second, a

[2]As common in practice, firms with market capitalisations exceeding $10bn or $2bn were defined as large- or medium-sized firms, respectively.

[3]See Table J.1 in Appendix J.

quasi-experiment utilising a sample of breached firms as well as non-breached competitors was set up. Regression-based factor models using a sample of 1,724 observations were established controlling for contemporaneous micro- and macroeconomic movements. Similarly, security breaches did not appear to be systematically linked to increases in default spreads in terms of CDS premia. These findings were robust to changes in the considered time periods, outlier treatments, and additional explanatory variables in the empirical models.

Accordingly, the null hypothesis in connection with Contribution **C3**'s central hypothesis, *severe security breaches in publicly listed companies are associated with increased cost of debt, as indicated by short-term abnormal CDS spread changes*, cannot be rejected. In line with previous studies (e.g., by Iyer et al. [307]), the short-term public debt market reaction to severe security breaches is not of statistically significant severity. However, the seemingly obvious "no" to Contribution **C3**'s initial research question *Do severe security breaches increase firms' cost of debt by elevating perceived default risk?* does not come without a caveat, as there might indeed be other factors influencing at-issue observable cost of debt besides default risk considerations.

As delineated in Section 2.8, CDS spreads are a proxy for how risky credit investors deem a firm's debt to be. Overall, the study did not find CDS spreads to react statistically significantly to security breaches. These findings imply that credit market participants, who mainly tend to be sophisticated investors, do not necessarily consider breached firms a greater investment risk. Theoretically, as investors' perception of default risk remains unaltered, their return expectations should not increase, and cost of debt should consequently remain flat. These findings are in line with previous literature demonstrating an absence of significant cost of debt increases on public debt (i.e., bond) markets following security breaches [201, 307]. Nevertheless, prior studies have indeed found statistically significant rises in cost of debt in terms of at-issue private debt (i.e., loan) spreads in more distant time periods (three to four years following a security breach, [201,306]). Contribution **C3** therefore discussed potential reasons as to why public debt markets — on which CDS contracts and bonds are traded — are seemingly indifferent about security breaches whereas lenders such as banks adjust their pricing models upwards beyond default spreads as proxied by CDS premia. Additionally, the potential presence of informed traders in the market anticipating security breach announcements, and the possibility of initial CDS market underreaction, were debated.

This study does not provide sufficient evidence to arrive at a final and conclusive answer as to whether severe security breaches elevate firms' cost of debt generally. Accordingly, these results are not to be understood by the stakeholder value-maximising security executive, who is incentivised and obligated to mitigate negative economic impacts of breaches [17, 18, 76],

as giving them a free pass on potential cost of debt issues. Instead, in conjunction with prior literature (see [201, 307]), the results of this study should act as a reminder that capital market participants do not necessarily always react fully economically rational to new information, and that different types of economic actors and markets might be driven by divergent goals and incentives. Additionally, important conclusions can be drawn to help executives attempting to quantify negative economic breach impacts (λ) for the purpose of Annual Loss Expectancy (ALE_s and ALE_0) calculations in the context of the ENBIS framework.

In terms of the expected costs stemming from security breaches (λ) in the ENBIS calculation, the study verified and extended previous findings ([201, 306, 307]). Specifically, the increase in cost of *private* debt — as observed in terms of at-issue loan interest rate spreads — should be considered as an additional underlying / consequential cost element within the financing costs category in the expected costs vector ($\lambda_{fincosts_{CoD\ loans}} > 0$). In contrast, the absence of an increase in cost of *public or traded* debt — in terms of CDS spreads and bond prices — does not constitute an additional underlying / consequential cost element within the financing cost category to be considered separately ($\lambda_{fincosts_{CoD\ corporate\ public\ debt}} \not> 0$).

Similar to the increase in cost of equity, the potential increase in cost of debt in terms of elevated bank loan spreads has a significant twofold impact on economic benefit of information security investment considerations. First, greater cost of debt can, for instance, lead to project NPV and funding targets not being met, research and development ideas not being pursued, and inventory not being renewed. In this context, $\lambda_{fincosts_{CoD\ loans}}$ has *consequential* cost characteristics, as such negative implications only substantiate indirectly and consequent to a security breach over time. Naturally, the effective $\lambda_{fincosts_{CoD\ loans}}$ figure is thereby dependent on multiple factors such as firm characteristics, access to and relationships with lenders, existing capital structures, tax rates, and macroeconomic market conditions. With an increase in the cost vector ($\lambda_{fincosts_{CoD\ loans}} > 0$) the expected benefit of information security investments (i.e., the difference between ALE_0 and ALE_s) increases. Rational information security executives attempting to quantify the economic impact of information security capital expenditure should therefore include $\lambda_{fincosts_{CoD\ loans}}$ in their considerations. If a given information security investment is effective in that it can mitigate total costs ($\lambda_\Sigma = \lambda_{ab\ initio} + \lambda_{fincosts_{CoD}}$), it is in the best interest of the executive to account for negative economic impacts stemming from elevated cost of debt in their ENBIS calculation process.

Second, all else being equal, greater cost of debt leads to greater cost of capital [58, 82, 105, 110, 111, 157, 216]. As delineated in Section 5.7, cost of capital is a highly relevant figure in the context of information security investment decisions, as it constitutes

the underlying discount rate r used to compute the net present value of security investment opportunities. Put differently, greater cost of debt reduce the NPV of investment projects at hand. Consequently, an investment thesis promoting security controls with strong potentials to reduce the vulnerability of information confidentiality, integrity and availability might end up being discarded as the lowered NPV does not meet a particular threshold. Accordingly, increases in cost of debt can feature *underlying* cost characteristics. Ironically, a particular information security investment project's NPV would ceteris paribus be lower in breached firms relative to ones that did not experience a security breach, potentially leading to security investment opportunities not being pursued.

The rational information security executive should also note that breached firms ought to be particularly mindful of their capital structure generally, and their long- and short-term liability positions particularly, to counteract any cost of capital increases. Breached firms are systematically associated with an increase in leverage (i.e., the proportion of debt finance in their capital structure) [200, 201]. Given the findings presented above indicating economically significant differences between bond and loan markets' reactions to security breaches ($\lambda_{fincosts_{CoD\ loans}} > 0$, but $\lambda_{fincosts_{CoD\ corporate\ public\ debt}} \not> 0$), security executives in breached firms might be incentivised to favour new bond issues as opposed to taking out additional loans.

This study made a number of contributions to the literature. First, it adds to the nascent stream of research on hidden, underlying and consequential costs associated with information security breaches. By highlighting the types of costs that are of (potentially less) concern to corporate decision makers, the results of this study allow information security executives to think holistically and strategically about the net economic benefit of information security investments. The study thereby conduces to the general endeavour to improve information security investment decision-making frameworks and models. In addition, Contribution **C3** furthers the information security economics literature by establishing that well-accepted [26, 30, 170–182] equity markets phenomena might manifest themselves differently on markets for corporate debt. Specifically, the results presented in this chapter add further evidence to the notion that professional (public debt) investors deem the impact of security breaches on default risk to be rather minor. Finally, the study improves the contemporary academic understanding of the CDS market, particularly with regards to its informational efficiency. Given that the market for credit default swaps is still relatively young, there is a less-substantial body of research on market reactions following corporate events relative to the equity market (see e.g., [461]).

Chapter 7
Security Breach Costs: Information Asymmetries

An analysis of changes in insider trading abnormal returns following information security breaches

In this chapter, the results and discussions pertaining to the assessment of changes in insider trading abnormal returns following security breaches are presented. This chapter constitutes Contribution **C4**, a provision of novel empirical evidence of long-term increases in information asymmetries following security breaches that can lead to greater cost of capital and should hence be considered as an underlying / consequential cost item by information security executives.

7.1 Overview

In this dissertation's fourth Contribution **C4**, abnormal returns following executives' buying and selling of shares in breached firms prior and subsequent to security breaches was examined. The study aimed to establish whether severe security breaches are systematically associated with an increase in long-term information asymmetries that can exacerbate cost of capital. To this effect, the following research question was posed: *Do severe security breaches increase firms' cost of capital by elevating information asymmetries in the long run?* The main hypothesis **C4-H1** outlined in Section 2.9 asserted that severe security breaches in publicly listed companies are associated with significant increases in information asymmetries as proxied by insider trading abnormal returns. The sub-hypothesis **C4-H1a** contended that insider purchase transactions, which generally convey greater informational content to the market, exhibit a stronger association between security breaches and information asymmetries measured in terms of insider trading abnormal returns.

Analysing up to 2,088 aggregated insider trades related to 129 severe security breaches from 2005–2019 using the methodology laid out in Section 3.7 showed that on average security breaches are indeed associated with long-term increases in information asymmetries in terms of insider trading abnormal returns. As hypothesised, the effect is prevalent in insiders' Net Buy transactions, which are associated with significant increases in information asymmetries, whereas the information content of Net Sell transactions remains unchanged following security breaches.

In Section 7.2, the empirical results are presented and analysed. First, descriptive results are examined. Then, results obtained from the main regression analysis are explained. Finally, in Section 7.3, the findings' implications for firms' cost of capital, individual insider profits, and costs to society are discussed. Moreover, the overall relevance of these findings from an ENBIS framework perspective are explicated.

In summary, the study found strong support in favour of sub-hypothesis **C4-H1a** and by implication sufficient support confirming the main hypothesis **C4-H1**. The findings establish that severe security breaches are associated with statistically significant increases in information asymmetries as measured by insider trading abnormal returns. The implications of these findings ought to be taken into account by information security executives and regulators.

7.2 Empirical Results Regression Model

Contribution **C4** aimed to demonstrate whether severe security breaches are associated with an increase in firms' cost of capital as indicated by increases in information asymmetries. As delineated in Section 2.9, previous studies have focused on the short-term impact of security breaches on information asymmetries. In order to detect a potential negative effect on cost of capital, however, the long-term impact of breaches on information asymmetries is of greater significance. Changes in insider trading abnormal returns over time periods of up to 24 months provide a strong proxy to measure whether increases in information asymmetries persist beyond the short-term event windows analysed in previous studies presented in [199, 372, 373].

Insider trading abnormal returns indicate the informational value new insider trading filings convey to the market. An insider trade's informational content is greater if there is more uncertainty as to the future value of the underlying firm, i.e., the firm's principal-agent information asymmetries are more substantial. Greater valuation uncertainty leads to elevated investor return requirements [214,222,338,339,341]. A security breach can introduce heightened uncertainties about the breached firm's future ability to generate stable (superior)

economic returns. An increase in post-breach information asymmetries, which would suggest greater return requirements (i.e., greater cost of capital), is therefore likely to emerge.

Due to the repeated observations and multi-year nature of the severe security breaches sample and the insider trades sample, a regression model controlling for changes in other indicators of trades' information content (*Reporting Lag*, *Trade Size*, and *Insider Rank*) and firms' information asymmetries (*Firm Size*, *R&D*, *Loss*, and *Book-to-Market*) was constructed in Section 3.7. The following tables reveal the results of the regression model-based analysis, whereby insider trade-induced three-day cumulative abnormal returns $CAR\ [0, 2]$ are the dependent variable and *Post Breach* is the main independent variable of interest.

Key variables' descriptive statistics are reported in Table 7.2. For each variable minimum, mean, maximum, and standard deviation figures are shown. Two time periods, 18 and 24 months, symmetrically centred on security breaches, were tested hypothesising that on average abnormal returns increase in the post-security breach half of the respective time frame. The ±9 and ±12 samples featured 2,409 (830 Net Buy and 1,579 Net Sell) and 3,256 (1,168 Net Buy and 2,088 Net Sell) aggregated insider trades pertaining to up to 125 and 129 security breaches, respectively. As insiders are awarded with shares as part of remuneration packages and sell such shares due to liquidity needs, the sample sizes for net sales transactions are larger across both time periods. For the same reason, Net Sell subsamples are larger than Net Buy ones for transactions in which a Top 20 executive was involved (i.e., $Insider\ Rank = 1$).

Unsurprisingly, there is little cross-subsample variation in firm size and book-to-market ratio, given that all time periods as well as Net Buy and Net Sell samples relate to the same severe security breaches and hence firms. The ratio of aggregate transactions in firms reporting R&D expenses divided by the total number of transactions is larger than 0.5 for Net Buy and smaller than 0.5 for Net Sell transactions. This is in line with the expectation that insiders in R&D-intensive firms capitalise on their superior knowledge of R&D projects' progress and success [408]. Similarly, Net Buy transactions in firms reporting losses appear to be less frequent than Net Sales transactions in such firms, indicating that insiders tend to be net sellers in loss-making firms. Reporting lags are on average longer in the case of Net Sell transactions, which might stem from insiders' attempts to delay divulging the negative information to the market.

Considering the dependent variable, insider trading cumulative abnormal returns, descriptive statistics provide some inconclusive indications. First, levels of both Net Buy and Net Sell insider trading abnormal returns are in line with previous literature (e.g., [384]). Comparing average nine-month pre-breach Net Buy $CAR\ [0, 2]$ to nine-month post-breach ones reveals that abnormal returns increased (i.e., got more positive) by 0.031 percentage

Table 7.1: Insider Trading [0, 2] CAR — Regression Model Descriptives

	n	Min	$Mean$	Max	SD
Unique Security Breaches					
9 mts - buy	109				
9 mts - sell	125				
12 mts - buy	116				
12 mts - sell	129				
CAR [0,2]					
9 mts - buy pre-breach	408	-4.877	0.192	4.609	2.365
9 mts - buy post-breach	422	-4.877	0.223	4.609	2.347
9 mts - sell pre-breach	779	-4.877	-0.208	4.609	2.248
9 mts - sell post-breach	800	-4.877	-0.097	4.609	2.352
12 mts - buy pre-breach	577	-4.863	0.245	4.661	2.387
12 mts - buy post-breach	591	-4.863	0.251	4.661	2.490
12 mts - sell pre-breach	1,033	-4.863	-0.187	4.661	2.239
12 mts - sell post-breach	1,055	-4.863	-0.145	4.661	2.293
Firm Size					
9 mts - buy	830	6.122	9.316	12.890	1.954
9 mts - sell	1,579	6.122	9.228	12.890	2.009
12 mts - buy	1,168	6.047	9.232	12.882	1.984
12 mts - sell	2,088	6.047	9.249	12.882	1.998
R&D = 1					
9 mts - buy	475				
9 mts - sell	751				
12 mts - buy	661				
12 mts - sell	995				
Loss = 1					
9 mts - buy	102				
9 mts - sell	224				
12 mts - buy	169				
12 mts - sell	294				
Book-to-Market					
9 mts - buy	830	0.066	0.333	1.012	0.278
9 mts - sell	1,579	0.066	0.367	1.012	0.261
12 mts - buy	1,168	0.069	0.339	0.988	0.273

Table 7.1 continued from previous page

	n	Min	$Mean$	Max	SD
12 mts - sell	2,088	0.069	0.364	0.988	0.252
Reporting Lag					
9 mts - buy	830	0.000	1.079	1.792	0.462
9 mts - sell	1,579	0.000	1.180	1.792	0.459
12 mts - buy	1,168	0.000	1.082	1.792	0.462
12 mts - sell	2,088	0.000	1.178	1.792	0.453
Trade Size					
9 mts - buy	830	0.693	9.355	11.334	1.619
9 mts - sell	1,579	-11.891	-9.095	-2.197	1.801
12 mts - buy	1,168	0.000	9.433	11.550	1.656
12 mts - sell	2,088	-11.953	-9.135	-2.079	1.830
Insider Rank = 1					
9 mts - buy	631				
9 mts - sell	1,335				
12 mts - buy	843				
12 mts - sell	1,747				

Note: n = (sub-)sample size of aggregated insider transactions; Min = Minimum; Max = Maximum; SD = Standard Deviation; mts = months before and after a security breach (i.e., covering time periods of 18 or 24 months around security breaches). CAR [0,2] is in percentage terms. Number of unique security breaches included for reference. See Section 3.7 for variable definitions. Same Min and Max values across subsamples are due to winsorising on higher levels of aggregation.

points or 16.146%. The same comparison for the twelve-month pre- and post-breach abnormal returns reveals an average increase of 0.006 percentage points or 2.449%. However, considering Net Sell transactions over the same time periods shows an average decrease in (i.e., less negative) abnormal returns of 0.111 and 0.042 percentage points (i.e., -53.365% and -22.460%), respectively.

Note that these average changes do not control for other contemporaneous shifts in information asymmetries as accounted for by the relevant variables in the regression model. Results obtained from running four independent regressions on Net Buy and Net Sell transactions for 18- and 24-months periods are shown in Table 7.2. Each model predicts the dependent variable, insider trading cumulative abnormal returns, as a function of the independent dummy variable, post-security breach, and multiple control variables. The coefficients indicate the strength of the relationship between the respective variable and cumulative abnormal returns in the [0, 2] aggregation period. Clustered standard errors are presented

Table 7.2: Insider Trading [0, 2] CAR — Net Buy and Sell Transactions Long Term

	Dependent variable:			
	[± 9 months]	[± 9 months]	[± 12 months]	[± 12 months]
	Net Buy	Net Sell	Net Buy	Net Sell
	(1)	(2)	(3)	(4)
Post Breach	3.253***	0.232	2.507***	0.372
	(1.191)	(0.643)	(0.852)	(0.528)
Firm Size	−0.952*	−1.568**	−0.749	−1.422***
	(0.520)	(0.644)	(0.500)	(0.460)
R&D	2.030*	−0.984	3.263***	−1.567***
	(1.065)	(1.131)	(0.987)	(0.284)
Loss	1.132**	−0.527**	0.324	−0.459**
	(0.566)	(0.248)	(0.580)	(0.225)
Book-to-Market	0.309	0.656	0.751	0.623
	(1.061)	(1.154)	(0.868)	(1.086)
Reporting Lag	−0.064	−0.231*	−0.250*	−0.214*
	(0.194)	(0.138)	(0.145)	(0.113)
Trade Size	0.138	0.023	0.191***	0.040
	(0.100)	(0.050)	(0.071)	(0.040)
Post Breach X	−0.325	0.016	−0.244	0.033
Trade Size	(0.128)	(0.070)	(0.090)	(0.058)
Insider Rank	−0.378	0.237	−0.333	0.353**
	(0.277)	(0.201)	(0.258)	(0.159)
Firm-fixed Effects	Yes	Yes	Yes	Yes
Year-fixed Effects	Yes	Yes	Yes	Yes
Constant	5.350	10.261**	3.780	10.372***
	(3.978)	(4.656)	(4.282)	(3.549)
Observations	830	1,579	1,168	2,088
R^2	0.217	0.097	0.172	0.084
Adjusted R^2	0.091	0.018	0.077	0.023
Residual Std. Error	2.245 (df = 714)	2.280 (df = 1,451)	2.343 (df = 1,047)	2.240 (df = 1,956)
F Statistic	1.722*** (df = 115; 714)	1.233** (df = 127; 1,451)	1.811*** (df = 120; 1,047)	1.370*** (df = 131; 1,956)
Note:				*p<0.1; **p<0.05; ***p<0.01

in parentheses. As customary, statistical significance and trends are accepted and discussed at p-values of less than 0.05 and less than 0.1, respectively. Note that for Net Buy models, positive coefficients indicate that insider trading abnormal returns become greater (i.e., more positive) with an increase of the respective regressor; whereas for Net Sell models, negative coefficients indicate that insider trading abnormal returns become greater (i.e., more negative) with an increase of the respective regressor.

All four models can be regarded as being overall-significant as per the F-Test of Overall

Significance, rejecting the null hypothesis that considering all regressors jointly does not explain variation in the dependent variable. The adjusted R^2 for Net Sell models is in line with Brochet [470], who assessed changes in the information content of insider trades before and after the introduction of the Sarbanes-Oxley Act. For Net Buy models, the adjusted R^2 is actually substantially greater, indicating that regression models accounting for security breaches explain a relatively large proportion of the variance in Net Buy insider trading abnormal returns.

As hypothesised, the main coefficient of interest, *Post Breach*, is positive and significant for Net Buy transactions across both time periods considered. Specifically, the coefficient in Model (1) indicates that in the nine months following a security breach, ceteris paribus, Net Buy insider trading *CARs* on average increase by 3.253 percentage points relative to the nine months before the breach. Similarly, the coefficient in Model (3) indicates that in the twelve months subsequent to a security breach, ceteris paribus, Net Buy insider trading *CARs* become on average 2.507 percentage points greater relative to the twelve months-period prior to the breach.

Considering the pre- and post-breach Net Sell mean cumulative abnormal returns in Table 7.2, it was already possible to deduce that the coefficient would not be negative as hypothesised. The positive coefficients in Models (2) and (4) signify that on average abnormal returns after insiders' Net Sell transactions decrease, i.e., they become less negative. However, these positive coefficients are not statistically significant, indicating that ceteris paribus, Net Sell abnormal returns do not change significantly after security breaches.

The negative coefficients for *Firm Size* in Models (1) and (3) are in line with previous research [372,396,397,408,472], but not statistically significant. The non-positive coefficients in Models (2) and (4) are counterintuitive as they indicate that with increasing firm size, and hence greater media and analyst coverage, Net Sell abnormal returns become more strongly negative.

All coefficients for *R&D* and *Loss* are of the expected direction (see [408, 470]). In Models (1), (3), and (4), the *R&D* coefficients indicate that insider trades in firms with R&D-intensive strategies attract greater (i.e., more positive for Net Buy and more negative for Net Sell transactions) cumulative abnormal returns. The *Loss* coefficients in Models (1), (2), and (4) show that firms reporting losses are associated with greater insider trading abnormal returns (i.e., more positive returns following Net Buy and more negative ones following Net Sell transactions). The *Reporting Lag* variable only exhibits statistical trends, indicating negative associations between an increase in filing delay and cumulative abnormal returns.

As predicted, the significant and positive *Trade Size* coefficient in Model (3) indicates that larger aggregated Net Buy transactions lead to greater abnormal returns. The interac-

tion term *Post Breach X Trade Size* does not exhibit statistically significant coefficients, meaning that the associated null hypothesis (i.e., larger trades do not carry greater informational value following a security breach) cannot be rejected. Unexpectedly, the *Insider Rank* coefficient is only significant and positive in Model (4), suggesting that top executives' Net Sell trades may be associated with less negative abnormal returns.

The regression results are similar across the two pre-/post-breach trading time periods and qualitatively robust to altering the dependent variable's aggregation time periods (i.e., *CARs* $[-1, 0]$, $[-1, 1]$, $[-1, 2]$, $[0, 0]$, and $[0, 1]$). Overall, the four models presented in Table 7.2 indicate that following security breaches, Net Buy insider transactions generate greater abnormal returns relative to the pre-breach period, whereas Net Sell insider transactions' abnormal returns do not change statistically significantly in the nine and twelve months following security breaches.

7.3 Discussion of Empirical Results

The motivation for Contribution **C4** stemmed from a gap in the literature pertaining to long-term changes in information asymmetries following security breaches that can compound firms' cost of capital. Previous studies found that security breaches are associated with short-term increases in information asymmetries as proxied by bid-ask spreads and trading volumes [199,372,373]. However, there is no previous evidence as to whether such heightened information asymmetries also manifest in the long-run following security breaches.

The study presented in this dissertation is the first analysis on long-term changes in information asymmetries as proxied by *CARs* induced by filings of insider trades. Insider trading abnormal returns constitute a suitable measurement of information asymmetries as they provide a direct indication of the value investors place in new information releases pertaining to the underlying firm and thereby reveal discrepancies in levels of information between knowledgeable agents and ill-informed principals. Moreover, whilst bid-ask spreads — a typical proxy for information asymmetries in previous academic studies — constitute a market maker-based measurement, insider trading abnormal returns are market-based. *CARs* are an indication of market participants' aggregate assessment of insider filings' information content, whereas bid-ask spreads mainly measure liquidity provision and feature substantial non-information components. In this section, the results' implications for security researchers and practitioners are discussed.

In summary, the regression results presented in Section 7.2 established a statistically significant post-breach increase in long-term information asymmetries as proxied by insider trading abnormal returns. The evidence is robust to changes in the empirical set-up, such

as changes to the cumulative abnormal returns aggregation time period. The results also demonstrated that significant increases in post-breach insider trading abnormal returns occur predominantly in the case of Net Buy transactions, whereas Net Sell transactions' abnormal returns remain unchanged following a breach.

Stock prices provide a reflection of investors' expectations of discounted future cash flows (see [82, 105]), whereby according to Fama's [108] Efficient Market Hypothesis, prices adjust to all newly issued information and events. Abnormal returns (i.e., unexpected movements in stock prices) are a manifestation of market participants' reactions to previously unknown information that influence investors' pricing process. The level of abnormal returns is thereby a direct indication of an event's information content. If investors ascribe more importance to a new piece of knowledge, abnormal returns become greater and vice versa.

The public filing of insider trades provides outside investors with an instrument to garner insights into executives' assessments of firms' prevailing stock prices relative to their respective fair values, which facilitates investors' price discovery process [39, 384–388]. Executives, who possess superior knowledge and sentiments as to their firms' future performance, tend to be net buyers, or net sellers, of their firms' stock if they deem current stock prices to be undervalued, or overvalued, respectively. Insider trading abnormal returns, the (cumulative) abnormal returns following insider trading filings, indicate the information content conveyed to market participants through insiders' buying or selling activities [383, 386, 386, 389, 389–393, 402–410].

Most importantly, as outsiders gain more knowledge from insider trades if information about the underlying firm is otherwise scarce, vague, or uncertain, insider trading abnormal returns are an indirect proxy of information asymmetries between outside investors and corporate insiders. Put simply, the greater the ex-ante principal-agent information asymmetries between outside investors and corporate insiders are, the greater the informativeness of aggregated insider trades is, and in turn, the more substantial the abnormal returns following the filing of insider trades become.

The finding that Net Buy post-breach insider trading abnormal returns increase significantly, whilst Net Sell ones do not change statistically meaningfully, accordingly signifies that insider trades' information content heightens as information asymmetries intensify after severe security breaches. The null hypothesis in connection with main hypothesis **C4-H1**, asserting that severe security breaches in publicly listed companies are associated with significant increases in information asymmetries as proxied by insider trading abnormal returns, can hence be rejected.

The finding is in line with intuition and previous literature. Quantifying the (long-term) impacts of security breaches is difficult generally, but even more challenging for outside

investors who do not have access to full information. Breached firms' executives on the other hand are likely to be briefed in detail on negative economic consequences of security breaches by internal and external experts. Outside investors' lack of access to the same information quantity and quality exacerbates situations of relative information scarcity. This disparity in knowledge does not only elevate investor uncertainty — which is likely to play a role in short-term slumps in breached firms' equity value (see [26, 30, 170–182]) — but also accentuates market participants' quest for information dilemma.

Besides the adverse selection issues caused by limited access to information, outside investors are also faced with moral hazard problems as security executives and other top managers can hide their post-breach activities, which is further exacerbated by a general post-breach reduction in trust (see [30, 423–427]).

Moreover, even if (security) executives in breached firms act in the best interest of shareholders and intend to deploy effective breach remediation strategies, principal-agent information asymmetries might intensify anyway. Strategies that are unique, novel, unknown, untested, or otherwise less straightforward to understand are generally associated with greater information asymmetries as evidenced by elevated insider trading abnormal returns [37]. Remediation strategies to mitigate negative economic consequences from severe security breaches inherently fall into the aforementioned category of strategies due to the infrequent nature of severe breaches. Executives lack a standard approach and the experience in executing such strategies effectively. Post-breach business and corporate strategies are hence prone to be unique, novel, and difficult-to-analyse, and rises in information asymmetries/insider trading abnormal returns are hence to be expected.

As a result, investors have a heightened interest in all pieces of information that may help them evaluate the future performance of the underlying firm, which is in line with the theoretical argument that sensitivity to price-relevant news increases with greater information uncertainty [510]. Accordingly, levels of (perceived) principal-agent information asymmetries exacerbate and insider trades, particularly insider Net Buy transactions, consequently convey greater information content to the market.

Insiders' Net Buy transactions are generally expected to be associated with greater abnormal returns than their Net Sell transactions [391,396,410], as in order to increase holdings in their firms' stock, executives need to spend personal funds. Outside investors hence expect insiders' net purchases to be based on superior information or estimations. In contrary, as their remuneration packages already tend to feature large equity-based proportions, insiders regularly sell large numbers of shares due to liquidity needs. As insider sales are not necessarily motivated by insiders' perception of overpricing, but rather often liquidity needs-based, Net Sell transactions do not convey as much information content to the market as

Net Buy transactions do [391,396,410]. In line with this logic, Brochet's [470] analysis of the informational value of insider trades before and after exogenous events also showed that only abnormal returns after insider purchases became greater following the event, whilst insider sales abnormal returns did not become more negative. As Net Buy transactions are more informative generally, it is not surprising that the informativeness of Net Buy transactions increases significantly following security breaches, whilst Net Sell transactions do not exhibit the same phenomenon.

The finding that information asymmetries increase in the medium- to long-run following severe security breaches carries three major implications pertaining to firms' cost of capital, insider gains, and costs to society.

First and foremost, as delineated in Section 2.5, exacerbated information asymmetries introduce frictions to market participants' valuation and investment risk assessment processes, create adverse selection issues, and eventually increase investors' return requirements and accordingly cost of capital for the underlying firm (see [112, 113, 214, 217, 218, 220–223, 284, 338, 339, 342, 342–350]). The positive correlation between investor-manager information asymmetries and financing costs in the context of this study's finding that severe security breaches are associated with an increase in medium- and long-term information asymmetries allows for an answer of **C4**'s research question *Do severe security breaches increase firms' cost of capital by elevating information asymmetries in the long run?*.

Based on the results presented above and the refutation of the null hypotheses in connection with hypotheses **C4-H1** and **C4-H1a**, it can be conjectured that severe security breaches in publicly listed companies increase firms' cost of capital by introducing elevated uncertainty and information asymmetries that persist beyond the short-term impact of a breach announcement event. The finding that severe security breaches are associated with significant increases in information asymmetries is thereby in line with previous studies that established positive shifts in terms of trading volumes and bid-ask spreads [199, 372, 373].

The effect size of security breach-induced increases in information asymmetries established in Table 7.2 can be considered economically significant. The results imply that relative to the hypothetical scenario in which the underlying firm had not been breached, on average breached firms' information asymmetries in terms of insider trading Net Buy $CARs$ increase by 3.253 percentage points and 2.507 percentage points in the nine and twelve months after a security breach relative to the same time periods before a breach, respectively. Whilst these surges do not directly translate into increases in cost of capital of the same 2.5–3.3% magnitude, they are nevertheless large enough to potentially affect investors' risk-adjusted return requirements and hence cost of capital.

Within the cost of capital framework depicted in Figure 2.1, information asymmetries

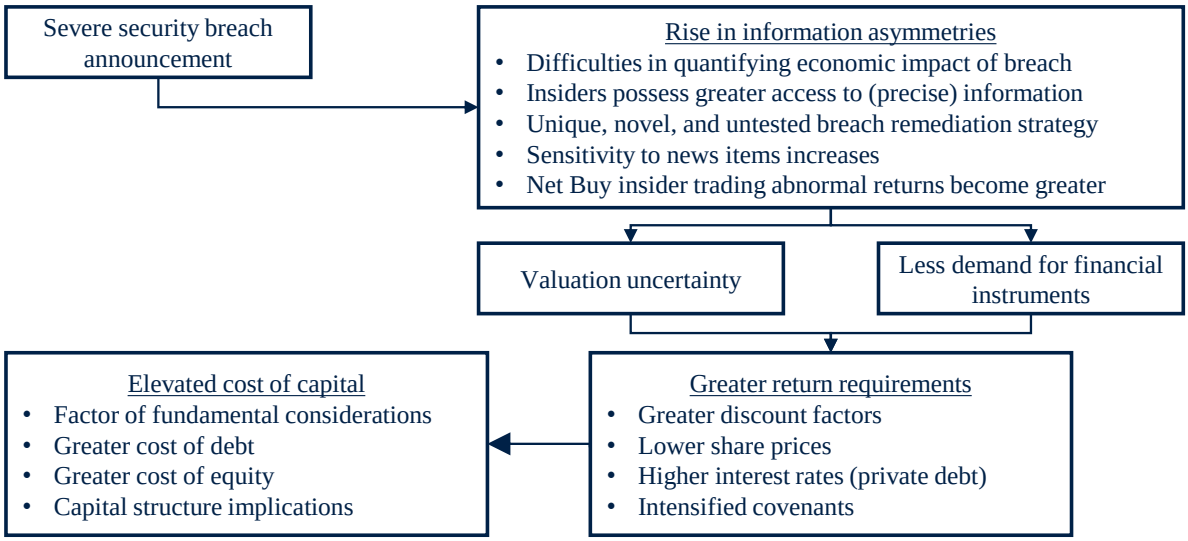


Figure 7.1: Overview Information Asymmetries and Financing Costs

are a constituent of financing costs' fundamental considerations that management ought to take into account alongside optimal capital structure considerations to achieve the lowest possible financing costs. Elevated risk-adjusted return requirements due to heightened information asymmetries thereby pertain to equity as well as debt investors. The discussions of implications arising from greater cost of equity and cost of debt following security breaches in Sections 5.7 and 6.4 therefore also apply here.

An increase in information asymmetries and investors' valuation uncertainty ceteris paribus leads to rising cost of capital, particularly if the precision of private information is high whilst the precision of public information is low (see [221]), which is often the case in security breach scenarios. In extreme cases, firms that already operated under constrained financing conditions before a security breach might no longer be able to pursue potentially profitable capital expenditure projects. In the context of information security investments, lower project net present values caused by greater discount factors might dissuade executives from investing in information security projects (see [22, 110, 157]). All other things being equal, rising financing costs elevate discount factors applied to firm valuations, potentially resulting in breach-induced information asymmetry surges causing lower share prices (see [58, 82, 105, 110, 111, 216]). Figure 7.1 provides an overview of the findings and implications for financing costs explained above.

Given the severe implications of heightened post-breach information asymmetries for cost of capital and capital structure considerations, executives in breached firms ought to increase quantity and quality of information disclosure to the market. An improved focus on capital

market communication should thereby focus on the immediate remediation of the underlying breach. From a purely information asymmetries-motivated perspective, it is possible to argue that even the release of bad news (e.g., actual amounts spent on compensation payments to customers and fines paid to regulatory institutions, or estimations of lost revenue) would foster a better information environment, which is likely to be beneficial for financing costs.

Another implication of the findings presented above pertains to gains insiders generate from their trading filings. Previous literature provided evidence that insiders trade on their knowledge of imminent security breach announcements and avoid incurring losses on their stockholdings [337, 413–419]. The results of this study imply that insiders may benefit from their private knowledge of security breaches and the severity of any negative economic repercussions not only before, but also subsequent to a security breach. Insiders tend to reverse their prior trades to realise profits particularly after stronger abnormal returns [511]. It is hence reasonable to expect that the increase in post-breach purchasing abnormal returns, combined with the absence of the same effect for post-breach selling abnormal returns, motivates insiders to realise gains more frequently by selling recently acquired shares after shorter holding periods.

Following a security breach, insiders may accordingly realise greater personal profits from their trades. In 2018, in reaction to insiders potentially trading on their knowledge of security issues and breaches — and at least partially in response to insider trades in connection with the 2017 Equifax security breach and the 2018 Intel chip vulnerabilities Spectre and Meltdown [420–422] — the United States Securities and Exchange Commission (SEC) issued a new guideline specifying that knowledge of security breaches may constitute material non-public information [337]. Based on the implications of this present study's findings, legislators intending to reduce insiders' ability to profit from material non-public information might be inclined to consider imposing limits not only on insiders' pre-breach but also post-breach trading activities.

A third implication of this study's findings is that security breaches also bring with them further underlying / consequential costs to society in general. Economic market participants — who are in a constant state of non-satiation of cash flow-relevant information — who are presented with additional breach-induced information asymmetries are likely to spend more time gathering and analysing additional information on the underlying firm. Due to resource scarcity, investors may therefore have less time and funding available to subject other firms to in-depth examinations. Accordingly, increases in information asymmetries following severe security breaches in one firm can have economy-wide implications by introducing additional frictions and reducing capital market efficiency generally[1].

[1]It is, however, worth noting that there are some proponents of insider trading who contend that insider

The study and resulting implications are subject to some limitations. First, changes in information asymmetries as proxied by insider trading abnormal returns were only considered in time periods of up to 24 months, centred on security breach announcements. The study showed that information asymmetries increase following a security breach. The mechanism and speed of how (quickly) information asymmetries translate into greater cost of capital was, however, not analysed in this study. The direct connection between this measure of uncertainty and elevated investor return requirements resulting in heightened financing costs can hence only be assumed based on previous theoretical and empirical research. Future studies are needed to examine longer post-breach time periods and establish more direct correlations between measures of asymmetrical levels of information and post-breach financing costs.

Second, the regression-based model explicitly controls for transaction- and firm-level indicators of trades' information content (*Reporting Lag*, *Trade Size*, and *Insider Rank*) and firms' information asymmetries (*Firm Size*, *R&D*, *Loss*, and *Book-to-Market*). Moreover, by including firm- and year-fixed effects, the study also controls for other characteristics time invariant within firms and ones that are constant on firm-level but varying over time. However, the study does not account for differences across security breach attributes and executives' handling of security breaches. The first issue was partially addressed by creating a relatively homogenous sample of severe security breaches[2]. Firms' breach management, which was not included in the study, might be of particular relevance to the topic of post-breach information asymmetries. Previous research showed that firms can mitigate the negative stock price impact of privacy breach disclosures by strategic news bundling [180] and voluntary disclosures [512–515][3]. It is therefore likely that proactive information management — e.g., more frequent or detailed information publications, contracting external PR advisors, or extending earnings call conferences to increase stakeholder engagement and transparency — alleviates some of the information burden introduced by security breaches as well.

trading filings actually contribute to price discovery efficiency as investors learn new information by means of filing publications [384].

[2]See Section 3.2 for explanations of the term severe security breaches and how the sample was constructed.

[3]More frequent voluntary disclosures (on information security issues and mitigation) alleviate information asymmetries by reducing analysts' costs of obtaining information which can be associated with greater market values [512–517].

7.4 Conclusion on Breach-Induced Changes in Information Asymmetries

In this chapter, novel empirical evidence on changes in information asymmetries following security breaches was established. Contribution **C4** thereby introduces another underlying / consequential cost item exacerbated by severe breaches that is potentially overlooked by executives.

The study of up to 2,088 net-aggregated insider trades related to 129 severe security breaches provided the first empirical analysis of long-term changes in information asymmetries following security breaches. Using insider trading abnormal returns as a proxy for information asymmetries, the study revealed that breaches are associated with statistically significant increases in insider trading Net Buy abnormal returns and statistically insignificant changes in Net Sell abnormal returns.

As insider trading abnormal returns are a direct indicator for the underlying filings' information content, an increase in $[0, 2]$ $CARs$ suggests that directors' trades become more informative for outside market participants subsequent to a breach. Given the inverse relationship between a firm's ex-ante information environment quality and insider trading events' abnormal returns, greater $CARs$ are a well-accepted proxy for elevated information asymmetries. Consequently, insider filings being ceteris paribus more informative to outsiders subsequent to security breaches signifies greater levels of principal-agent information asymmetries. The finding that security breaches exacerbate information asymmetry issues is in line with previous studies that analysed short-term information asymmetry surges in terms of stock liquidity [199, 372, 373].

The finding that security breaches are associated with greater information asymmetries implies that investors feel more uncertain about the prospects of the underlying firm. Greater uncertainty leads to investors demanding higher levels of risk compensation (i.e., return requirements). Consequently, security breaches can lead to increases in cost of capital. The null hypothesis in connection with main hypothesis **C4-H1** can therefore be rejected, and the related research question *Do severe security breaches increase firms' cost of capital by elevating information asymmetries in the long run?* can reasonably be answered in the affirmative. This implication is particularly relevant for stakeholder value-maximising security executives[4].

A rational security executive analysing potential investments in information security from an ENBIS perspective is incentivised to quantify and mitigate negative economic impacts (λ)

[4]See [17, 18, 76, 77] for the notion of stakeholder value-maximising executives mitigating negative cash flows and investing in the most economically efficient way.

to minimise the Annual Loss Expectancy (ALE_s) at given investment costs (c). Considering only obvious breach costs might lead to severe underestimations of the true negative economic consequences stemming from security breaches. To this end, Contribution **C4** provides an important additional perspective on underlying / consequential costs to the information security economics literature and managerial practice.

Specifically, this study presented evidence that issues of investor uncertainty and asymmetric access to information exacerbate following a security breach, which leads to greater return requirements and accordingly cost of capital. The underlying / consequential cost element should thus be recognised in the expected cost vector in terms of an increase in financing costs ($\lambda_{fincosts_{Info\ Asymmetries}} > 0$). In practice, an increase in information asymmetries does not necessarily translate into a rise in financing cost of the same percentage value. In order to quantify the eventual effect on cost of capital, security executives would need to examine how previous shifts in information asymmetries (e.g., following the announcement of other operational risk incidences) converted into elevated financing costs.

Chapters 5 and 6 thematised the impact of severe security breaches on cost of equity and cost of debt separately. As information asymmetries constitute an element of fundamental consideration as per the cost of capital framework depicted in Figure 2.1, elevated levels of perceived informational disadvantages can affect the pricing and terms of both types of financing sources. Moreover, information asymmetries are decisive for a firm's capital structure, i.e., the mixture of debt and equity financing [112, 113, 223], which in and of itself carries implications for a firm's WACC. In this context, given that information asymmetries are at the very basis of all financing-related decisions and activities, the cost element $\lambda_{fincosts_{Info\ Asymmetries}}$ is of truly *underlying* nature.

Moreover, information asymmetries are of relevance for both investors' at-issue and post-issue considerations. At the inception of a financial instrument, information asymmetries can affect the intensity and cost of monitoring, due diligence, and covenants (see e.g., [518, 519] for the influence of information asymmetry on private debt issuances or [520] for information asymmetry in the context of IPOs). Later on, during the life of a financial instrument, stocks associated with greater information asymmetries are traded at discounts (see [521]). Given that the cost element $\lambda_{fincosts_{Info\ Asymmetries}}$ is likely to affect financing costs not only immediately after a security breach, but also potentially in the long-term, for instance, in terms of depressed share prices, it also features distinct *consequential* characteristics.

In line with the cost elements examined in previous chapters, executives interested in holistically quantifying the positive economic consequences of security investments ought to include $\lambda_{fincosts_{Info\ Asymmetries}} > 0$ in the ENBIS cost vector to emphasise the expected benefit of information security investments (i.e., $ALE_0 - ALE_s$) if a given security investment

opportunity is indeed effective in mitigating total costs λ. Such considerations should also include the potential follow-on costs incurred to remedy increases in information asymmetries (e.g., PR advisor expenses and intensified information disclosure expenses).

Overall, Contribution **C4** adds to the literature in multiple ways. First, it contributes new empirical evidence to the nascent field of research on underlying / consequential costs by demonstrating long-term surges in information asymmetries that can affect firms' cost of capital. It thereby conduces to the wider endeavour of improving rational security investment decision making and extends existing frameworks and models, particularly in terms of the ENBIS equation. More generally, the study provides relevant insights for the wider financial economics and accounting community concerned with market efficiency (see e.g., [438] for a contemporary survey of empirical stock market efficiency literature) and insider trading (see e.g., [384, 386, 389, 391, 394–398, 400–410] for related studies on firm characteristics and events in the context of insider trading abnormal returns). Contribution **C4** also offers valuable insights to practitioners. Information security executives might want to consider additional (financing) costs introduced by elevated information asymmetries in their investment decision-making frameworks. Policy makers might be more inclined to strengthen the regulation of insider trading around security breaches due to insiders' potential ability to generate greater individual short-term profits from their trades.

Chapter 8
Conclusion

This chapter provides a summary of the findings and implications of the studies presented in Chapters 4– 7, integrates them to conceptualise a more comprehensive ENBIS framework and the Iceberg Model of Information Security Costs, and outlines limitations and potential avenues for future research. Based on the empirical contributions of this thesis, this chapter thereby presents an overall unifying discussion and addresses the overarching research question.

Some deliberations on contributions, impacts, and potential future research directions in this chapter are based on **MP1** [1] and **MP2** [2].

8.1 Contributions & Implications

This section presents the twofold overarching contribution: (a) the provision of novel underlying / consequential cost elements and (b) the introduction of a new information security cost model, based on the empirical insights in Chapters 4– 7 and the novel cost classification introduced in Section 2.4. Whilst the overarching contribution is naturally of relevance to academic theorising and research, it also conduces to the practice-oriented perspective of this dissertation, whose main beneficiaries — publicly listed firms and their (security) executives — can apply the insights presented here to further their objectives and strategies.

8.1.1 Empirical Contributions

The starting point of this dissertation was information security researchers' and practitioners' necessity to think strategically about investments intended to mitigate operational risk, arising from information security threats and potential impacts on firms' assets and objectives, and to deploy scarce economic resources in the most economically efficient way. In order to minimise information security risk whilst maximising shareholder value, information security investment models to guide decision-making processes are needed. The Expected

Net Benefit of Information Security (ENBIS) framework is thereby one suitable tool for multiple groups of stakeholders.

In order to conduct holistic cost-benefit analyses and make effective use of the ENBIS framework in their investment decision-making process, executives need to be aware of all underlying cost and benefit elements. Due to difficulties in observing and measuring indirect or non-obvious costs, previous literature and practice typically focused on (direct) obvious costs. Indirect costs have been given less attention in the information security economics literature, even though such costs may actually exceed direct costs in gravity [26–30]. This is particularly true in the case of — what in this dissertation has been termed — *underlying and consequential costs*. Being aware of underlying / consequential costs is thereby the first step towards better-informed investments in information security controls, as only once breach-induced costs are known, the resulting benefit of mitigating them can be calculated. To promote a more holistic perspective on information security costs, and to facilitate security investments, the overarching research question *How can publicly listed firms leverage financial market data to achieve a better understanding of costs associated with information security to conduct more thorough information security investment cost-benefit analyses?* was posed.

In Chapter 2, previous conceptual and empirical literature was presented and the term underlying and consequential costs was explained in further detail. The ensuing empirical analyses in this dissertation then focused on four underlying / consequential cost elements that all affect financing costs, a highly important metric for for-profit firms.

Contribution **C1** in Chapter 4 approached the topic of financing costs in the information security investment context from an internal financing perspective. In order to answer the research question *Are corporate investments in security certificates associated with value destruction (i.e., hidden underlying / consequential costs) or creation (i.e., secondary benefits or negative underlying / consequential costs) as evidenced by stocks' abnormal returns?*, cumulative abnormal returns following security standards certifications were analysed. Examining abnormal returns following 145 Cyber Essentials awards between 2014 and 2018, and 76 ISO/IEC 27001 certifications between 2001 and 2018, the research found that investments in ISO/IEC 27001 certificates are associated with consequential costs in the form of equity value destruction, whilst the award of Cyber Essentials (Plus) certificates carries negative costs, or secondary benefits, in the form of equity value creation. These short-term firm value implications can be interpreted as evidence that ISO/IEC 27001 and Cyber Essentials investments lead to higher and lower cost of capital, respectively.

In Chapters 5 and 6 an external financing perspective on post-breach cost of capital was taken. Contribution **C2** presented in Chapter 5 thematised breach-induced increases in financial systematic risk by finding answers to the research questions *Do severe security*

breaches increase firms' cost of equity by elevating systematic risk? and *Do severe security breaches affect firms' cost of equity differently in bearish and bullish markets by affecting downside and upside risk differently?*. As hypothesised, the study of 202 severe security breaches between 2005 and 2019 found that breaches are associated with significantly positive increases of systematic risk and systematic downside risk in terms of regular and downside beta, respectively. Contribution **C2** accordingly introduced novel empirical insights into persistent positive changes in cost of equity following security breaches.

The study in Chapter 6, which gave rise to Contribution **C3**, was the first to demonstrate empirical evidence on the effect of security breaches on what arguably constitutes the most relevant and accurate reflections of market participants' cost of debt assessments: credit default swap (CDS) spreads. The chapter worked towards an answer of the research question *Do severe security breaches increase firms' cost of debt by elevating perceived default risk?* by hypothesising the presence of short-term abnormal CDS spread changes following severe security breaches. However, the study did not establish such effects across the 75 severe security breaches for which CDS data was available, neither in the rating-matched portfolio analysis nor in the regression-based model controlling for various contemporaneous micro- and macroeconomic changes. Contribution **C3** hence provided further support to the notion that more sophisticated public debt market investors are less sensitive to security breach announcements than private debt and equity market participants.

The research undertaken in Chapter 7 for Contribution **C4** was the first to examine long-term changes in insider trading abnormal returns around security breaches. Motivated by the review of extant literature and recent high-profile pre-breach insider trading cases, the research question *Do severe security breaches increase firms' cost of capital by elevating information asymmetries in the long run?* was posed. Studying long-term changes in information asymmetries as proxied by insider trading abnormal returns in Chapter 7 suggested that breaches exacerbate adverse selection and moral hazard agency problems. Investors are presented with greater uncertainty regarding breached firms' cash flows, risk-appropriate discount rates, and breach remediation strategies.

8.1.2 Methodological Contributions

Besides the major empirical contributions delineated above, which coalesce into the model described below, this dissertation also made a number of methodological contributions to the information security economics literature.

First, not only are security breaches' likelihood, impact, and organisational resilience difficult to quantify [188–190], but a general lack of high-quality security breaches data

available for researchers to analyse further compounds this problem (see [158, 435, 436]). One part of the data availability problem is that not all security breaches get discovered, and out of the ones that are actually discovered, not all are reported appropriately. The other issue for researchers and practitioners is that no two breaches are perfectly alike, as there is a substantial variance in security breach features and characteristics. Moreover, when conducting financial markets-driven research, narrowing down lists of security breaches and attributing them to underlying (publicly listed) firms is not without complexity either.

Chapter 3.2 described how a new hand-picked sample of — what is referred to as — severe security breaches in publicly listed firms based on the PRC database was created. Looking up ownership structures of breached firms manually on *S&P Capital IQ*, filtering out indirect subsidiaries, and applying a qualitative approach to classifying breaches as (non-)severe, led to a high-quality, internally consistent, homogenous sample. In contrast, many previous empirical studies either used smaller samples, focusing only on particular industries (e.g., [33]), or based their research on large but unadjusted samples, including not only large-scale intentional security breaches but also minor incidents (e.g., [164]).

Researchers, security executives, and financial market analysts do not necessarily have sufficient resources to expend the same effort when creating data-based insights upon which information security investment decisions or firm valuations might be based. In order to facilitate the generation of future information security knowledge and insights, the samples used throughout this dissertation are provided in Appendices A–C. The data sample contributions of this dissertation can be considered part of a nascent commendable stream of literature that provides curated breach samples with a focus on information security financial economics studies (see e.g., [522] for a recently published dataset intended to facilitate studies exploring economic and business impacts of data breaches).

Separately, whilst all four contributions in this dissertation applied novel empirical research design specifications, the studies in Chapters 5 and 7 particularly introduced new methodological considerations that might be of help to researchers' and practitioners' future analytical endeavours. Chapter 5 presented the first information security economics study that made use of the dual-beta model, which is considered a more appropriate measure of risk than the CAPM's regular symmetric single beta [36, 260–266]. The asymmetric effect of security breaches on upside and downside beta thereby implied that markets tend to react differently to breach announcements in bearish and bullish times. Future studies and security executives are likely to benefit from the insight that the general macroeconomic environment can be determinative for negative post-breach economic consequences.

Additionally, as delineated in Section 2.9, long-term studies of event-driven changes in information asymmetries are generally scarce, which is partially due to the difficulty of finding

appropriate empirical proxies for information asymmetries. Using changes in insider trading abnormal returns as a measurement of event- or strategy-induced shifts in information asymmetries is still a relatively nascent approach[1]. It is hoped that making breach-elevated information asymmetries more salient through insider trading data will help future analysts when deciding on empirical proxies for their studies.

8.1.3 Overarching Model Contributions

Whilst each of Contributions **C1**–**C4** provided relevant individual results and implications in their own right, they all worked towards an answer of the overarching research question *How can publicly listed firms leverage financial market data to achieve a better understanding of costs associated with information security to conduct more thorough information security investment cost-benefit analyses?* Using publicly available (financial) data — share prices, CDS prices, and insider trading filings — this dissertation introduced novel empirical evidence on four underlying and consequential cost items imposed on firms following security investments and breaches.

These four cost elements, which are interrelated and all part of firms' financing costs, are examples of underlying / consequential costs that ought to be integrated in more holistic information security investment cost-benefit analyses. Specifically, in terms of the ENBIS framework (see Equation 2.2), Contribution **C1** showed that information security executives can incur additional costs from investing in information security (c) if investors deem the investment to be net-value destructive ($c_{fincosts_{CAR}} > 0$), or negative costs (i.e., secondary benefits) if investors deem investments to be net-value accretive ($c_{fincosts_{CAR}} < 0$). These firm value effects result in greater ($c_{fincosts_{CAR}} > 0$) or lower ($c_{fincosts_{CAR}} < 0$) internal financing costs, respectively.

Contribution **C2** demonstrated the existence of an additional underlying / consequential cost element in the expected costs vector (λ) in the form of increases in financial systematic risk and hence cost of equity and financing costs ($\lambda_{fincosts_{CoE}} > 0$). The research presented in Contribution **C3** provided evidence that whilst post-breach cost of private debt are likely to increase and should be recognised in the respective cost vector ($\lambda_{fincosts_{CoD\ loans}} > 0$), cost of public or traded debt does not systematically increase following a breach ($\lambda_{fincosts_{CoD\ corporate\ public\ debt}} \not> 0$). Taken together, surges in cost of equity and debt elicited by security breaches influence external financing costs, which can in turn introduce further costs inter alia by reducing share prices.

[1] In previous analyses, insider trading abnormal returns were, for instance, applied as an empirical proxy for differences in information asymmetries stemming from difficult-to-analyse strategies (see [37]).

Contribution **C4** showed that information asymmetries, and with it valuation uncertainties, increase in the medium- and long-term following security breaches. The underlying / consequential cost element in the expected costs vector ($\lambda_{fincosts_{InfoAsymm}} > 0$) may in fact be underlying many other (more directly observable) costs associated with information security breaches. As information asymmetries impede valuation processes, they can inter alia lead to diminished share prices and elevated financing costs (see e.g., [110]). Similarly, the effect of negative news on CDS spread changes (i.e., the proxy for cost of debt applied in Contribution **C3**) is more pronounced for firms with higher information asymmetries [454].

In order to deploy scarce resources in the most efficient way, (information security) executives need to be aware of all cost types associated with security breaches and investments. In addition to direct costs following investments or the discovery of, response to, and mitigation of security breaches, there are also multiple indirect underlying and consequential costs introduced or elevated by security breaches and investments. In previous studies, multiple frameworks and models to help guide information security cost-benefit analyses were developed (see e.g., [21,25,30,123,127,140,145–147]). However, empirical evidence and theorising on more indirect economic consequences of security breaches and investments is needed.

Considering all four cost elements newly introduced in this dissertation in combination implies that one particular underlying / consequential cost type — financing costs — can increase following security breaches and security investments. Financing costs bear a dichotomous relevance for ENBIS assessments. First, such costs ought to be considered as part of the probability-weighted annual losses stemming from security breaches (ALE). Second, elevated financing costs lead to greater discount rates (r) and thus reduce the present value of investment projects due to the time value of money concept (see [110]). Both ALE and r are accordingly of relevance for the NPV of ENBIS, upon which information security investment decisions can be based.

Tying the four sets of empirical evidence and implications of novel underlying / consequential cost elements together allows for establishing an extended version of the ENBIS framework. The dissertation builds upon and complements previous cost-benefit tools, and particularly updates previous ENBIS conceptualisations by making financing costs more salient and emphasising the possibility of negative costs (i.e., secondary benefits) $c < 0$. Figure 8.1 provides a summary of the new cost elements introduced in this dissertation and how they all interact, generating higher or lower financing costs and ENBIS NPVs, respectively. In the descriptive boxes, $+$, $-$, and o thereby indicate that the respective cost element results in an increase, decrease, or no change in losses (λ), investment costs (c), and discount rates (r).

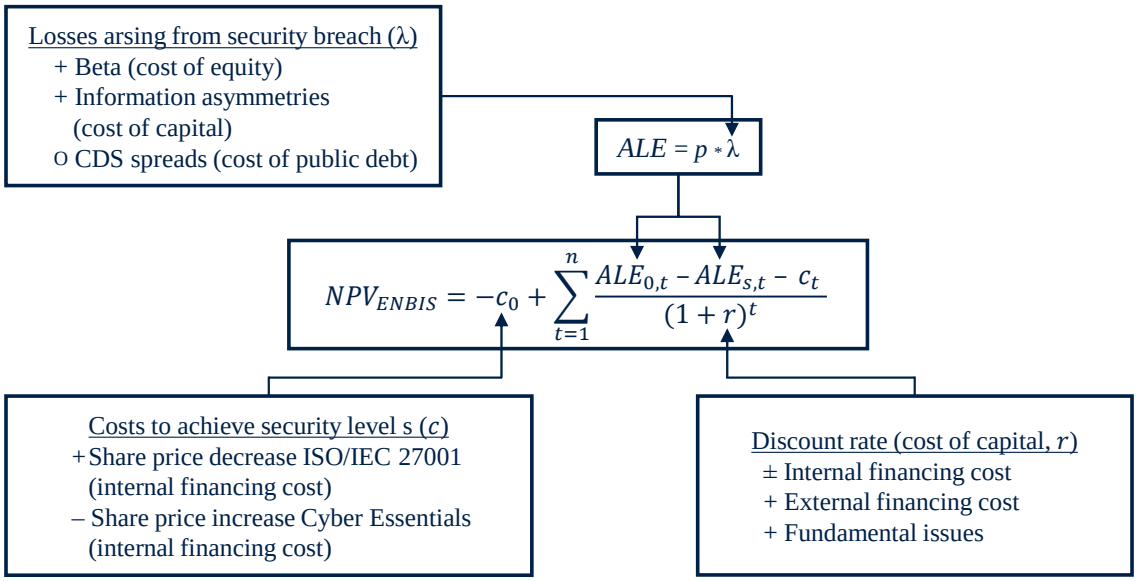


Figure 8.1: Summary of Proposed ENBIS Framework Extensions

The four contributions in this dissertation showed that indirect underlying / consequential costs, which tend to be neglected in information security economic analyses, can actually be of high importance. However, in order to gain an even more holistic understanding of, and in turn inform, corporate information security spending, legislative activities, and academic research, information security investment frameworks need to include further costs that go beyond the specific cost elements detailed in this dissertation. To this end, the Iceberg Model of Information Security Costs presented in Figure 8.2 was designed to help structure more holistic information security cost-benefit analyses and to add to nascent theories on information security management generally[2].

The Iceberg Model amalgamates and extends previous classifications, such as the ones distinguishing between direct/indirect and tangible/intangible costs [27–30, 147], by making use of the novel cost classification introduced in Section 2.4 and the empirical contributions in Chapters 4–7. The iceberg analogy is thereby not uncommon in the cyber security economics literature. For instance, Bisogni and colleagues [436] make use of an iceberg model to emphasise the extent of unreported data breach notifications.

The creation of a novel Iceberg Model of Information Security Costs was guided by considerations presented in previous literature (within the field of Computer Science) on

[2]For the avoidance of doubt, the purpose of the ENBIS extension and the Iceberg Model is neither to present a completely new information security investment model nor to make claims as to the effectiveness of particular security investment opportunities. Instead, it is aspired to support academics and practitioners by providing insights into additional cost categories to inform their information security investment decision-making models. The dissertation was hence not concerned with analysing other factors that contribute to the NPV of ENBIS such as companies' vulnerability to or frequency and likelihood of being attacked.

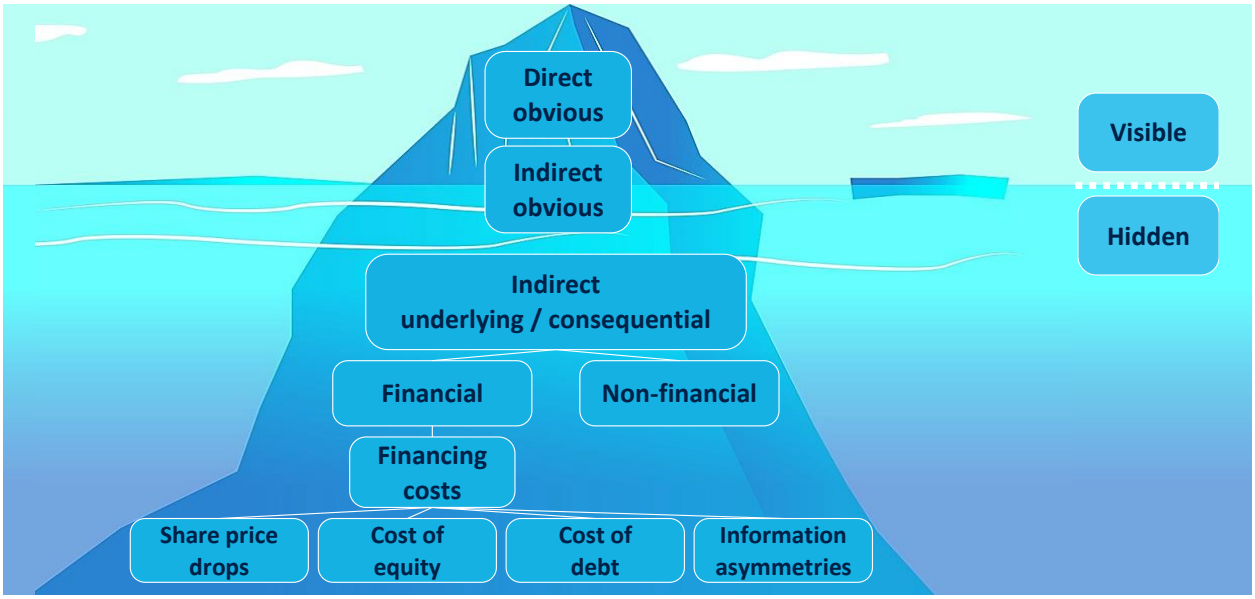


Figure 8.2: The Iceberg Model of Information Security Costs

building effective conceptual frameworks and models [523–530], and previous visualisations and tools within information security economics [21, 25, 27, 28, 123, 127, 140, 145–147, 163, 188, 193, 194, 531, 532]. Following the Framework for Classifying and Comparing Models of Cyber Security Investment [123], the Iceberg Model broadly falls into the category of *accounting models* to inform *quantitative appraisement* or *expected value analysis* [140, 142].

The Model depicts different information security cost categories, their visibility to (outside) investors, and their magnitude of economic severity. The tip of the iceberg, the only part that is observable without usage of any sophisticated tools, represents direct obvious costs and to some extend indirect obvious costs. The former costs include billed expenses for IT security systems or post-breach forensics and audit fees. Examples for the latter are expenses to provide training on the new systems and customer (re-)acquisition costs. Indirect obvious costs are thereby already considered partially hidden, as they are only indirectly attributable to security investments and breaches.

Indirect underlying / consequential costs constitute the submerged, and most voluminous, part of the iceberg. This cost type can be further subdivided into financial and non-financial indirect underlying / consequential costs. The figure signifies how such difficult-to-observe costs can actually make up the largest part of total security cost considerations. This depiction is in line with the notion that indirect or non-obvious costs exceed direct costs in gravity [26–30], and the contributions of this dissertation which showed that changes in financing costs — one example of financial indirect underlying / consequential costs — are of great magnitude as they affect virtually all activities of the firm.

The central recommendation of the novel cost classification, ENBIS extension, and Iceberg Model for value-maximising (security) executives, the main beneficiaries of this research, and academics is to factor in underlying / consequential costs in cost-benefit analyses of information security investments. It is hoped that practitioners and academics will find the empirical results and updated tools helpful for such endeavours[3].

Put differently, in a more direct response to the overarching research question, *How can publicly listed firms leverage financial market data to achieve a better understanding of costs associated with information security to conduct more thorough information security investment cost-benefit analyses?*: executives in publicly listed companies can use financial market data to improve their understanding of information security events-induced changes in financing costs. Gaining improved insights into security breach- and investment-related changes in financing costs makes one particular underlying / consequential cost category more salient. The enhanced understanding of one cost type, in combination with the novel cost classification distinguishing between obvious and underlying / consequential costs, provides a starting point for executives attempting to holistically assess the impact of information security breaches and investments. Generating first tangible insights, and realising that some information security costs are difficult to observe, can thereby facilitate further analyses of other financial and non-financial indirect underlying and consequential costs. Such holistic awareness of information security investment costs and benefits is necessary to invest economically in security controls.

Additionally, policy makers might find the results of this dissertation's empirical studies and contributions conducive to promoting investments in information security to for-profit firms. By making underlying and consequential costs more salient to executives, corporate decision makers might be more inclined to undertake appropriate investments in security controls, improve processes, and train staff. This is an important endeavour for governmental bodies as corporate information security incentives are often misaligned given that firms can externalise costs to society and invest more in damage control than in attack deterrence [125].

8.2 Future Research

The research described in this dissertation can be considered part of a wider endeavour to establish an enhanced understanding of underlying and consequential information security costs and benefits in order to advance cyber-risk quantification and inform information security investment decisions. Having presented the results of four analyses on changes in cost

[3]In fact, an earlier version of the Iceberg Model of Information Security Costs was presented at WEIS 2020 and received positive feedback from information security researchers and corporate practitioners.

of capital following security breaches and investments, this section provides an outline of how potential future work could be conducted, for instance, in the context of postdoctoral research or by other researchers in the field.

Regarding the empirical study presented in Chapter 4, future studies should aim to enlarge the sample used to analyse the impact of certifications on equity value and include more events, firms, and countries to verify the robustness and generalisability of the study's findings. Due to the ambivalent nature of the results, future research should replicate the present study on other financial markets and take into account other certificates. Furthermore, in an extended version of this dissertation's study, one could also consider re-classifying the timing of certification events' occurrence (e.g., considering publications of news items on certifications to be the event date as opposed to auditors' award dates, and distinguishing explicitly between initial certifications and re-certifications).

Additionally, given that the study is primarily of an exploratory nature, in future work, the initial regression analysis should be expanded to dissect factors that contribute to positive and negative abnormal returns, respectively. Particularly the argument that greater abnormal returns induced by Cyber Essentials certificates are due to the certificate's commercial exploitability merits further scientific exploration. Specifically, further research could analyse whether firms which (continue to) engage in work for the UK Government are systematically associated with greater abnormal returns relative to those firms which do not seek Cyber Essentials compliance to provide products or services to the Government. Future studies could also focus on the role of regulatory environments, IT maturity, and other country-level characteristics.

Moreover, additional firm-level characteristics such as different governance structures and the timing of investments relative to security breaches could be considered. Relatedly, multiple potential explanations of the results were discussed which should be tested empirically. Methodologically, future work could also include binomial/binary logistic regression models to examine variables influencing conditions under which cumulative abnormal returns tend to be negative. A separate (qualitative) study might also assess firms that choose not to re-certify and their respective reasons. Another way in which the study can be extended is to assess long-term firm value and financial performance implications, given that event studies are only designed to measure short-term market reactions.

Future work related to Chapter 5 could take into account unlevered betas (see [33]) as well as additional time frames to establish whether post-breach changes in costs of equity are influenced by financial risk and whether cost of capital changes persist over time. Additionally, given that cost of equity is a rather theoretical figure, a new practitioner-oriented study could demonstrate the effect of security breaches on cost of equity in monetary terms,

as well as relative to the respective risk-free rates and industry averages, in order to convey the relevance of this underlying / consequential cost to practitioners even more effectively.

Preliminary regression analysis results in Chapter 5 did not provide additional insights into factors influencing changes in systematic and downside risk. Further research could aim to extend the results by including additional factors that might help to explain why particular firms are more susceptible to breach-induced changes in systematic risk. Specifically, such studies could account for further factors related to firms' capital structures [485], including leverage (debt/equity and debt-service-coverage ratios), working capital management (changes over time, amount relative to industry competitors), as well as shareholder compensation (buybacks and dividends). Future versions of the analysis presented in this dissertation could also include factors intended to measure firms' operational resources and capabilities, such as operating profits, cash flows, marketing expenses, and patenting activities[4].

From strategic management and investment perspectives, it is generally accepted that systematic risk results from two main components: operating risk and financial risk (i.e., leverage) [483, 534–536]. Further research could examine whether breach-induced changes in systematic risk are connected to one or both components of systematic risk in the long term.

The results and implications presented in Chapter 6 could be taken forward by enlarging the underlying sample and conducting cross-sectional analyses. First, the low availability of CDS spread data resulted in a small useable sample, which rendered all t-tests to be associated with very low statistical power as per Cohen [506, 507]. To strengthen the generalisability of results presented in Contribution **C3**, the study should be reproduced on a larger sample of breached firms for which CDS data is available. Second, it could be interesting for academics and practitioners to determine firm characteristics that influence the magnitude of security breaches on CDS spreads. For instance, Huang and Wang [306] found that firms within healthcare, services, computer, electronic equipment and transportation industries experience particularly strong effects of breaches on loans. Whether such industry-level effects exist in the context of public debt as well is left to further research.

Moreover, the results in Chapter 6 indicated that CDS spreads peak prior to security breach announcements, which indicates the presence of informed traders in the market. There is a nascent stream of literature exploring insider trading in the time leading up to security breach announcements [413, 415–419]. It might be worth exploring whether this phenomenon can also be replicated in the market for CDS contracts.

The discussions presented in Chapters 5 and 6 imply that firms' cost of equity and cost of private debt increase after severe security breaches, whilst cost of corporate public debt

[4]See [48, 533] for the (operating) resource-based view of the firm.

seem less affected. Prior research also indicated that breached firms raise their cash holdings, decrease external financing, and increase financial leverage [200, 201, 486]. Given the economically significant differences between reactions on bond/CDS and loan markets to security breaches, breached firms are likely to not only increase leverage following a breach, but also alter their debt mix by taking on more public debt (as opposed to private debt/loans). Future researchers might hence be inclined to analyse post-breach capital structure changes with a focus on firms' debt-capital mix.

There are substantial differences across firms regarding their risk of suffering from a severe security attack and the associated negative financial repercussions [537]. The natural extension of the findings in Chapter 7 would be to further analyse firm-level differences that affect the extent to which information asymmetry issues exacerbate following security breaches. As higher levels of governance are generally associated with lower information asymmetry [355, 368, 471], measures of board structures, ownership, and activist investor presence would provide a natural starting point for such examinations (see e.g., [538,539] for well-established measures of corporate governance). Moreover, Hillier et al. [475] showed that insiders' personal attributes might have greater explanatory power for variations in insider trading abnormal returns than firm characteristics; and firms' breach remediation strategies and their respective effectiveness are likely dependent on executives' qualifications and previous experience as well. Accordingly, future empirical models might consider the mitigating influence of management teams' IT, information security, and disaster management experience on post-breach increases in information asymmetry issues.

Separately, security executives are likely to attempt mitigating intensified post-breach information asymmetries, for instance, via strategic news bundling [180], more frequent voluntary disclosures (see [512–515]), or strategy presentations (see [540]). Future quantitative and qualitative studies could establish ways in which managers in breached firms can improve their capital market communication to reduce principal-agent problems exacerbated by security breaches.

On a more general level, the four contributions of this dissertation are based on extensive data collection and empirical analyses. Quantitative information security studies are inherently subject to issues of data availability and quality. In order to improve security investment research, future studies could aim to extend and improve the studies presented in this dissertation by broadening the sample and enhancing the process of filtering out security breach events that are considered non-severe by stock market participants. For instance, to strengthen the robustness and generalisability of US-centric findings, other researchers might aim to include more security incidents in European companies.

Relatedly, the approach pursued to construct the final sample for the analyses in Chap-

ter 5—7 was based on an attempt to model an average investor who has an understanding of capital markets, actively follows equity analyst and media reports, and has a limited technical understanding of information security risks and breaches. Such a lay person is assumed to only consider highly severe security breaches in parent companies and direct subsidiaries in their research and pricing processes. The sampling process intending to mirror investors' perception of security breaches' severity was based on limited informal explorative conversations with professional and retail investors.

However, in reality, there is a broad range of stock market participants with diverse sets of financial and technological resources and capabilities. Accordingly, they might consider different factors in their assessments of security breaches, which might in turn result in breach severity assessments divergent from the classification scheme applied in this dissertation. Future work could establish investors' decision-making processes in a more formal way, for instance, by conducting (semi-)structured interviews or even behavioural experiments with investors to establish more holistically how market participants, and different subsets of investors, define security breach severity.

A similar (qualitative) approach could be applied to investigate whether security executives, the main beneficiaries of this research, can indeed benefit from the application of the ENBIS extension and Iceberg Model presented in Figures 8.1 and 8.2. Part of such an investigation should focus on executives' understanding of the cost classification first introduced in Section 2.4 and eventually returned to in the Iceberg Model. This is particularly relevant as the cost categories introduced in the Iceberg Model are not necessarily always mutually exclusive or independent, impeding the ability to definitively distinguish between, for instance, indirect obvious and indirect underlying / consequential costs[5].

Relatedly, given the scarcity of research on underlying and consequential costs imposed on firms, future work establishing further cost elements is needed. Most previous studies on indirect post-breach financial impacts are based on short-term abnormal equity market returns[6]. In this dissertation, four underlying / consequential cost elements, which are more reflective of medium- to long-term implications than short-term share price reactions alone, were made more salient. However, this dissertation only investigated one stream of indirect underlying and consequential costs, namely financial underlying / consequential costs. The Iceberg Model of Information Security Costs is also intended to serve as a platform

[5]This potential limitation of the Iceberg Model of Information Security Costs is accepted as its main purpose is not to authoritatively divide costs into different categories, but rather to highlight that there are more types of costs than those immediately visible to information security practitioners and researchers, and that those indirect costs can actually be of high relevance to information security cost-benefit analyses.

[6]For instance, there is an abundance of literature on short-term stock market reactions following security breaches [26, 30, 170–182].

for future studies to explore other underlying or consequential information security cost items. Graphically speaking, at the deepest part of the iceberg in Figure 8.2, there is still a lot of room left to be filled with other financial and non-financial indirect underlying / consequential cost items.

Additionally, although the increase in financing costs documented in this dissertation can be interpreted as negative economic consequences imposed not only on the focal firms but also on society, as increases in cost of capital and information asymmetries hinder effective price discovery for market participants, the dissertation offers only limited insights into quantifiable social costs or externalities incurred by other non-breached parties or society at large. Such societal and macroeconomic considerations raise other important research topics which are left to further investigation.

8.3 Conclusion

Taken together, the research presented in this dissertation has helped to advance the field and practice of information security financial economics in the context of information security investing. By adding novel empirical evidence on security investment-induced equity value implications and breach-induced changes in cost of equity, cost of debt, and information asymmetries, this dissertation contributed to the wider endeavour of establishing underlying/consequential information security costs. Using different methods and empirical settings across four studies provided reliable and robust overall results.

The insights stemming from these studies have significant implications for information security researchers and practitioners. Most relevantly, the studies revealed indirect underlying and consequential cost items executives ought to be aware of; facilitated an extension of the ENBIS framework; and allowed for establishing a new model — the Iceberg Model of Information Security Costs — supporting holistic information security cost-benefit analyses. Being aware of all cost and benefit types associated with information security investments is the first vital step in allocating capital economically efficiently towards information security controls.

Information security executives are interested in developing, implementing, and reviewing cost-effective systems to safeguard their organisations from severe impacts of security breaches. Deciding which security projects to invest in can be a complex issue for such executives. In order to actively manage information security risk, executives may consider a multitude of alternatives to mitigate the frequency, probability, and impact of successful security attacks on the firm. Quantifying the costs and benefits associated with information security breaches and investments is rife with complexities, and executives lack comprehen-

sive models to guide their thinking about all potential cost types encountered in the course of security breaches and investments. This dissertation provided an important step in the direction towards more comprehensive information security cost models.

In referring back to the initial overarching research question, it can be concluded that executives in publicly listed firms can leverage financial market data to establish changes in financing costs following security investments and breaches. Generating these new insights allows them to achieve a better understanding of information security costs generally and facilitates conducting more thorough information security investment cost-benefit analyses that incorporate underlying and consequential costs. It is hoped that the insights and models contributed in this dissertation will advance the research and practice of information security investment decision making and motivate further studies.

Bibliography

[1] Dennis D Malliouris and Andrew C Simpson. The Stock Market Impact of Information Security Investments: The Case of Security Standards. *Proceedings of the 18th Workshop on the Economics of Information Security (WEIS) 2019*, pages 1–32, 2019.

[2] Dennis D Malliouris and Andrew C Simpson. Underlying and Consequential Costs of Cyber Security Breaches: Changes in Systematic Risk. *Proceedings of the 19th Workshop on the Economics of Information Security (WEIS) 2020*, pages 1–59, 2020.

[3] Ponemon Institute and IBM Security. 2018 Cost of Data Breach Report. *Available at: https://www.ibm.com/security/data-breach (last accessed 01/05/2021)*, 2018.

[4] Gemalto Breach Level Index. Data Breach Database - Breach Level Index. *Available at: https://breachlevelindex.com/data-breach-database (last accessed 01/08/2018)*, 2018.

[5] Ernst and Young. Cybersecurity Regained: Preparing to Face Cyber Attacks. *20th Global Information Security Survey 2017-18. Available at: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/digital/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf (last accessed 01/05/2021)*, 2017.

[6] International Organization for Standardization. ISO/IEC 27000:2018. *Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en (last accessed 10/04/2021)*, 2018.

[7] C West Churchman. Wicked Problems. *Management Science*, 14(4):141–142, 1967.

[8] Horst W J Rittel and Melvin M Webber. Dilemmas in a General Theory of Planning. *Policy Sciences*, 4(2):155–169, 1973.

[9] John C Camillus. Strategy as a Wicked Problem. *Harvard Business Review*, 86(5):98–106, 2008.

[10] James F Courtney. Decision Making and Knowledge Management in Inquiring Organizations: Toward a New Decision-Making Paradigm for DSS. *Decision Support Systems*, 31(1):17–38, 2001.

[11] Omar F El-Gayar and Brian D Fritz. A Web-based Multi-perspective Decision Support System for Information Security Planning. *Decision Support Systems*, 50(1):43–54, 2010.

[12] Eloise F Malone and Michael J Malone. The "Wicked Problem" of Cybersecurity Policy: Analysis of United States and Canadian Policy Response. *Canadian Foreign Policy Journal*, 19(2):158–177, 2013.

[13] Tyler Moore. The Economics of Cybersecurity: Principles and Policy Options. *International Journal of Critical Infrastructure Protection*, 3(3-4):103–117, 2010.

[14] Ross Anderson. Why Information Security is Hard - An Economic Perspective. *17th Annual Computer Security Applications Conference*, pages 358–365, 2001.

[15] Ross Anderson and Tyler Moore. The Economics of Information Security. *Science*, 314(5799):610–613, 2006.

[16] Tyler Moore and Ross Anderson. Economics and Internet Security: A Survey of Recent Analytical, Empirical, and Behavioral Research. *Harvard Computer Science Group Technical Report TR-03-11*, pages 1–26, 2011.

[17] R Edward Freeman, Andrew C Wicks, and Bidhan Parmar. Stakeholder Theory and "the Corporate Objective Revisited". *Organization Science*, 15(3):364–369, 2004.

[18] Alfred Rappaport. *Creating Shareholder Value: The New Standard for Business Performance*. Free Press, New York City, NY, 1986.

[19] Avner Kalay and Uri Loewenstein. Predictable Events and Excess Returns: The Case of Dividend Announcements. *Journal of Financial Economics*, 14(3):423–449, 1985.

[20] Geert Bekaert and Robert J Hodrick. Characterizing Predictable Components in Excess Returns on Equity and Foreign Exchange Markets. *Journal of Finance*, 47(2):467–509, 1992.

[21] Lawrence A Gordon and Martin P Loeb. The Economics of Information Security Investment. *ACM Transactions on Information and System Security (TISSEC)*, 5(4):438–457, 2002.

[22] Chad D Heitzenrater and Andrew C Simpson. Policy, Statistics, and Questions: Reflections on UK Cyber Security Disclosures. *Proceedings of the 14th Workshop on the Economics of Information Security (WEIS) 2015*, pages 1–28, 2015.

[23] Rainer Böhme and Tyler Moore. Security Metrics and Security Investment. *Available at: https://tylermoore.ens.utulsa.edu/courses/econsec/f13/reading/lnse-secinv2.pdf (last accessed 23/09/2020)*, 2013.

[24] Chad D Heitzenrater and Andrew C Simpson. Policy, Statistics and Questions: Reflections on UK Cyber Security Disclosures. *Journal of Cybersecurity*, 2(1):43–56, 2016.

[25] Rainer Böhme. Security Metrics and Security Investment Models. In Isao Echizen, Noboru Kunihiro, and Ryoichi Sasaki, editors, *Advances in Information and Computer Security*, pages 10–24, Berlin, 2010. Springer.

[26] Alvin Leung and Indranil Bose. Indirect Financial Loss of Phishing to Global Market. In *International Conference on Information Systems (ICIS) 2008*, pages 1–15, 2008.

[27] Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michael J G van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. Measuring the Cost of Cybercrime. *Proceedings of the 11th Workshop on the Economics of Information Security (WEIS) 2012*, pages 1–31, 2012.

[28] Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Carlos Ganán, Tom Grasso, Michael Levi, Tyler Moore, and Marie Vasek. Measuring the Changing Cost of Cybercrime. *Proceedings of the 18th Workshop on the Economics of Information Security (WEIS) 2019*, pages 1–32, 2019.

[29] Stefan Laube and Rainer Böhme. The Economics of Mandatory Security Breach Reporting to Authorities. *Journal of Cybersecurity*, 2(1):29–41, 2016.

[30] Huseyin Cavusoglu, Birendra Mishra, and Srinivasan Raghunathan. The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, 9(1):70–104, 2004.

[31] Howard Kunreuther and Geoffrey Heal. Interdependent Security. *Journal of Risk and Uncertainty*, 26(2-3):231–249, 2003.

[32] Parliament of the United Kingdom. Companies Act 2006 (c 46) - Part 18. *Available at: https://www.legislation.gov.uk/ukpga/2006/46/part/18 (last accessed 13/11/2020)*, 2006.

[33] Oliver Hinz, Michael Nofer, Dirk Schiereck, and Julian Trillig. The Influence of Data Theft on the Share Prices and Systematic Risk of Consumer Electronics Companies. *Information & Management*, 52(3):337–347, 2015.

[34] Jesus Cardenas, Adolfo Coronado, Aurelia Donald, Fernando Parra, and M Adam Mahmood. The Economic Impact of Security Breaches on Publicly Traded Corporations: An Empirical Investigation. *AMCIS 2012 Proceedings*, pages 1–10, 2012.

[35] Aurelia Nicholas-Donald, Jesus Francisco Matus, SeungEui Ryu, and Adam M Mahmood. The Economic Effect of Privacy Breach Announcements on Stocks: A Comprehensive Empirical Investigation. *AMCIS 2011 Proceedings*, pages 1–15, 2011.

[36] Son-Nan Chen. An Examination of Risk-Return Relationship in Bull and Bear Markets Using Time-Varying Betas. *Journal of Financial and Quantitative Analysis*, 17(2):265–286, 1982.

[37] Dennis D Malliouris, Alphons T Vermorken, and Maximilian A M Vermorken. Strategy Uniqueness and Insider Trading: Evidence from Europe. *Awaiting Decision by Editor: International Journal of Finance & Economics*, pages 1–22, 2021.

[38] Zahoor A Soomro, Mahmood H Shah, and Javed Ahmed. Information Security Management Needs More Holistic Approach: A Literature Review. *International Journal of Information Management*, 36(2):215–225, 2016.

[39] Dennis D Malliouris, Alphons T Vermorken, and Maximilian A M Vermorken. Aggregate Insider Trading and Future Market Returns in the US, Europe, and Asia. *International Journal of Finance & Economics*, In Press:1–20, 2020.

[40] Dennis D Malliouris. Underlying and Consequential Costs of Cyber Security - Cost of Equity. *Willis Research Network Annual Review 2021. Available at: https://www.willistowerswatson.com/en-GB/Insights/2021/02/willis-research-network-annual-review-2021 (last accessed 01/05/2021)*, pages 94–97, 2021.

[41] Bruce Schneier. Information Security and Externalities. *ENISA Quarterly*, 2(4):3–4, 2007.

[42] Luca Allodi, Fabio Massacci, and Julian Williams. The Work-Averse Cyber Attacker Model: Theory and Evidence From Two Million Attack Signatures. *Proceedings of the 16th Workshop on the Economics of Information Security (WEIS) 2017*, pages 1–35, 2017.

[43] Luca Allodi. Economic Factors of Vulnerability Trade and Exploitation. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1483–1499, 2017.

[44] Serge Egelman, Cormac Herley, and Paul C Van Oorschot. Markets for Zero-Day Exploits: Ethics and Implications. In *Proceedings of the 2013 New Security Paradigms Workshop (NSPW)*, pages 41–46. ACM, 2013.

[45] Gary Stoneburner. Toward a Unified Security-Safety Model. *Computer*, 39(8):96–97, 2006.

[46] Mary Sumner. Information Security Threats: A Comparative Analysis of Impact, Probability, and Preparedness. *Information Systems Management*, 26(1):2–12, 2009.

[47] Jay B Barney. Firm Resources and Sustained Competitive Advantage. *Journal of Management*, 17(1):99–120, 1991.

[48] Birger Wernerfelt. A Resource-Based View of the Firm. *Strategic Management Journal*, 5(2):171–180, 1984.

[49] Anandhi Bharadwaj, Omar A El Sawy, Paul A Pavlou, and N Venkatraman. Digital Business Strategy: Toward a Next Generation of Insights. *MIS Quarterly*, 37(2):471–482, 2013.

[50] Anandhi S Bharadwaj. A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation. *MIS Quarterly*, 24(1):169–196, 2000.

[51] Christopher Theisen, Nuthan Munaiah, Mahran Al-Zyoud, Jeffrey C Carver, Andrew Meneely, and Laurie Williams. Attack Surface Definitions: A Systematic Literature Review. *Information and Software Technology*, 104:94–103, 2018.

[52] Pythagoras Petratos and Alessio Faccia. Accounting Information Systems and System of Systems: Assessing Security with Attack Surface Methodology. *Proceedings of the 2019 3rd International Conference on Cloud and Big Data Computing*, pages 100–105, 2019.

[53] Adrian Baldwin, Iffat Gheyas, Christos Ioannidis, David Pym, and Julian Williams. Contagion in Cyber Security Attacks. *Journal of the Operational Research Society*, 68(7):780–791, 2017.

[54] Lawrence A Gordon, Martin P Loeb, William Lucyshyn, and Tashfeen Sohail. The Impact of the Sarbanes-Oxley Act on the Corporate Disclosures of Information Security Activities. *Journal of Accounting and Public Policy*, 25(5):503–530, 2006.

[55] Linda Wallace, Hui Lin, and Meghann Abell Cefaratti. Information Security and Sarbanes-Oxley Compliance: An Exploratory Study. *Journal of Information Systems*, 25(1):185–211, 2011.

[56] Carolyn Y Woo. An Empirical Test of Value-Based Planning Models and Implications. *Management Science*, 30(9):1031–1050, 1984.

[57] Harry M Markowitz. Portfolio Selection. *Journal of Finance*, 7(1):77–91, 1952.

[58] Thomas E Copeland, Tim Koller, and Jack Murrin. *Valuation: Measuring and Managing the Value of Companies*. Wiley, Hoboken, NJ, 1994.

[59] Amy J Hillman and Gerald D Keim. Shareholder Value, Stakeholder Management, and Social Issues: What's the Bottom Line? *Strategic Management Journal*, 22(2):125–139, 2001.

[60] William Lazonick and Mary O'Sullivan. Maximizing Shareholder Value: A New Ideology for Corporate Governance. *Economy and Society*, 29(1):13–35, 2000.

[61] Christopher D Ittner and David F Larcker. Assessing Empirical Research in Managerial Accounting: A Value-based Management Perspective. *Journal of Accounting and Economics*, 32(1-3):349–410, 2001.

[62] Ronald H Coase. The Nature of the Firm. *Economica*, 4(16):386–405, 1937.

[63] Oliver E Williamson. *Markets and Hierarchies*. Free Press, New York City, NY, 1975.

[64] Oliver E Williamson. The Economics of Organization: The Transaction Cost Approach. *American Journal of Sociology*, 87(3):548–577, 1981.

[65] Oliver E Williamson. The Vertical Integration of Production: Market Failure Considerations. *The American Economic Review*, 61(2):112–123, 1971.

[66] Oliver E Williamson. Markets and Hierarchies: Some Elementary Considerations. *The American Economic Review*, 63(2):316–325, 1973.

[67] Jay B Barney. Strategic Factor Markets: Expectations, Luck, and Business Strategy. *Management Science*, 32(10):1231–1241, 1986.

[68] Steven A Lippman and Richard P Rumelt. A Bargaining Perspective on Resource Advantage. *Strategic Management Journal*, 24(11):1069–1086, 2003.

[69] Jan W Rivkin. Imitation of Complex Strategies. *Management Science*, 46(6):745–873, 2000.

[70] Richard P Rumelt. Towards a Strategic Theory of the Firm. *Competitive Strategic Management*, 26(3):556–570, 1984.

[71] A M Brandenburger and H W Stuart. Value-Based Business Strategy. *Journal of Economics and Management Strategy*, 5(1):5–24, 1996.

[72] Michael E Porter. *Competitive Advantage: Creating and Sustaining Superior Performance*. Free Press, New York City, NY, 1985.

[73] Costas Markides. What Is Strategy And How Do You Know If You Have One? *Business Strategy Review*, 15(2):5–12, 2004.

[74] Phanish Puranam and Bart Vanneste. *Corporate Strategy: Tools for Analysis and Decision-making*. Cambridge University Press, Cambridge, UK, 2016.

[75] Milton Friedman. The Social Responsibility Of Business Is to Increase Its Profits. *The New York Times 13/09/1970*, page 17, 1970.

[76] John Tyler. Negating the Legal Problem of Having Two Masters: A Framework for L3C Fiduciary Duties and Accountability. *Vermont Law Review*, 35(1):117–161, 2010.

[77] R Edward Freeman, Jeffrey S Harrison, Andrew C Wicks, Bidhan L Parmar, and Simone De Colle. *Stakeholder Theory: The State of the Art*. Cambridge University Press, Cambridge, UK, 2010.

[78] Sanford J Grossman and Joseph E Stiglitz. On Value Maximization and Alternative Objectives of the Firm. *Journal of Finance*, 32(2):389–402, 1977.

[79] Michael C Jensen. Value Maximization, Stakeholder Theory, and the Corporate Objective Function. *European Financial Management*, 7(3):297–317, 2001.

[80] James S Wallace. Value Maximization and Stakeholder Theory: Compatible or Not? *Journal of Applied Corporate Finance*, 15(3):120–127, 2003.

[81] Milton Friedman. *Capitalism and Freedom*. University of Chicago Press, Chicago, IL, 1962.

[82] Joshua Rosenbaum and Joshua Pearl. *Investment Banking: Valuation, Leveraged Buyouts, and Mergers & Acquisitions*. Wiley, Hoboken, NJ, 2nd edition, 2013.

[83] Richard Whittington. Big Strategy/Small Strategy. *Strategic Organization*, 10(3):263–268, 2012.

[84] Robert G Eccles, Ioannis Ioannou, and George Serafeim. The Impact of Corporate Sustainability on Organizational Processes and Performance. *Management Science*, 60(11):2835–2857, 2014.

[85] Michael E Porter and Mark R Kramer. Creating Shared Value. *Harvard Business Review*, 89(1/2):62–77, 2011.

[86] Yuval Deutsch, Thomas Keil, and Tomi Laamanen. A Dual Agency View of Board Compensation: The Joint Effects of Outside Director and CEO Stock Options on Firm Risk. *Strategic Management Journal*, 32(2):212–227, 2011.

[87] Brian J Hall and Jeffrey B Liebman. Are CEOs Really Paid Like Bureaucrats? *The Quarterly Journal of Economics*, 113(3):653–691, 1998.

[88] David Yermack. Do Corporations Award CEO Stock Options Effectively? *Journal of Financial Economics*, 39(2-3):237–269, 1995.

[89] Joshua Gans, Stephen King, and N Gregory Mankiw. *Principles of Microeconomics*. Cengage Learning, Boston, MA, 5th edition, 2011.

[90] Herbert A Simon. Rational Decision Making in Business Organizations. *The American Economic Review*, 69(4):493–513, 1979.

[91] Herbert A Simon. *Administrative Behavior*. Free Press, New York City, NY, 4th edition, 1997.

[92] John Scott. Rational Choice Theory. In Gary Browning, Abigail Halcli, and Frank Webster, editors, *Understanding Contemporary Society: Theories of the Present*, volume 129, pages 126–138. SAGE Publications, London, UK, 2000.

[93] David Besanko, David Dranove, Mark Shanley, and Scott Schaefer. *Economics of Strategy*. Wiley, Hoboken, NJ, 7th edition, 2017.

[94] Neil F Doherty and Heather Fulford. Aligning the Information Security Policy with the Strategic Information Systems Plan. *Computers & Security*, 25(1):55–63, 2006.

[95] Huseyin Cavusoglu, Hasan Cavusoglu, Jai-Yeol Son, and Izak Benbasat. Institutional Pressures in Security Management: Direct and Indirect Influences on Organizational Investment in Information Security Control Resources. *Information & Management*, 52(4):385–400, 2015.

[96] Juhee Kwon and M Eric Johnson. Health-Care Security Strategies for Data Protection and Regulatory Compliance. *Journal of Management Information Systems*, 30(2):41–66, 2013.

[97] Manuel Hepfer and Thomas C Powell. Make Cybersecurity a Strategic Asset. *MIT Sloan Management Review*, 62(1):40–45, 2020.

[98] Michael Wade and John Hulland. The Resource-Based View and Information Systems Research: Review, Extension, and Suggestions for Future Research. *MIS Quarterly*, 28(1):107–142, 2004.

[99] Thomas C Powell and Anne Dent-Micallef. Information Technology as Competitive Advantage: The Role of Human, Business, and Technology Resources. *Strategic Management Journal*, 18(5):375–405, 1997.

[100] Francisco J Mata, William L Fuerst, and Jay B Barney. Information Technology and Sustained Competitive Advantage: A Resource-Based Analysis. *MIS Quarterly*, 19(4):487–505, 1995.

[101] Robert C Merton. Applications of Option-Pricing Theory: Twenty-Five Years Later. *American Economic Review*, 88(3):323–349, 1998.

[102] Irving Fisher. *The Nature of Capital and Income*. Macmillan, New York City, NY, 1906.

[103] Irving Fisher. *The Theory of Interest*. Macmillan, New York City, NY, 1930.

[104] John Burr Williams. *The Theory of Investment Value*. Harvard University Press, Cambridge, MA, 1938.

[105] Steven N Kaplan and Richard S Ruback. The Valuation of Cash Flow Forecasts: An Empirical Analysis. *Journal of Finance*, 50(4):1059–1093, 1995.

[106] Myron J Gordon and Eli Shapiro. Capital Equipment Analysis: The Required Rate of Profit. *Management Science*, 3(1):102–110, 1956.

[107] Myron J Gordon. Dividends, Earnings, and Stock Prices. *Review of Economics and Statistics*, 41(2):99–105, 1959.

[108] Eugene F Fama. Efficient Capital Markets: A Review of Theory and Empirical Work. *Journal of Finance*, 25(2):383–417, 1970.

[109] Eugene F Fama. Random Walks in Stock Market Prices. *Financial Analysts Journal*, 51(1):75–80, 1995.

[110] Richard A Brealey, Stewart C Myers, and Franklin Allen. *Principles of Corporate Finance*. McGraw-Hill Education, New York City, NY, 13th edition, 2020.

[111] Franco Modigliani and Merton H Miller. The Cost of Capital, Corporation Finance and the Theory of Investment. *American Economic Review*, 48(3):261–297, 1958.

[112] Stewart C Myers and Nicholas S Majluf. Corporate Financing and Investment Decisions When Firms Have Information That Investors Do Not Have. *Journal of Financial Economics*, 13(2):187–221, 1984.

[113] Stewart C Myers. Capital Structure Puzzle. *National Bureau of Economic Research Working Paper Series No. 1393*, pages 1–35, 1984.

[114] Robert C Merton. On the Pricing of Corporate Debt: The Risk Structure of Interest Rates. *Journal of Finance*, 29(2):449–470, 1974.

[115] Raghuram G Rajan and Luigi Zingales. What Do We Know About Capital Structure? Some Evidence From International Data. *Journal of Finance*, 50(5):1421–1460, 1995.

[116] Stewart C Myers. Capital Structure. *Journal of Economic Perspectives*, 15(2):81–102, 2001.

[117] William F Sharpe. A Simplified Model for Portfolio Analysis. *Management Science*, 9(2):277–293, 1963.

[118] William F Sharpe. Capital Asset Prices: A Theory of Market Equilibrium Under Conditions of Risk. *Journal of Finance*, 19(3):425–442, 1964.

[119] John Lintner. The Valuation of Risk Assets and the Selection of Risky Investments in Stock Portfolios and Capital Budgets. *Review of Economics and Statistics*, 47(1):13–37, 1965.

[120] Jack L Treynor. How to Rate Management of Investment Funds. *Harvard Business Review*, 43(1):63–75, 1965.

[121] Jan Mossin. Equilibrium in a Capital Asset Market. *Econometrica*, 34(4):768–783, 1966.

[122] Mark Rubinstein. Markowitz's "Portfolio Selection": A Fifty-Year Retrospective. *Journal of Finance*, 57(3):1041–1045, 2002.

[123] Rachel Rue, Shari Lawrence Pfleeger, and David Ortiz. A Framework for Classifying and Comparing Models of Cyber Security Investment to Support Policy and Decision-Making. *Proceedings of the 6th Workshop on the Economics of Information Security (WEIS) 2007*, pages 1–23, 2007.

[124] Sangmi Chai, Minkyun Kim, and H Raghav Rao. Firms' Information Security Investment Decisions: Stock Market Evidence of Investors' Behavior. *Decision Support Systems*, 50(4):651–661, 2011.

[125] Wing M W Lam. Attack-Deterring and Damage-Control Investments in Cybersecurity. *Proceedings of the 14th Workshop on the Economics of Information Security (WEIS) 2015*, pages 1–24, 2015.

[126] Tyler Moore, Scott Dynes, and Frederick R Chang. Identifying How Firms Manage Cybersecurity Investment. *Proceedings of the 15th Workshop on the Economics of Information Security (WEIS) 2016*, pages 1–27, 2016.

[127] Eva Weishäupl, Emrah Yasasin, and Guido Schryen. Information Security Investments: An Exploratory Multiple Case Study on Decision-Making, Evaluation and Learning. *Computers & Security*, 77:807–823, 2018.

[128] Madeline Carr and Leonie M Tanczer. UK Cybersecurity Industrial Policy: An Analysis of Drivers, Market Failures and Interventions. *Journal of Cyber Policy*, 3(3):430–444, 2018.

[129] Karen Renaud, Stephen Flowerday, Merrill Warkentin, Paul Cockshott, and Craig Orgeron. Is the Responsibilization of the Cyber Security Risk Reasonable and Judicious? *Computers & Security*, 78:198–211, 2018.

[130] European Parliament and the Council. General Data Protection Regulation. *Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (last accessed 01/05/2021)*, 2016.

[131] Janine L Spears and Robert J Cole. A Preliminary Investigation of the Impact of the Sarbanes-Oxley Act on Information Security. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, pages 1–10. IEEE, 2006.

[132] Matthew P Barrett. NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. *NIST. Available at: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11 (last accessed 01/05/2021)*, 2018.

[133] United Kingdom Department for Culture Media and Sport; Ipsos MORI's Social Research Institute; University of Portsmouth. UK Cyber Security Breaches Survey 2017. *Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017 (last accessed 01/05/2021)*, 2017.

[134] United Kingdom Department for Culture Media and Sport; Ipsos MORI's Social Research Institute; University of Portsmouth. UK Cyber Security Breaches Survey 2018. *Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018 (last accessed 01/05/2021)*, 2018.

[135] Claudia Biancotti. The Price of Cyber (In)security: Evidence from the Italian Private Sector. *Proceedings of the 17th Workshop on the Economics of Information Security (WEIS) 2018*, pages 1–44, 2018.

[136] Christos Ioannidis, David Pym, and Julian Williams. Investments and Trade-offs in the Economics of Information Security. In R Dingledine and P Golle, editors, *Financial Cryptography and Data Security. 13th International Conference, FC 2009. Lecture Notes in Computer Science, Vol. 5628*, pages 148–166. Springer, Berlin, 2009.

[137] Christos Ioannidis, David Pym, and Julian Williams. Information Security Trade-Offs and Optimal Patching Policies. *European Journal of Operational Research*, 216(2):434–444, 2012.

[138] Christos Ioannidis, David Pym, and Julian Williams. Fixed Costs, Investment Rigidities, and Risk Aversion in Information Security: A Utility-Theoretic Approach. *Proceedings of the 10th Workshop on the Economics of Information Security (WEIS) 2011*, pages 1–16, 2011.

[139] Karen Elliott, Fabio Massacci, and Julian Williams. Action, Inaction, Trust, and Cybersecurity's Common Property Problem. *IEEE Security & Privacy*, 14(1):82–86, 2016.

[140] Alireza Shameli-Sendi, Rouzbeh Aghababaei-Barzegar, and Mohamed Cheriet. Taxonomy of Information Security Risk Assessment (ISRA). *Computers & Security*, 57:14–30, 2016.

[141] Chi-Chun Lo and Wan-Jia Chen. A Hybrid Information Security Risk Assessment Procedure Considering Interdependences Between Controls. *Expert Systems with Applications*, 39(1):247–257, 2012.

[142] Lili Sun, Rajendra P Srivastava, and Theodore J Mock. An Information Systems Security Risk Assessment Model Under the Dempster-Shafer Theory of Belief Functions. *Journal of Management Information Systems*, 22(4):109–142, 2006.

[143] Rex Kelly Rainer Jr, Charles A Snyder, and Houston H Carr. Risk Analysis for Information Technology. *Journal of Management Information Systems*, 8(1):129–147, 1991.

[144] Bob Blakley, Ellen McDermott, and Dan Geer. Information Security is Information Risk Management. *Proceedings of the 2001 Workshop on New Security Paradigms (NSPW)*, pages 97–104, 2001.

[145] M-Elisabeth Paté-Cornell, Marshall Kuypers, Matthew Smith, and Philip Keller. Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies. *Risk Analysis*, 38(2):226–241, 2018.

[146] Daniel Dor and Yuval Elovici. A Model of the Information Security Investment Decision-Making Process. *Computers & Security*, 63:1–13, 2016.

[147] Bin Srinidhi, Jia Yan, and Giri Kumar Tayi. Allocation of Resources to Cyber-Security: The Effect of Misalignment of Interest Between Managers and Investors. *Decision Support Systems*, 75:49–62, 2015.

[148] Brent R Rowe and Michael P Gallaher. Private Sector Cyber Security Investment: An Empirical Analysis. *Proceedings of the 5th Workshop on the Economics of Information Security (WEIS) 2006*, pages 1–23, 2006.

[149] Michel Benaroch and Robert J Kauffman. A Case for Using Real Options Pricing Analysis to Evaluate Information Technology Project Investments. *Information Systems Research*, 10(1):70–86, 1999.

[150] Michel Benaroch. Managing Information Technology Investment Risk: A Real Options Perspective. *Journal of Management Information Systems*, 19(2):43–84, 2002.

[151] Michail Chronopoulos, Emmanouil Panaousis, and Jens Grossklags. An Options Approach to Cybersecurity Investment. *IEEE Access*, 6:12175–12186, 2018.

[152] Andrew Fielder, Emmanouil Panaousis, Pasquale Malacaria, Chris Hankin, and Fabrizio Smeraldi. Decision Support Approaches for Cyber Security Investment. *Decision Support Systems*, 86:13–23, 2016.

[153] Yong Wu, Gengzhong Feng, Nengmin Wang, and Huigang Liang. Game of Information Security Investment: Impact of Attack Types and Network Vulnerability. *Expert Systems with Applications*, 42(15-16):6132–6146, 2015.

[154] Huseyin Cavusoglu, Birendra Mishra, and Srinivasan Raghunathan. A Model for Evaluating IT Security Investments. *Communications of the ACM*, 47(7):87–92, 2004.

[155] Gerhard A Perschke, Stephen J Karabin, and Terry L Brock. Four Steps To Information Security. *Journal of Accountancy*, 161(4):104–113, 1986.

[156] Lawrence A Gordon and Martin P Loeb. Return on Information Security Investments: Myths vs. Realities. *Strategic Finance*, 84(5):26–31, 2002.

[157] Kent D Miller and Philip Bromiley. Strategic Risk and Corporate Performance: An Analysis of Alternative Risk Measures. *Academy of Management Journal*, 33(4):756–779, 1990.

[158] Sasha Romanosky. Examining the Costs and Causes of Cyber Incidents. *Journal of Cybersecurity*, 2(2):121–135, 2016.

[159] Dinei Florêncio and Cormac Herley. Sex, Lies and Cyber-Crime Surveys. In *Economics of Information Security and Privacy III*, pages 35–53. Springer, 2013.

[160] Eric Jardine. Mind the Denominator: Towards a More Effective Measurement System for Cybersecurity. *Journal of Cyber Policy*, 3(1):116–139, 2018.

[161] Paul Hyman. Cybercrime: It's Serious, But Exactly How Serious? *Communications of the ACM*, 56(3):18–20, 2013.

[162] Gartner. Gartner Forecasts Worldwide Security and Risk Management Spending Growth to Slow but Remain Positive in 2020. *Available at: https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem (last accessed 25/09/2020)*, 2020.

[163] Ponemon Institute and IBM Security. 2019 Cost of Data Breach Report. *Available at: https://www.ibm.com/security/data-breach (last accessed 01/05/2021)*, 2019.

[164] Benjamin Edwards, Steven Hofmeyr, and Stephanie Forrest. Hype and Heavy Tails: A Closer Look at Data Breaches. *Journal of Cybersecurity*, 2(1):3–14, 2016.

[165] NetDiligence. NetDiligence Cyber Claims Study 2019. *Available at: https://netdiligence.com/wp-content/uploads/2020/05/2019_NetD_Claims_Study_Report_1.2.pdf (last accessed 25/09/2020)*, 2019.

[166] Accenture. Ninth Annual Cost of Cybercrime Study. *Available at: https://www.accenture.com/us-en/insights/security/cost-cybercrime-study (last accessed 01/05/2021)*, 2019.

[167] United Kingdom Department for Culture Media and Sport; Ipsos MORI's Social Research Institute; University of Portsmouth. Cyber Security Breaches Survey 2019. *Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019 (last accessed 01/05/2020)*, 2020.

[168] Michihiro Yamada, Hiroaki Kikuchi, Naoki Matsuyama, and Koji Inui. Mathematical Model to Estimate Loss by Cyber Incident in Japan. *5th International Conference on Information Systems Security and Privacy (CISSP) 2019*, pages 353–360, 2019.

[169] Martin Eling and Jan H Wirfs. What are the Actual Costs of Cyber Risk Events? *European Journal of Operational Research*, 272(3):1109–1119, 2019.

[170] Francis K Andoh-Baidoo, Kwasi Amoako-Gyampah, and Kweku-Muata Osei-Bryson. How Internet Security Breaches Harm Market Value. *IEEE Security & Privacy*, 8(1):36–42, 2010.

[171] Katherine Campbell, Lawrence A Gordon, Martin P Loeb, and Lei Zhou. The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security*, 11(3):431–448, 2003.

[172] Anat Hovav and John D'Arcy. The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms. *Risk Management and Insurance Review*, 6(2):97–121, 2003.

[173] Anat Hovav and John D'Arcy. The Impact of Virus Attack Announcements on the Market Value of Firms. *Information Systems Security*, 13(3):32–40, 2004.

[174] Karthik Kannan, Jackie Rees, and Sanjay Sridhar. Market Reactions to Information Security Breach Announcements: An Empirical Analysis. *International Journal of Electronic Commerce*, 12(1):69–91, 2007.

[175] James Goldstein, Anna Chernobai, and Michel Benaroch. An Event Study Analysis of the Economic Impact of IT Operational Risk and its Subcategories. *Journal of the Association for Information Systems*, 12(9):606–631, 2011.

[176] Sanjay Goel and Hany A Shawky. Estimating the Market Impact of Security Breach Announcements on Firm Values. *Information & Management*, 46(7):404–410, 2009.

[177] Edward A Morse, Vasant Raval, and John R Wingender. Market Price Effects of Data Security Breaches. *Information Security Journal: A Global Perspective*, 20(6):263–273, 2011.

[178] Ali A Yayla and Qing Hu. The Impact of Information Security Events on the Stock Value of Firms: The Effect of Contingency Factors. *Journal of Information Technology*, 26(1):60–77, 2011.

[179] Georgios Spanos and Lefteris Angelis. The Impact of Information Security Events to the Stock Market: A Systematic Literature Review. *Computers & Security*, 58:216–229, 2016.

[180] Sebastien Gay. Strategic News Bundling and Privacy Breach Disclosures. *Journal of Cybersecurity*, 3(2):91–108, 2017.

[181] Eli Amir, Shai Levi, and Tsafrir Livne. Do Firms Underreport Information on Cyber-Attacks? Evidence from Capital Markets. *Review of Accounting Studies*, 23(3):1177–1206, 2018.

[182] Alessandro Acquisti, Allan Friedman, and Rahul Telang. Is There a Cost to Privacy Breaches? An Event Study. *Proceedings of the 5th Workshop on the Economics of Information Security (WEIS) 2006*, pages 1–20, 2006.

[183] Pierangelo Rosati, Peter Deeney, Mark Cummins, Lisa van der Werff, and Theo Lynn. Social Media and Stock Price Reaction to Data Breach Announcements: Evidence from US Listed Companies. *Research in International Business and Finance*, 47:458–469, 2019.

[184] Elena Kvochko and Rajiv Pant. Why Data Breaches Don't Hurt Stock Prices. *Harvard Business Review. Available at: https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices (last accessed 01/05/2021)*, 2015.

[185] Joshua Danielson. Breaches Don't Correlate To Real Results. *Forbes. Available at: https://www.forbes.com/sites/forbestechcouncil/2018/09/25/breaches-dont-correlate-to-real-results/ (last accessed 01/05/2021)*, 2018.

[186] Russell Lange and Eric W Burger. Long-Term Market Implications of Data Breaches, Not. *Journal of Information Privacy and Security*, 13(4):186–206, 2017.

[187] Vernon J Richardson, Rodney E Smith, and Marcia Weidenmier Watson. Much Ado About Nnothing: The (Lack of) Economic Impact of Data Privacy Breaches. *Journal of Information Systems*, 33(3):227–265, 2019.

[188] Russel C Thomas, Marcin Antkiewicz, Patrick Florer, Suzanne Widup, and Matthew Woodyard. How Bad Is It? – A Branching Activity Model to Estimate the Impact of Information Security Breaches. *Proceedings of the 12th Workshop on the Economics of Information Security (WEIS) 2013*, pages 1–34, 2013.

[189] Vilhelm Verendel. Quantified Security is a Weak Hypothesis: A Critical Survey of Results and Assumptions. In *Proceedings of the 2009 Workshop on New Security Paradigms (NSPW)*, pages 37–50, 2009.

[190] James E Lerums and J Eric Dietz. The Economics of Critical Infrastructure Controls Systems' Cyber Security. In *2018 IEEE International Symposium on Technologies for Homeland Security (HST)*, pages 1–9, 2018.

[191] Fariborz Farahmand, Shamkant B Navathe, Gunter P Sharp, and Philip H Enslow. A Management Perspective on Risk of Security Threats to Information Systems. *Information Technology and Management*, 6(2):203–225, 2005.

[192] European Union Agency for Cybersecurity (ENISA). Incentives and Barriers of the Cyber Insurance Market in Europe. *Available at: https://www.enisa.europa.eu/publications/incentives-and-barriers-of-the-cyber-insurance-market-in-europe (last accessed 01/05/2021)*, pages 1–45, 2012.

[193] Sriram Somanchi and Rahul Telang. Impact of Security Events and Fraudulent Transactions on Customer Loyalty: A Field Study. *Proceedings of the 16th Workshop on the Economics of Information Security (WEIS) 2017*, pages 1–16, 2017.

[194] Juhee Kwon and M Eric Johnson. The Market Effect of Healthcare Security: Do Patients Care about Data Breaches? *Proceedings of the 14th Workshop on the Economics of Information Security (WEIS) 2015*, pages 1–34, 2015.

[195] Srikanth Parameswaran, Srikanth Venkatesan, and Manish Gupta. Cloud Computing Security Announcements: Assessment of Investors' Reaction. *Journal of Information Privacy and Security*, 9(1):17–46, 2013.

[196] Eva Szubartowicz and Guido Schryen. Timing in Information Security: An Event Study on the Impact of Information Security Investment Announcements (Working Paper). *University of Regensburg Working Paper. Available at: https://epub.uni-regensburg.de/37576/ (last accessed 01/11/2018)*, pages 1–33, 2018.

[197] Niaz Kammoun, Ahmed Bounfour, Altay Özaygen, and Rokhaya Dieye. Financial Market Reaction to Cyberattacks. *Cogent Economics & Finance*, 7(1):1–20, 2019.

[198] Thomas J Smith, Julia L Higgs, and Robert E Pinsker. Do Auditors Price Breach Risk in Their Audit Fees? *Journal of Information Systems*, 33(2):177–204, 2019.

[199] Daniele Bianchi and Onur Kemal Tosun. Cyber Attacks and Stock Market Activity. *WBS Finance Group Research Paper No. 251*, pages 1–50, 2019.

[200] Shinichi Kamiya, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, and René M Stulz. What is the Impact of Successful Cyberattacks on Target Firms? *National Bureau of Economic Research Working Paper Series*, No. 24409:1–59, 2018.

[201] Matteo Binfarè. The Real Effects of Operational Risk: Evidence from Data Breaches. *Working Paper available at SSRN: https://ssrn.com/abstract=3411553*, pages 1–63, 2020.

[202] Sung Choi and M Eric Johnson. Do Hospital Data Breaches Reduce Patient Care Quality? *Proceedings of the 16th Workshop on the Economics of Information Security (WEIS) 2017*, pages 1–32, 2017.

[203] Christos Makridis and Benjamin Dean. Measuring the Economic Effects of Data Breaches on Firm Outcomes: Challenges and Opportunities. *Journal of Economic and Social Measurement*, 43(1-2):59–83, 2018.

[204] Claire Lending, Kristina Minnick, and Patrick J Schorno. Corporate Governance, Social Responsibility, and Data Breaches. *Financial Review*, 53(2):413–455, 2018.

[205] Jacob Haislip, Kalin Kolev, Robert E Pinsker, and Thomas Steffen. The Economic Cost of Cybersecurity Breaches: A Broad-based Analysis. *Proceedings of the 18th Workshop on the Economics of Information Security (WEIS) 2019*, pages 1–37, 2019.

[206] Chris Zhijian He, Tracie Frost, and Robert E Pinsker. The Impact of Reported Cybersecurity Breaches on Firm Innovation. *Journal of Information Systems*, 34(2):187–209, 2020.

[207] Bhagwan Chowdhry and Joshua D Coval. Internal Financing of Multinational Subsidiaries: Debt vs. Equity. *Journal of Corporate Finance*, 4(1):87–106, 1998.

[208] Evsey D Domar. The Case for Accelerated Depreciation. *The Quarterly Journal of Economics*, 67(4):493–519, 1953.

[209] Claudia Curi and Maurizio Murgia. *Asset Sales Their Role in Restructuring and Financing Firms*. Springer, Cham, Switzerland, 2020.

[210] Andrei Shleifer and Robert W Vishny. Liquidation Values and Debt Capacity: A Market Equilibrium Approach. *Journal of Finance*, 47(4):1343–1366, 1992.

[211] Deloitte. IAS 38 - Intangible Assets. *IAS Plus. Available at: https://www.iasplus.com/en/standards/ias/ias38 (last accessed 01/05/2021)*, 2020.

[212] Deloitte. IAS 39 - Financial Instruments: Recognition and Measurement. *IAS Plus. Available at: https://www.iasplus.com/en/standards/ias/ias39 (last accessed 01/05/2021)*, 2020.

[213] Deloitte. IFRS 9 - Financial Instruments. *IAS Plus. Available at: https://www.iasplus.com/en/standards/ifrs/ifrs9 (last accessed 01/05/2021)*, 2020.

[214] Richard A Lambert, Christian Leuz, and Robert E Verrecchia. Information Asymmetry, Information Precision, and the Cost of Capital. *Review of Finance*, 16(1):1–29, 2012.

[215] Ian A Cooper and Sergei A Davydenko. Estimating the Cost of Risky Debt. *Journal of Applied Corporate Finance*, 19(3):90–95, 2007.

[216] Aswath Damodaran. *Applied Corporate Finance*. John Wiley & Sons, Hoboken, NJ, 3rd edition, 2011.

[217] Mary J Benner and Todd R Zenger. The Lemons Problem in Markets for Strategy. *Strategy Science*, 1(2):71–89, 2016.

[218] Lubomir P Litov, Patrick Moreton, and Todd R Zenger. Corporate Strategy, Analyst Coverage, and the Uniqueness Paradox. *Management Science*, 58(10):1797–1815, 2012.

[219] George A Akerlof. The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, 84(3):488–500, 1970.

[220] Bruce C Greenwald, Joseph E Stiglitz, and Andrew Weiss. Informational Imperfections in the Capital Market and Macro-Economic Fluctuations. *National Bureau of Economic Research Working Paper Series No. 1335*, pages 1–15, 1984.

[221] Christine A Botosan, Marlene A Plumlee, and Yuan Xie. The Role of Information Precision in Determining the Cost of Equity Capital. *Review of Accounting Studies*, 9(2):233–259, 2004.

[222] David Easley and Maureen O'Hara. Information and the Cost of Capital. *Journal of Finance*, 59(4):1553–1583, 2004.

[223] Lakshmi Shyam-Sunder and Stewart C Myers. Testing Static Tradeoff Against Pecking Order Models of Capital Structure. *Journal of Financial Economics*, 51(2):219–244, 1999.

[224] Rolf W Banz. The Relationship Between Return and Market Value of Common Stocks. *Journal of Financial Economics*, 9(1):3–18, 1981.

[225] Simon Benninga. *Financial Modeling*. MIT Press, Cambridge, MA, 4th edition, 2014.

[226] Stephen J Brown and Jerold B Warner. Using Daily Stock Returns: The Case of Event Studies. *Journal of Financial Economics*, 14(1):3–31, 1985.

[227] Stephen J Brown and Jerold B Warner. Measuring Security Price Performance. *Journal of Financial Economics*, 8(3):205–258, 1980.

[228] A Craig MacKinlay. Event Studies in Economics and Finance. *Journal of Economic Literature*, 35(1):13–39, 1997.

[229] Ross Anderson, Rainer Böhme, Richard Clayton, and Tyler Moore. Security Economics and European Policy. *Proceedings of the 7th Workshop on the Economics of Information Security (WEIS) 2008*, pages 1–62, 2008.

[230] Rahul Telang and Sunil Wattal. Impact of Software Vulnerability Announcements on the Market Value of Software Vendors - An Empirical Investigation. *Proceedings of the 4th Workshop on the Economics of Information Security (WEIS) 2005*, pages 1–34, 2005.

[231] Indranil Bose and Alvin Chung Man Leung. The Impact of Adoption of Identity Theft Countermeasures on Firm Value. *Decision Support Systems*, 55(3):753–763, 2013.

[232] Brian L Dos Santos, Ken Peffers, and David C Mauer. The Impact of Information Technology Investment Announcements on the Market Value of the Firm. *Information Systems Research*, 4(1):1–23, 1993.

[233] Kun Shin Im, Kevin E Dow, and Varun Grover. A Reexamination of IT Investment and the Market Value of the Firm - An Event Study Methodology. *Information Systems Research*, 12(1):103–117, 2001.

[234] Debabroto Chatterjee, Carl Pacini, and V Sambamurthy. The Shareholder-Wealth and Trading-Volume Effects of Information-Technology Infrastructure Investments. *Journal of Management Information Systems*, 19(2):7–42, 2002.

[235] Bruce Dehning, Vernon J Richardson, and Robert W Zmud. The Value Relevance of Announcements of Transformational Information Technology Investments. *MIS Quarterly*, 27(4):637–656, 2003.

[236] Manish Agrawal, Rajiv Kishore, and H Raghav Rao. Market Reactions to e-Business Outsourcing Announcements: An Event Study. *Information & Management*, 43(7):861–873, 2006.

[237] Vincent J Shea, Kevin E Dow, Alain Yee-Loong Chong, and Eric W T Ngai. An Examination of the Long-Term Business Value of Investments in Information Technology. *Information Systems Frontiers*, 21:2013–227, 2017.

[238] Jason K Deane, David M Goldberg, Terry R Rakes, and Loren P Rees. The Effect of Information Security Certification Announcements on the Market Value of the Firm. *Information Technology and Management*, 20(3):107–121, 2019.

[239] Feng Xu, Xin (Robert) Luo, Hongyun Zhang, Shan Liu, and Wei (Wayne) Huang. Do Strategy and Timing in IT Security Investments Matter? An Empirical Investigation of the Alignment Effect. *Information Systems Frontiers*, 21(5):1069–1083, 2017.

[240] Indranil Bose and Alvin Chung Man Leung. Adoption of Identity Theft Countermeasures and its Short-and Long-Term Impact on Firm Value. *MIS Quarterly*, 43(1):313–327, 2019.

[241] Christina Y Jeong, Sang-Yong Tom Lee, and Jee-Hae Lim. Information Security Breaches and IT Security Investments: Impacts on Competitors. *Information & Management*, 56(5):681–695, 2018.

[242] Linda Brock and Yair Levy. The Market Value of Information System (IS) Security for e-banking. *Online Journal of Applied Knowledge Management*, 1(1):1–17, 2013.

[243] Wolfgang Böhmer. Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001. In *Second International Conference on Emerging Security Information, Systems and Technologies, 2008. SECURWARE'08.*, pages 224–231. IEEE, 2008.

[244] Juhee Kwon and M Eric Johnson. Proactive Versus Reactive Security Investments in the Healthcare Sector. *MIS Quarterly*, 38(2):451–471, 2014.

[245] Wei Liu, Hideyuki Tanaka, and Kanta Matsuura. An Empirical Analysis of Security Investment in Countermeasures Based on an Enterprise Survey in Japan. *Proceedings of the 5th Workshop on the Economics of Information Security (WEIS) 2006*, pages 1–15, 2006.

[246] Mukul Gupta, Alok R Chaturvedi, Shailendra Mehta, and Lorenzo Valeri. The Experimental Analysis of Information Security Management Issues for Online Financial Services. *Proceedings of the 21st International Conference on Information Systems*, pages 667–675, 2000.

[247] Daniel W Woods and Andrew C Simpson. Monte Carlo Methods to Investigate How Aggregated Cyber Insurance Claims Data Impacts Security Investments. *Proceedings of the 17th Workshop on the Economics of Information Security (WEIS) 2018*, pages 1–24, 2018.

[248] Daniel W Woods, Ioannis Agrafiotis, Jason R C Nurse, and Sadie Creese. Mapping the Coverage of Security Controls in Cyber Insurance Proposal Forms. *Journal of Internet Services and Applications*, 8(1):8, 2017.

[249] Tridib Bandyopadhyay and Vijay Mookerjee. A Model to Analyze the Challenge of Using Cyber Insurance. *Information Systems Frontiers*, 21(2):301–325, 2019.

[250] Sasha Romanosky, Lillian Ablon, Andreas Kuehn, and Therese Jones. Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk? *Journal of Cybersecurity*, 5(1):1–19, 2019.

[251] Constance E Helfat and David J Teece. Vertical Integration and Risk Reduction. *Journal of Law, Economics, and Organization*, 3(1):47–67, 1987.

[252] Michael Lubatkin and Hugh M O'Neill. Merger Strategies and Capital Market Risk. *Academy of Management Journal*, 30(4):665–684, 1987.

[253] Pablo T Spiller. On Vertical Mergers. *Journal of Law, Economics, and Organization*, 1(2):285–312, 1985.

[254] Michael Lubatkin and Ronald C Rogers. Diversification, Systematic Risk, and Shareholder Return: A Capital Market Extension of Rumelt's 1974 Study. *Academy of Management Journal*, 32(2):454–465, 1989.

[255] Sayan Chatterjee, Michael Lubatkin, and Timothy Schoenecker. Vertical Strategies and Market Structure: A Systematic Risk Analysis. *Organization Science*, 3(1):138–156, 1992.

[256] Seth W Norton. Vertical Integration and Systematic Risk: Oil Refining Revisited. *Journal of Institutional and Theoretical Economics*, 149(4):656–669, 1993.

[257] Baruch Lev. On the Association Between Operating Leverage and Risk. *Journal of Financial and Quantitative Analysis*, 9(4):627–641, 1974.

[258] Gershon N Mandelker and S Ghon Rhee. The Impact of the Degrees of Operating and Financial Leverage on Systematic Risk of Common Stock. *Journal of Financial and Quantitative Analysis*, 19(1):45–57, 1984.

[259] Frank J Fabozzi and Jack C Francis. Stability Tests for Alphas and Betas over Bull and Bear Market Conditions. *Journal of Finance*, 32(4):1093–1099, 1977.

[260] Moon K Kim and J Kenton Zumwalt. An Analysis of Risk in Bull and Bear Markets. *Journal of Financial and Quantitative Analysis*, 14(5):1015–1025, 1979.

[261] Ravinder K Bhardwaj and LeRoy D Brooks. Dual Betas from Bull and Bear Markets: Reversal of the Size Effect. *Journal of Financial Research*, 16(4):269–283, 1993.

[262] James Chong and G Michael Phillips. Measuring Risk for Cost of Capital: The Downside Beta Approach. *Journal of Corporate Treasury Management*, 4(4):344–352, 2012.

[263] James B Wiggins. Betas in Up and Down Markets. *Financial Review*, 27(1):107–123, 1992.

[264] Glenn Pettengill, Sridhar Sundaram, and Ike Mathur. Payment For Risk: Constant Beta vs. Dual-Beta Models. *Financial Review*, 37(2):123–135, 2002.

[265] Robert Faff. A Multivariate Test of a Dual-Beta CAPM: Australian Evidence. *Financial Review*, 36(4):157–174, 2001.

[266] Frank J Fabozzi and Jack C Francis. Mutual Fund Systematic Risk for Bull and Bear Markets: An Empirical Examination. *Journal of Finance*, 34(5):1243–1250, 1979.

[267] Andrew J Patton and Michela Verardo. Does Beta Move with News? Firm-Specific Information Flows and Learning about Profitability. *The Review of Financial Studies*, 25(9):2789–2839, 2012.

[268] Ray Ball and S P Kothari. Security Returns Around Earnings Announcements. *The Accounting Review*, 66(4):718–738, 1991.

[269] Theoharry Grammatikos and Robert Vermeulen. The 2007–2009 Financial Crisis: Changing Market Dynamics and the Impact of Credit Supply and Aggregate Demand Sensitivity. *Applied Economics*, 46(8):895–911, 2014.

[270] Taha Havakhor, Mohammad S Rahman, and Tianjian Zhang. Cybersecurity Investments and the Cost of Capital. *Proceedings of the 19th Workshop on the Economics of Information Security (WEIS) 2020*, pages 1–48, 2020.

[271] Faheem Ahmed Shaikh and Damien Joseph. Effects of Information Security Legitimacy on Data Breach Consequences: Moderating Effect of Impression Management. *Proceedings of the 2019 ACM Computers and People Research Conference*, pages 118–121, 2019.

[272] Amos Tversky and Daniel Kahneman. Loss Aversion in Riskless Choice: A Reference-dependent Model. *The Quarterly Journal of Economics*, 106(4):1039–1061, 1991.

[273] Amos Tversky and Daniel Kahneman. Advances in Prospect Theory: Cumulative Representation of Uncertainty. *Journal of Risk and Uncertainty*, 5(4):297–323, 1992.

[274] Daniel Kahneman and Amos Tversky. Prospect Theory: An Analysis of Decision Under Risk. *Econometrica*, 47(2):263–291, 1979.

[275] Robert S Kaplan. Accounting Scholarship that Advances Professional Knowledge and Practice. *The Accounting Review*, 86(2):367–383, 2011.

[276] S&P Global Ratings. Default, Transition, and Recovery: 2019 Annual Global Corporate Default And Rating Transition Study. *Available at: https://www.spglobal.com/ratings/en/research/articles/200429-default-transition-and-recovery-2019-annual-global-corporate-default-and-rating-transition-study-11444862 (last accessed 01/05/2021)*, 2020.

[277] Michael Minnis. The Value of Financial Statement Verification in Debt Financing: Evidence from Private US Firms. *Journal of Accounting Research*, 49(2):457–506, 2011.

[278] Jules H Van Binsbergen, John R Graham, and Jie Yang. The Cost of Debt. *Journal of Finance*, 65(6):2089–2136, 2010.

[279] Jennifer Francis, Ryan LaFond, Per Olsson, and Katherine Schipper. The Market Pricing of Accruals Quality. *Journal of Accounting and Economics*, 39(2):295–327, 2005.

[280] Jeffrey A Pittman and Steve Fortin. Auditor Choice and the Cost of Debt Capital for Newly Public Firms. *Journal of Accounting and Economics*, 37(1):113–136, 2004.

[281] Seth Armitage. *The Cost of Capital: Intermediate Theory*. Cambridge University Press, Cambridge, UK, 2005.

[282] Lara Cathcart, Nina M Gotthelf, Matthias Uhl, and Yining Shi. News Sentiment and Sovereign Credit Risk. *European Financial Management*, 26(2):261–287, 2020.

[283] Charles W Haley. A Note on the Cost of Debt. *Journal of Financial and Quantitative Analysis*, 1(4):72–93, 1966.

[284] Partha Sengupta. Corporate Disclosure Quality and the Cost of Debt. *The Accounting Review*, 73(4):459–474, 1998.

[285] Sandro C Andrade, Gennaro Bernile, and Frederick M Hood. SOX, Corporate Transparency, and the Cost of Debt. *Journal of Banking & Finance*, 38:145–165, 2014.

[286] Darrell Duffie. Credit Swap Valuation. *Financial Analysts Journal*, 55(1):73–87, 1999.

[287] Nuno Fernandes. *Finance for Executives: A Practical Guide for Managers*. NPV Publishing, London, UK, 2014.

[288] Jeffrey L Callen, Joshua Livnat, and Dan Segal. The Impact of Earnings on the Pricing of Credit Default Swaps. *The Accounting Review*, 84(5):1363–1394, 2009.

[289] Francis A Longstaff, Sanjay Mithal, and Eric Neis. Corporate Yield Spreads: Default Risk or Liquidity? New Evidence from the Credit Default Swap Market. *Journal of Finance*, 60(5):2213–2253, 2005.

[290] John Hull, Mirela Predescu, and Alan White. The Relationship Between Credit Default Swap Spreads, Bond Yields, and Credit Rating Announcements. *Journal of Banking & Finance*, 28(11):2789–2811, 2004.

[291] Haibin Zhu. An Empirical Comparison of Credit Spreads Between the Bond Market and the Credit Default Swap Market. *Journal of Financial Services Research*, 29(3):211–235, 2006.

[292] Roberto Blanco, Simon Brennan, and Ian W Marsh. An Empirical Analysis of the Dynamic Relation Between Investment-Grade Bonds and Credit Default Swaps. *Journal of Finance*, 60(5):2255–2281, 2005.

[293] Edwin J Elton, Martin J Gruber, Deepak Agrawal, and Christopher Mann. Explaining the Rate Spread on Corporate Bonds. *Journal of Finance*, 56(1):247–277, 2001.

[294] Joshua Aizenman, Michael Hutchison, and Yothin Jinjarak. What is the Risk of European Sovereign Debt Defaults? Fiscal Space, CDS Spreads and Market Pricing of Risk. *Journal of International Money and Finance*, 34:37–59, 2013.

[295] Lakshmanan Shivakumar, Oktay Urcan, Florin P Vasvari, and Li Zhang. The Debt Market Relevance of Management Earnings Forecasts: Evidence from Before and During the Credit Crisis. *Review of Accounting Studies*, 16(3):464–486, 2011.

[296] EY. Practitioner's Guide to Cost of Capital & WACC Calculation. *Available at: https://web.archive.org/web/20200301160742/https://www.eycom.ch/en/Publications/20200227-Practitioners-guide-to-cost-of-capital-And-WACC-calculation/download (last accessed 01/05/2021)*, pages 1–25, 2020.

[297] Aswath Damodaran. The Credit Default Swap (CDS) Market. *Available at: https://web.archive.org/web/20190818093008/http://aswathdamodaran.blogspot.com/2010/02/credit-default-swap-cds-market.html (last accessed 01/05/2021)*, 2010.

[298] Florian Kiesel and Jonathan Spohnholtz. CDS Spreads as an Independent Measure of Credit Risk. *Journal of Risk Finance*, 18(2):122–144, 2017.

[299] John C Hull. *Risk Management and Financial Institutions*. John Wiley & Sons, Hoboken, NJ, 3rd edition, 2012.

[300] John C Hull and Alan D White. The Valuation of Credit Default Swap Options. *Journal of Derivatives*, 10(3):40–50, 2003.

[301] Jan Annaert, Marc De Ceuster, Patrick Van Roy, and Cristina Vespro. What Determines Euro Area Bank CDS Spreads? *Journal of International Money and Finance*, 32:444–461, 2013.

[302] Jun Pan and Kenneth J Singleton. Default and Recovery Implicit in the Term Structure of Sovereign CDS Spreads. *Journal of Finance*, 63(5):2345–2384, 2008.

[303] Giovanni Calice, Jing Chen, and Julian Williams. Liquidity Spillovers in Sovereign Bond and CDS Markets: An Analysis of the Eurozone Sovereign Debt Crisis. *Journal of Economic Behavior & Organization*, 85:122–143, 2013.

[304] Ivan T Ivanov, Joao A C Santos, and Thu Vo. The Transformation of Banking: Tying Loan Interest Rates to Borrowers' CDS Spreads. *Journal of Corporate Finance*, 38:150–165, 2016.

[305] John C Hull and A White. Valuing Credit Default Swaps I: No Counterparty Default Risk. *Journal of Derivatives*, 8(1):29–40, 2000.

[306] Hentry He Huang and Chong Wang. Do Banks Price Firms' Data Breaches. *The Accounting Review*, 96(3):261–286, 2021.

[307] Subramanian R Iyer, Betty J Simkins, and Heng Wang. Cyberattacks and Impact on Bond Valuation. *Finance Research Letters*, 33:1–11, 2020.

[308] Lijing Du. The CDS Market Reaction to Restatement Announcements. *Journal of Business Finance & Accounting*, 44(7-8):1015–1035, 2017.

[309] Patrick Augustin, Marti G Subrahmanyam, Dragon Yongjun Tang, and Sarah Qian Wang. Credit Default Swaps - A survey. *Foundations and Trends in Finance*, 9(1-2):1–196, 2014.

[310] Lars Norden and Martin Weber. Informational Efficiency of Credit Default Swap and Stock Markets: The Impact of Credit Rating Announcements. *Journal of Banking & Finance*, 28(11):2813–2843, 2004.

[311] Andreas Wengner, Hans-Peter Burghof, and Johannes Schneider. The Impact of Credit Rating Announcements on Corporate CDS Markets - Are Intra-Industry Effects Observable? *Journal of Economics and Business*, 78:79–91, 2015.

[312] Koresh Galil and Gil Soffer. Good News, Bad News and Rating Announcements: An Empirical Investigation. *Journal of Banking & Finance*, 35(11):3101–3119, 2011.

[313] Marian Micu, Eli M Remolona, and Philip D Wooldridge. The Price Impact of Rating Announcements: Which Announcements Matter? *Bank for International Settlements (BIS) Working Paper No. 207*, 2006.

[314] John D Finnerty, Cameron D Miller, and Ren-Raw Chen. The Impact of Credit Rating Announcements on Credit Default Swap Spreads. *Journal of Banking & Finance*, 37(6):2011–2030, 2013.

[315] Rosella Castellano and Luisa Scaccia. CDS and Rating Announcements: Changing Signaling during the Crisis? *Review of Managerial Science*, 6(3):239–264, 2012.

[316] Olivier Nataf and Lieven De Moor. Debt Rating Downgrades of Financial Institutions: Causality Tests on Single-Issue CDS and iTraxx. *Quantitative Finance*, 19(12):1975–1993, 2019.

[317] Sanjiv R Das, Paul Hanouna, and Atulya Sarin. Accounting-Based Versus Market-Based Cross-Sectional Models of CDS Spreads. *Journal of Banking & Finance*, 33(4):719–730, 2009.

[318] George Batta. The Direct Relevance of Accounting Information for Credit Default Swap Pricing. *Journal of Business Finance & Accounting*, 38(9-10):1096–1122, 2011.

[319] George Eli Batta, Jiaping Qiu, and Fan Yu. Credit Derivatives and Analyst Behavior. *The Accounting Review*, 91(5):1315–1343, 2016.

[320] Maria Correia, Scott Richardson, and İrem Tuna. Value Investing in Credit Markets. *Review of Accounting Studies*, 17(3):572–609, 2012.

[321] Paul A Griffin. The Market for Credit Default Swaps: New Insights Into Investors' Use of Accounting Information? *Accounting & Finance*, 54(3):847–883, 2014.

[322] Caitlin A Greatrex. The Credit Default Swap Market's Reaction to Earnings Announcements. *Journal of Applied Finance*, 19(1-2):193–216, 2009.

[323] Gaiyan Zhang and Sanjian Zhang. Information Efficiency of the US Credit Default Swap Market: Evidence from Earnings Surprises. *Journal of Financial Stability*, 9(4):720–730, 2013.

[324] Pervaiz Alam, Xiaoling Pu, and Barry Hettler. The Sensitivity of the Credit Default Swap Market to Financial Analysts' Forecast Revisions. *Accounting & Finance*, 58(3):697–725, 2018.

[325] Paulo Pereira da Silva. Earnings Surprises and the Response of CDS Markets. *Studies in Economics and Finance*, 33(3):377–402, 2016.

[326] Pepa Kraft, Wayne R Landsman, and Zilu Shan. Effect of Mandatory IFRS Adoption on Accounting-Based Prediction Models for CDS Spreads. *European Accounting Review*, 30(2):223–250, 2020.

[327] Gauri Bhat, Jeffrey L Callen, and Dan Segal. Credit Risk and IFRS: The Case of Credit Default Swaps. *Journal of Accounting, Auditing & Finance*, 29(2):129–162, 2014.

[328] Tzu-Ting Chiu, Yuyan Guan, and Jeong-Bon Kim. The Effect of Risk Factor Disclosures on the Pricing of Credit Default Swaps. *Contemporary Accounting Research*, 35(4):2191–2224, 2018.

[329] Carlos Alves, Victor Mendes, and Paulo Pereira da Silva. Do Stress Tests Matter? A Study on the Impact of the Disclosure of Stress Test Results on European Financial Stocks and CDS Markets. *Applied Economics*, 47(12):1213–1229, 2015.

[330] Danilo Drago, Concetta Carnevale, and Raffaele Gallo. Do Corporate Social Responsibility Ratings Affect Credit Default Swap Spreads? *Corporate Social Responsibility and Environmental Management*, 26(3):644–652, 2019.

[331] Denisa Lleshaj and Jannik Kocian. Short Selling Disclosure and Its Impact on CDS Spreads. *The European Journal of Finance*, In Press:1–34, 2020.

[332] Lindsay Baran, Ying Li, Chang Liu, Zilong Liu, and Xiaoling Pu. S&P 500 Index Revisions and Credit Spreads. *Review of Financial Economics*, 36(4):348–363, 2018.

[333] Joachim Rojahn and Florian Zechser. The Effect of Corporate Diversification on Credit Risk: New Evidence from European Credit Default Swap Spreads. *Accounting & Finance*, 59(4):2679–2704, 2019.

[334] Hayne E Leland and David H Pyle. Informational Asymmetries, Financial Structure, and Financial Intermediation. *Journal of Finance*, 32(2):371–387, 1977.

[335] Joseph E Stiglitz and Andrew Weiss. Credit Rationing in Markets with Imperfect Information. *The American Economic Review*, 71(3):393–410, 1981.

[336] Douglas W Diamond. Optimal Release of Information by Firms. *Journal of Finance*, 40(4):1071–1094, 1985.

[337] Securities and Exchange Commission. Commission Statement and Guidance on Public Company Cybersecurity Disclosures. *Available at: https://www.sec.gov/rules/interp/2018/33-10459.pdf (last accessed 01/05/2021)*, 2018.

[338] Shai Levi and Xiao-Jun Zhang. Do Temporary Increases in Information Asymmetry Affect the Cost of Equity? *Management Science*, 61(2):354–371, 2015.

[339] Yakov Amihud and Haim Mendelson. Asset Pricing and the Bid-Ask Spread. *Journal of Financial Economics*, 17(2):223–249, 1986.

[340] Thomas E Copeland and Dan Galai. Information Effects on the Bid-Ask Spread. *Journal of Finance*, 38(5):1457–1469, 1983.

[341] Lawrence R Glosten and Paul R Milgrom. Bid, Ask and Transaction Prices in a Specialist Market with Heterogeneously Informed Traders. *Journal of Financial Economics*, 14(1):71–100, 1985.

[342] Christian Leuz and Robert E Verrecchia. The Economic Consequences of Increased Disclosure. *Journal of Accounting Research*, 38:91–124, 2000.

[343] Sadok El Ghoul, Omrane Guedhami, Yang Ni, Jeffrey Pittman, and Samir Saadi. Does Information Asymmetry Matter to Equity Pricing? Evidence from Firms' Geographic Location. *Contemporary Accounting Research*, 30(1):140–181, 2013.

[344] Nilabhra Bhattacharya, Frank Ecker, Per M Olsson, and Katherine Schipper. Direct and Mediated Associations among Earnings Quality, Information Asymmetry, and the Cost of Equity. *The Accounting Review*, 87(2):449–482, 2012.

[345] Christine A Botosan and Marlene A Plumlee. Are Information Attributes Priced? *Journal of Business Finance & Accounting*, 40(9-10):1045–1067, 2013.

[346] Jefferson Duarte, Xi Han, Jarrad Harford, and Lance Young. Information Asymmetry, Information Dissemination and the Effect of Regulation FD on the Cost of Capital. *Journal of Financial Economics*, 87(1):24–44, 2008.

[347] David Easley, Soeren Hvidkjaer, and Maureen O'Hara. Is Information Risk a Determinant of Asset Returns? *Journal of Finance*, 57(5):2185–2221, 2002.

[348] William Peng He, Andrew Lepone, and Henry Leung. Information Asymmetry and the Cost of Equity Capital. *International Review of Economics & Finance*, 27:611–620, 2013.

[349] François Derrien, Ambrus Kecskés, and Sattar A Mansi. Information Asymmetry, the Cost of Debt, and Credit Events: Evidence from Quasi-Random Analyst Disappearances. *Journal of Corporate Finance*, 39:295–311, 2016.

[350] Tony T Tang. Information Asymmetry and Firms' Credit Market Access: Evidence from Moody's Credit Rating Format Refinement. *Journal of Financial Economics*, 93(2):325–351, 2009.

[351] John S Hughes, Jing Liu, and Jun Liu. Information Asymmetry, Diversification, and Cost of Capital. *The Accounting Review*, 82(3):705–729, 2007.

[352] Anne Beyer, Daniel A Cohen, Thomas Z Lys, and Beverly R Walther. The Financial Reporting Environment: Review of the Recent Literature. *Journal of Accounting and Economics*, 50(2-3):296–343, 2010.

[353] John McInnis. Earnings Smoothness, Average Returns, and Implied Cost of Equity Capital. *The Accounting Review*, 85(1):315–341, 2010.

[354] John Affleck-Graves, Carolyn M Callahan, and Niranjan Chipalkatti. Earnings Predictability, Information Asymmetry, and Market Liquidity. *Journal of Accounting Research*, 40(3):561–583, 2002.

[355] Kiridaran Kanagaretnam, Gerald J Lobo, and Dennis J Whalen. Does Good Corporate Governance Reduce Information Asymmetry Around Quarterly Earnings Announcements? *Journal of Accounting and Public Policy*, 26(4):497–522, 2007.

[356] Nilabhra Bhattacharya, Hemang Desai, and Kumar Venkataraman. Does Earnings Quality Affect Information Asymmetry? Evidence from Trading Costs. *Contemporary Accounting Research*, 30(2):482–516, 2013.

[357] Faten Lakhal. Stock Market Liquidity and Information Asymmetry Around Voluntary Earnings Disclosures: New Evidence from France. *International Journal of Managerial Finance*, 4(1):60–75, 2008.

[358] Itzhak Krinsky and Jason Lee. Earnings Announcements and the Components of the Bid-Ask Spread. *Journal of Finance*, 51(4):1523–1535, 1996.

[359] Charles M C Lee, Belinda Mucklow, and Mark J Ready. Spreads, Depths, and the Impact of Earnings Information: An Intraday Analysis. *The Review of Financial Studies*, 6(2):345–374, 1993.

[360] Stephen Brown, Stephen A Hillegeist, and Kin Lo. The Effect of Earnings Surprises on Information Asymmetry. *Journal of Accounting and Economics*, 47(3):208–225, 2009.

[361] P C Venkatesh and Raymond Chiang. Information Asymmetry and the Dealer's Bid-Ask Spread: A Case Study of Earnings and Dividend Announcements. *Journal of Finance*, 41(5):1089–1102, 1986.

[362] Zoe-Vonna Palmrose, Vernon J Richardson, and Susan Scholz. Determinants of Market Reactions to Restatement Announcements. *Journal of Accounting and Economics*, 37(1):59–89, 2004.

[363] Maribeth Coller and Teri L Yohn. Management Forecasts and Information Asymmetry: An Examination of Bid-Ask Spreads. *Journal of Accounting Research*, 35(2):181–191, 1997.

[364] Alex Frino, Stewart Jones, and Jin Boon Wong. Market Behaviour Around Bankruptcy Announcements: Evidence from the Australian Stock Exchange. *Accounting & Finance*, 47(4):713–730, 2007.

[365] Moshe Hagigi, Brian D Kluger, and David Shields. Auditor Change Announcements and Dispersion of Investor Expectations. *Journal of Business Finance & Accounting*, 20(6):787–802, 1993.

[366] Diana R Franz, Ramesh P Rao, and Niranjan Tripathy. Informed Trading Risk and Bid-Ask Spread Changes Around Open Market Stock Repurchases in the Nasdaq Market. *Journal of Financial Research*, 18(3):311–327, 1995.

[367] Joon Chae. Trading Volume, Information Asymmetry, and Timing Information. *Journal of Finance*, 60(1):413–442, 2005.

[368] Ahmed Barakat, Anna Chernobai, and Mark Wahrenburg. Information Asymmetry Around Operational Risk Announcements. *Journal of Banking & Finance*, 48:152–179, 2014.

[369] Raymond M Brooks, Ajay Patel, and Tie Su. How the Equity Market Responds to Unanticipated Events. *The Journal of Business*, 76(1):109–133, 2003.

[370] Yong Jick Lee, Robert J Kauffman, and Ryan Sougstad. Profit-Maximizing Firm Investments in Customer Information Security. *Decision Support Systems*, 51(4):904–920, 2011.

[371] Palaniappan Shamala, Rabiah Ahmad, and Mariana Yusoff. A Conceptual Framework of Info Structure for Information Security Risk Assessment (ISRA). *Journal of Information Security and Applications*, 18(1):45–52, 2013.

[372] Pierangelo Rosati, Mark Cummins, Peter Deeney, Fabian Gogolin, Lisa van der Werff, and Theo Lynn. The Effect of Data Breach Announcements Beyond the Stock Price: Empirical Evidence on Market Activity. *International Review of Financial Analysis*, 49:146–154, 2017.

[373] Shariful Islam. *Three Essays on Information Security Breaches and Big Data Analytics: Accounting and Auditing Perspective*. PhD thesis, Louisiana Tech University, 2019.

[374] Andros Gregoriou, Christos Ioannidis, and Len Skerratt. Information Asymmetry and the Bid-Ask Spread: Evidence from the UK. *Journal of Business Finance & Accounting*, 32(9-10):1801–1826, 2005.

[375] Roger D Huang and Hans R Stoll. The Components of the Bid-Ask Spread: A General Approach. *The Review of Financial Studies*, 10(4):995–1034, 1997.

[376] Roger D Huang and Hans R Stoll. Dealer Versus Auction Markets: A Paired Comparison of Execution Costs on NASDAQ and the NYSE. *Journal of Financial Economics*, 41(3):313–357, 1996.

[377] Albert S Kyle. Continuous Auctions and Insider Trading. *Econometrica*, 53(6):1315–1335, 1985.

[378] Anat R Admati and Paul Pfleiderer. A Theory of Intraday Patterns: Volume and Price Variability. *The Review of Financial Studies*, 1(1):3–40, 1988.

[379] F Douglas Foster and Sean Viswanathan. A Theory of the Interday Variations in Volume, Variance, and Trading Costs in Securities Markets. *The Review of Financial Studies*, 3(4):593–624, 1990.

[380] Sarine Karajian and Saif Ullah. Consequences of Fraud and Overcoming Negative Market Reaction. *Global Finance Journal*, In Press:1–19, 2021.

[381] Christian Biener, Martin Eling, and Jan H Wirfs. Insurability of Cyber Risk: An Empirical Analysis. *The Geneva Papers on Risk and Insurance: Issues and Practice*, 40:131–158, 2015.

[382] Lawrence A Gordon, Martin P Loeb, and Tashfeen Sohail. A Framework for Using Insurance for Cyber-Risk Management. *Communications of the ACM*, 46(3):81–85, 2003.

[383] Joseph D Piotroski and Darren T Roulstone. Do Insider Trades Reflect both Contrarian Beliefs and Superior Knowledge About Future Cash Flow Realizations? *Journal of Accounting and Economics*, 39(1):55–81, 2005.

[384] Nihat Aktas, Eric de Bodt, and Hervé Van Oppens. Legal Insider Trading and Market Efficiency. *Journal of Banking and Finance*, 32(7):1379–1392, 2008.

[385] Dennis W Carlton and Daniel R Fischel. The Regulation of Insider Trading. *Stanford Law Review*, 35(5):857–895, 1983.

[386] Russell W Coff and Peggy M Lee. Insider Trading as a Vehicle to Appropriate Rent from R&D. *Strategic Management Journal*, 24(2):183–190, 2003.

[387] Hayne E Leland. Insider Trading: Should It Be Prohibited? *Journal of Political Economy*, 100(4):859–887, 1992.

[388] Henry G Manne. *Insider Trading and the Stock Market*. Free Press, New York City, NY, 1966.

[389] Gautam Ahuja, Russell W Coff, and Peggy M Lee. Managerial Foresight and Attempted Rent Appropriation: Insider Trading on Knowledge of Imminent Breakthroughs. *Strategic Management Journal*, 26(9):791–808, 2005.

[390] Jana P Fidrmuc, Adriana Korczak, and Piotr Korczak. Why Does Shareholder Protection Matter for Abnormal Returns After Reported Insider Purchases and Sales? *Journal of Banking and Finance*, 37(6):1915–1935, 2013.

[391] Jana P Fidrmuc, Marc Goergen, and Luc Renneboog. Insider Trading, News Releases, and Ownership Concentration. *Journal of Finance*, 61(6):2931–2973, 2006.

[392] Aswath Damodaran and Crocker H Liu. Insider Trading as a Signal of Private Information. *The Review of Financial Studies*, 6(1):79–119, 1993.

[393] Kose John and Banikanta Mishra. Information Content of Insider Trading Around Corporate Announcements: The Case of Capital Expenditures. *Journal of Finance*, 45(3):835–855, 1990.

[394] Joseph E Finnerty. Insiders and Market Efficiency. *Journal of Finance*, 31(4):1141–1148, 1976.

[395] Jeffrey F Jaffe. Special Information and Insider Trading. *The Journal of Business*, 47(3):410–428, 1974.

[396] Josef Lakonishok and Inmoo Lee. Are Insider Trades Informative? *The Review of Financial Studies*, 14(1):79–111, 2001.

[397] H Nejat Seyhun. Insiders' Profits, Costs of Trading, and Market Efficiency. *Journal of Financial Economics*, 16(2):189–212, 1986.

[398] Wolfgang Aussenegg, Ranko Jelic, and Robert Ranzi. Corporate Insider Trading in Europe. *Journal of International Financial Markets, Institutions and Money*, 54:27–42, 2018.

[399] Kaspar Dardas and Andre Güttler. Are Directors' Dealings Informative? Evidence from European Stock Markets. *Financial Markets and Portfolio Management*, 25(2):111–148, 2011.

[400] Arturo Bris. Do Insider Trading Laws Work? *European Financial Management*, 11(3):267–312, 2005.

[401] Bikki Jaggi and Judy Tsui. Insider Trading, Earnings Management and Corporate Governance: Empirical Evidence based on Hong Kong Firms. *Journal of International Financial Management & Accounting*, 18(3):192–222, 2007.

[402] Lauren Cohen, Christopher Malloy, and Lukasz Pomorski. Decoding Inside Information. *Journal of Finance*, 67(3):1009–1043, 2012.

[403] Joseph E Finnerty. Insiders' Activity and Inside Information: A Multivariate Analysis. *Journal of Financial and Quantitative Analysis*, 11(2):205–215, 1976.

[404] Peter F Pope, Richard C Morris, and David A Peel. Insider Trading: Some Evidence on Market Efficiency and Directors' Share Dealings in Great Britain. *Journal of Business Finance & Accounting*, 17(3):359–380, 1990.

[405] Arthur J Keown and John M Pinkerton. Merger Announcements and Insider Trading Activity: An Empirical Investigation. *Journal of Finance*, 36(4):855–869, 1981.

[406] Jonathan M Karpoff and Daniel Lee. Insider Trading Before New Issue Announcements. *Financial Management*, 20(1):18–26, 1991.

[407] Kose John and Larry H P Lang. Insider Trading Around Dividend Announcements: Theory and Evidence. *Journal of Finance*, 46(4):1361–1389, 1991.

[408] David Aboody and Baruch Lev. Information Asymmetry, R&D, and Insider Gains. *Journal of Finance*, 55(6):2747–2766, 2000.

[409] Russell W Coff. The Coevolution of Rent Appropriation and Capability Development. *Strategic Management Journal*, 31(7):711–733, 2010.

[410] Sylvain Friederich, Alan Gregory, John Matatko, and Ian Tonks. Short-Run Returns Around the Trades of Corporate Insiders on the London Stock Exchange. *European Financial Management*, 8(1):7–30, 2002.

[411] Ali Ataullah, Marc Goergen, and Hang Le. Insider Trading and Financing Constraints. *Financial Review*, 49(4):685–712, 2014.

[412] Kee H Chung and Charlie Charoenwong. Insider Trading and the Bid-Ask Spread. *Financial Review*, 33(3):1–20, 1998.

[413] Taha Havakhor, Obi Ogbanufe, and Anthony Vance. Can Insider Trades Reliably Predict Cybersecurity Hazards in Public Firms? *Proceedings of the 19th Workshop on the Economics of Information Security (WEIS) 2020*, pages 1–25, 2020.

[414] Dennis D Malliouris. Insider Trading on Security Breaches. *Unpublished CDT First-Year Mini-Project 1 Report*, pages 1–16, 2018.

[415] Joshua Mitts and Eric L Talley. Informed Trading and Cybersecurity Breaches. *Harvard Business Law Review*, 9(1):1–51, 2019.

[416] Zhaoxin Lin, Travis R A Sapp, Jackie Rees Ulmer, and Rahul Parsa. Insider Trading Ahead of Cyber Breach Announcements. *Journal of Financial Markets*, 50:1–15, 2020.

[417] Heng Emily Wang, Qin Emma Wang, and Wentao Wu. Short Selling Surrounding Data Breach Announcements. *Working Paper available at SSRN: https://ssrn.com/abstract=3554487*, pages 1–41, 2020.

[418] Louis R Piccotti and Heng Emily Wang. Informed Trading Surrounding Data Breaches in Options Markets. *Working Paper available at SSRN: https://ssrn.com/abstract=3478263*, 2021.

[419] Henk Berkman, Jonathan Jona, Gladys Lee, and Naomi S Soderstrom. Digital Insiders and Informed Trading Before Earnings Announcements. *Working Paper available at SSRN: https://ssrn.com/abstract=3180531*, pages 1–45, 2019.

[420] Bloomberg. Three Equifax Managers Sold Stock Before Cyber Hack Revealed. *Available at: https://www.bloomberg.com/news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack (last accessed 01/05/2021)*, 2017.

[421] Bloomberg. Equifax CIO Put '2 and 2 Together' Then Sold Stock, SEC Says. *Available at: https://www.bloomberg.com/news/articles/2018-03-14/sec-says-former-equifax-executive-engaged-in-insider-trading (last accessed 01/05/2021)*, 2018.

[422] Bloomberg. Intel CEO's Stock Sales May Warrant SEC Examination. *Available at: https://www.bloomberg.com/news/articles/2018-01-08/intel-ceo-krzanich-s-stock-sales-seen-warranting-sec-examination (last accessed 01/05/2021)*, 2018.

[423] Francis Fukuyama. *Trust: The Social Virtues and the Creation of Prosperity*. Free Press, New York City, NY, 1995.

[424] Manuel Beccerra and Anil K Gupta. Trust Within the Organization: Integrating the Trust Literature with Agency Theory and Transaction Costs Economics. *Public Administration Quarterly*, 23(2):177–203, 1999.

[425] Paul A Pavlou, Huigang Liang, and Yajiong Xue. Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective. *MIS Quarterly*, 31(1):105–136, 2007.

[426] Thomas C Schelling. An Essay on Bargaining. *The American Economic Review*, 46(3):281–306, 1956.

[427] David Knights, Faith Noble, Theo Vurdubakis, and Hugh Willmott. Chasing Shadows: Control, Virtuality and the Production of Trust. *Organization Studies*, 22(2):311–336, 2001.

[428] Crown Commercial Service. Procurement Policy Note: Cyber Essentials Scheme. *Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/526200/ppn_update_cyber_essentials_0914.pdf (last accessed 01/05/2021)*, 2016.

[429] Department for Digital Culture Media & Sport. Cyber Essentials Scheme: Overview. *Available at: https://www.gov.uk/government/publications/cyber-essentials-scheme-overview (last accessed 01/05/2021)*, 2018.

[430] National Cyber Security Centre (NCSC). Cyber Essentials: Requirements for IT Infrastructure. *Available at: https://www.cyberessentials.ncsc.gov.uk/requirements-for-it-infrastructure (last accessed 01/12/2018)*, 2018.

[431] National Cyber Security Centre (NCSC). Cyber Essentials: Getting Certified. *Available at: https://www.cyberessentials.ncsc.gov.uk/getting-certified/ (last accessed 01/12/2018)*, 2018.

[432] International Organization for Standardization. ISO/IEC 27000 Family - Information Security Management Systems. *Available at: https://www.iso.org/isoiec-27001-information-security.html (last accessed 10/04/2021)*, 2018.

[433] International Organization for Standardization. ISO/IEC 27001:2013(en) Information Technology - Security Techniques - Information Security Management Systems - Requirements. *ISO Standards. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en (last accessed 01/05/2021)*, 2013.

[434] International Organization for Standardization. The ISO Survey of Management System Standard Certifications - 2019 - Explanatory Note. *Available at: https://isotc.iso.org/livelink/livelink/fetch/-8853493/8853511/8853520/18808772/0._Explanatory_note_and_overview_on_ISO_Survey_2019_results.pdf?nodeid=21413237&vernum=-2 (last accessed 01/05/2021)*, 2020.

[435] Spencer Wheatley, Annette Hofmann, and Didier Sornette. Data Breaches in the Catastrophe Framework & Beyond. *arXiv preprint arXiv:1901.00699*, pages 1–23, 2019.

[436] Fabio Bisogni, Hadi Asghari, and Michel J G Van Eeten. Estimating the Size of the Iceberg from its Tip. *Proceedings of the 16th Workshop on the Economics of Information Security (WEIS) 2017*, pages 1–29, 2017.

[437] Joseph Buckman, Jesse C Bockstedt, Matthew J Hashim, and Tiemen Woutersen. Do Organizations Learn from a Data Breach? *Proceedings of the 16th Workshop on the Economics of Information Security (WEIS) 2017*, pages 1–22, 2017.

[438] Kian-Ping Lim and Robert Brooks. The Evolution of Stock Market Efficiency Over Time: A Survey of the Empirical Literature. *Journal of Economic Surveys*, 25(1):69–108, 2011.

[439] Fang Frank Yu. Analyst Coverage and Earnings Management. *Journal of Financial Economics*, 88(2):245–271, 2008.

[440] Paul Lavrakas. *Encyclopedia of Survey Research Methods*. SAGE Publications, Thousand Oaks, CA, 2008.

[441] Patrick Hable and Patrick Launhardt. Aggregate Insider Trading and the Prediction of Corporate Credit Spread Changes. *Financial Markets and Portfolio Management*, 34(1):1–31, 2020.

[442] Abagail McWilliams and Donald Siegel. Event Studies in Management Research: Theoretical and Empirical Issues. *Academy of Management Journal*, 40(3):626–657, 1997.

[443] Abagail McWilliams, Donald Siegel, and Siew Hong Teoh. Issues in the Use of the Event Study Methodology: A Critical Analysis of Corporate Social Responsibility Studies. *Organizational Research Methods*, 2(4):340–365, 1999.

[444] John Hughes, Jing Liu, and Jun Liu. Information Asymmetry, Diversification, and Cost of Capital. *The Accounting Review*, 82(3):705–729, 2006.

[445] Frank Wilcoxon. Individual Comparisons by Ranking Methods. *Biometrics Bulletin*, 1(6):80–83, 1945.

[446] Joseph L Hodges and Erich L Lehmann. Estimates of Location Based on Rank Tests. *Annals of Mathematical Statistics*, 34(2):598–611, 1963.

[447] Hyun-Chul Cho and Shuzo Abe. Is Two-Tailed Testing for Directional Research Hypotheses Tests Legitimate? *Journal of Business Research*, 66(9):1261–1266, 2013.

[448] David J Denis and Gregory B Kadlec. Corporate Events, Trading Activity, and the Estimation of Systematic Risk: Evidence from Equity Offerings and Share Repurchases. *Journal of Finance*, 49(5):1787–1811, 1994.

[449] Ross Stephen. The Arbitrage Theory of Capital Asset Pricing. *Journal of Economic Theory*, 13(3):341–360, 1976.

[450] Sergio Mayordomo, Juan I Peña, and Eduardo S Schwartz. Are All Credit Default Swap Databases Equal? *European Financial Management*, 20(4):677–713, 2014.

[451] Fabio Bertoni and Stefano Lugo. Detecting Abnormal Changes in Credit Default Swap Spreads Using Matching-Portfolio Models. *Journal of Banking & Finance*, 90:146–158, 2018.

[452] Lei Meng and Owain ap Gwilym. The Determinants of CDS Bid-Ask Spreads. *The Journal of Derivatives*, 16(1):70–80, 2008.

[453] Benjamin Y Zhang, Hao Zhou, and Haibin Zhu. Explaining Credit Default Swap Spreads with the Equity Volatility and Jump Risks of Individual Firms. *The Review of Financial Studies*, 22(12):5099–5131, 2009.

[454] Shanxiang Yang, Zhechen Liu, and Xinjie Wang. News Sentiment, Credit Spreads, and Information Asymmetry. *The North American Journal of Economics and Finance*, 52:1–19, 2020.

[455] Nicole T Jenkins, Michael D Kimbrough, and Juan Wang. The Extent of Informational Efficiency in the Credit Default Swap Market: Evidence from Post-Earnings Announcement Returns. *Review of Quantitative Finance and Accounting*, 46(4):725–761, 2016.

[456] S P Kothari and Jerold B Warner. Measuring Long-Horizon Security Price Performance. *Journal of Financial Economics*, 43(3):301–339, 1997.

[457] Ramesh Chandra, Shane Moriarity, and G Lee Willinger. A Reexamination of the Power of Alternative Return-Generating Models and the Effect of Accounting for Cross-Sectional Dependencies in Event Studies. *Journal of Accounting Research*, 28(2):398–408, 1990.

[458] Lawrence J White. Markets: The Credit Rating Agencies. *Journal of Economic Perspectives*, 24(2):211–226, 2010.

[459] Patrick Bolton, Xavier Freixas, and Joel Shapiro. The Credit Ratings Game. *Journal of Finance*, 67(1):85–111, 2012.

[460] Philippe Jorion and Gaiyan Zhang. Credit Contagion from Counterparty Risk. *Journal of Finance*, 64(5):2053–2087, 2009.

[461] Stephen Lok and Scott Richardson. Credit Markets and Financial Information. *Review of Accounting Studies*, 16(3):487–500, 2011.

[462] Koresh Galil, Offer Moshe Shapir, Dan Amiram, and Uri Ben-Zion. The Determinants of CDS Spreads. *Journal of Banking & Finance*, 41:271–282, 2014.

[463] Giovanni Calice, Christos Ioannidis, and RongHui Miao. A Markov Switching Unobserved Component Analysis of the CDX Index Term Premium. *International Review of Financial Analysis*, 44:189–204, 2016.

[464] Jeffrey M Woolridge. *Econometric Analysis of Cross Section and Panel Data*. MIT Press, Cambridge, MA, 2010.

[465] A Colin Cameron, Jonah B Gelbach, and Douglas L Miller. Robust Inference with Multiway Clustering. *Journal of Business & Economic Statistics*, 29(2):238–249, 2012.

[466] Halbert White. A Heteroskedasticity-Consistent Covariance Matrix Estimator and a Direct Test for Heteroskedasticity. *Econometrica*, 48(4):817–838, 1980.

[467] Mitchell A Petersen. Estimating Standard Errors in Finance Panel Data Sets: Comparing Approaches. *The Review of Financial Studies*, 22(1):435–480, 2009.

[468] James Durbin and Geoffrey S Watson. Testing for Serial Correlation in Least Squares Regression I. *Biometrika*, 37(3/4):409–428, 1950.

[469] James Durbin and Geoffrey S Watson. Testing for Serial Correlation in Least Squares Regression II. *Biometrika*, 38(1/2):159–177, 1951.

[470] Francois Brochet. Information Content of Insider Trades Before and After the Sarbanes-Oxley Act. *The Accounting Review*, 85(2):419–446, 2010.

[471] Harjeet S Bhabra and Ashrafee T Hossain. Market Conditions, Governance and the Information Content of Insider Trades. *Review of Financial Economics*, 24:1–11, 2015.

[472] Christopher B Barry and Stephen J Brown. Differential Information and the Small Firm Effect. *Journal of Financial Economics*, 13(2):283–294, 1984.

[473] Michael S Rozeff and Mir A Zaman. Overreaction and Insider Trading: Evidence from Growth and Value Portfolios. *Journal of Finance*, 53(2):701–716, 1998.

[474] Martha L Carter, Sattar A Mansi, and David M Reeb. Quasi-Private Information and Insider Trading. *Financial Analysts Journal*, 59(3):60–68, 2003.

[475] David Hillier, Adriana Korczak, and Piotr Korczak. The Impact of Personal Attributes on Corporate Insider Trading. *Journal of Corporate Finance*, 30:150–167, 2015.

[476] Jennifer N Carpenter and Barbara Remmers. Executive Stock Option Exercises and Inside Information. *The Journal of Business*, 74(4):513–534, 2001.

[477] David Yermack. Good Timing: CEO Stock Option Awards and Company News Announcements. *Journal of Finance*, 52(2):449–476, 1997.

[478] Cabinet Office. Press Release: Government Mandates New Cyber Security Standard for Suppliers. *Available at: https://www.gov.uk/government/news/government-mandates-new-cyber-security-standard-for-suppliers (last accessed 01/05/2021)*, 2014.

[479] Financial Times. G4S Profits Dented By Staff Compensation Charges. *Available at: https://www.ft.com/content/daea0a2e-4496-11e9-b168-96a37d002cd3 (last accessed 01/05/2021)*, 2019.

[480] Aswath Damodaran. 2018 Cost of Capital by Sector (US). *Available at: https://web.archive.org/web/20181020131527/people.stern.nyu.edu/adamodar/New_Home_Page/datafile/wacc.htm (last accessed 01/05/2021)*, 2018.

[481] Aswath Damodaran. Equity Risk Premiums (ERP): Determinants, Estimation and Implications - The 2019 Edition. *Working Paper available at SSRN: https://ssrn.com/abstract=3378246*, pages 1–135, 2019.

[482] Sayan Chatterjee and Michael Lubatkin. Corporate Mergers, Stockholder Diversification, and Changes in Systematic Risk. *Strategic Management Journal*, 11(4):255–268, 1990.

[483] Carolyn Y Woo and Karel O Cool. The Impact of Strategic Management on Systematic Risk. *Advances in Strategic Management*, 6:51–69, 1990.

[484] Chris Florackis, Christodoulos Louca, Roni Michaely, and Michael Weber. Cybersecurity Risk. *National Bureau of Economic Research Working Paper Series*, No. 28196:1–72, 2020.

[485] Robert S Hamada. The Effect of the Firm's Capital Structure on the Systematic Risk of Common Stocks. *Journal of Finance*, 27(2):435–452, 1972.

[486] Kwabena A Boasiako and Michael O'Connor Keefe. Data Breaches and Corporate Liquidity Management. *European Financial Management*, In Press, 2020.

[487] Joseph D Piotroski and Darren T Roulstone. The Influence of Analysts, Institutional Investors, and Insiders on the Incorporation of Market, Industry, and Firm-Specific Information into Stock Prices. *The Accounting Review*, 79(4):1119–1151, 2004.

[488] James Jiambalvo, Shivaram Rajgopal, and Mohan Venkatachalam. Institutional Ownership and the Extent to which Stock Prices Reflect Future Earnings. *Contemporary Accounting Research*, 19(1):117–145, 2002.

[489] Randolph B Cohen, Paul A Gompers, and Tuomo Vuolteenaho. Who Underreacts to Cash-Flow News? Evidence from Trading Between Individuals and Institutions. *Journal of Financial Economics*, 66(2-3):409–462, 2002.

[490] Miguel A Ferreira and Pedro Matos. The Colors of Investors' Money: The Role of Institutional Investors around the World. *Journal of Financial Economics*, 88(3):499–533, 2008.

[491] Mark Grinblatt and Matti Keloharju. The Investment Behavior and Performance of Various Investor Types: A Study of Finland's Unique Data Set. *Journal of Financial Economics*, 55(1):43–67, 2000.

[492] Brad M Barber and Terrance Odean. All that Glitters: The Effect of Attention and News on the Buying Behavior of Individual and Institutional Investors. *The Review of Financial Studies*, 21(2):785–818, 2008.

[493] Michael Liebmann, Alexei G Orlov, and Dirk Neumann. The Tone of Financial News and the Perceptions of Stock and CDS Traders. *International Review of Financial Analysis*, 46:159–175, 2016.

[494] Arnoud W A Boot and Anjan V Thakor. Can Relationship Banking Survive Competition? *Journal of Finance*, 55(2):679–713, 2000.

[495] Linda Allen and Stavros Peristiani. Loan Underpricing and the Provision of Merger Advisory Services. *Journal of Banking & Finance*, 31(12):3539–3562, 2007.

[496] Stuart I Greenbaum, George Kanatas, and Itzhak Venezia. Equilibrium Loan Pricing Under the Bank-Client Relationship. *Journal of Banking & Finance*, 13(2):221–235, 1989.

[497] Leonardo Gambacorta. How Do Banks Set Interest Rates? *European Economic Review*, 52(5):792–819, 2008.

[498] Redouane Elkamhi, Kris Jacobs, Hugues Langlois, and Chayawat Ornthanalai. Accounting Information Releases and CDS Spreads. *Midwest Finance Association 2012 Annual Meetings Paper*, pages 1–48, 2012.

[499] Jongsub Lee, Andy Naranjo, and Guner Velioglu. When do CDS Spreads Lead? Rating Events, Private Entities, and Firm-Specific Information Flows. *Journal of Financial Economics*, 130(3):556–578, 2018.

[500] Paresh Kumar Narayan and Deepa Bannigidadmath. Financial News and CDS Spreads. *Journal of Behavioral and Experimental Finance*, 29:1–14, 2021.

[501] Florian Kiesel, Sascha Kolaric, and Dirk Schiereck. Market Integration and Efficiency of CDS and Equity Markets. *The Quarterly Review of Economics and Finance*, 61:209–229, 2016.

[502] Jens Hilscher, Joshua M Pollet, and Mungo Wilson. Are Credit Default Swaps a Sideshow? Evidence that Information Flows from Equity to CDS Markets. *Journal of Financial and Quantitative Analysis*, 50(3):543–567, 2015.

[503] Konstantinos Tolikas and Nikolas Topaloglou. Is Default Risk Priced Equally Fast in the Credit Default Swap and the Stock Markets? An Empirical Investigation. *Journal of International Financial Markets, Institutions and Money*, 51:39–57, 2017.

[504] Maryam Akbari Nasiri, Paresh Kumar Narayan, and Sagarika Mishra. Reaction of the Credit Default Swap Market to the Release of Periodic Financial Reports. *International Review of Financial Analysis*, 65:1–12, 2019.

[505] Thomas Y To, Sirimon Treepongkaruna, and Eliza Wu. Are all Insiders on the Inside? Evidence from the Initiation of CDS Trading and Short Selling in the Financial Sector. *Journal of International Financial Markets, Institutions and Money*, 54:114–129, 2018.

[506] Jacob Cohen. *Statistical Power Analysis for the Behavioral Sciences*. Academic Press, New York City, NY, 2nd edition, 1988.

[507] Jacob Cohen. Statistical Power Analysis. *Current Directions in Psychological Science*, 1(3):98–101, 1992.

[508] Xinjie Wang, Weike Xu, and Zhaodong Zhong. Economic Policy Uncertainty, CDS Spreads, and CDS Liquidity Provision. *Journal of Futures Markets*, 39(4):461–480, 2019.

[509] Jennie Bai and Liuren Wu. Anchoring Credit Default Swap Spreads to Firm Fundamentals. *Journal of Financial and Quantitative Analysis*, 51(5):1521–1543, 2016.

[510] Mark Lang. Time-Varying Stock Price Response to Earnings Induced by Uncertainty About the Time-Series Process of Earnings. *Journal of Accounting Research*, 29(2):229–257, 1991.

[511] R Richardson Pettit and P C Venkatesh. Insider Trading and Long-Run Return Performance. *Financial Management*, 24(2):88–103, 1995.

[512] Lawrence A Gordon, Martin P Loeb, and Tashfeen Sohail. Market Value of Voluntary Disclosures Concerning Information Security. *MIS Quarterly*, 34(3):567–594, 2010.

[513] Henk Berkman, Jonathan Jona, Gladys Lee, and Naomi Soderstrom. Cybersecurity Awareness and Market Valuations. *Journal of Accounting and Public Policy*, 37(6):508–526, 2018.

[514] Paul M Healy and Krishna G Palepu. Information Asymmetry, Corporate Disclosure, and the Capital Markets: A Review of the Empirical Disclosure Literature. *Journal of Accounting and Economics*, 31(1-3):405–440, 2001.

[515] Karthik Balakrishnan, Mary Brooke Billings, Bryan Kelly, and Alexander Ljungqvist. Shaping Liquidity: On the Causal Effects of Voluntary Disclosure. *Journal of Finance*, 69(5):2237–2278, 2014.

[516] Ning Jia. Corporate Innovation Strategy, Analyst Forecasting Activities and the Economic Consequences. *Journal of Business Finance & Accounting*, 44(5-6):812–853, 2017.

[517] K Stephen Haggard, Xiumin Martin, and Raynolde Pereira. Does Voluntary Disclosure Improve Stock Price Informativeness? *Financial Management*, 37(4):747–768, 2008.

[518] Amir Sufi. Information Asymmetry and Financing Arrangements: Evidence from Syndicated Loans. *Journal of Finance*, 62(2):629–668, 2007.

[519] Regina Wittenberg-Moerman. The Role of Information Asymmetry and Financial Reporting Quality in Debt Trading: Evidence from the Secondary Loan Market. *Journal of Accounting and Economics*, 46(2-3):240–260, 2008.

[520] Boyd D Cohen and Thomas J Dean. Information Asymmetry and Investor Valuation of IPOs: Top Management Team Legitimacy as a Capital Market Signal. *Strategic Management Journal*, 26(7):683–690, 2005.

[521] Kalok Chan, Albert J Menkveld, and Zhishu Yang. Information Asymmetry and Asset Prices: Evidence from the China Foreign Share Discount. *Journal of Finance*, 63(1):159–196, 2008.

[522] Pierangelo Rosati and Theo Lynn. A Dataset for Accounting, Finance and Economics Research on US Data Breaches. *Data in Brief*, 35:1–6, 2021.

[523] Sharon M Ravitch and Matthew Riggan. *Reason & Rigor: How Conceptual Frameworks Guide Research*. SAGE Publications, Thousand Oaks, CA, 2016.

[524] Nik Rushdi Hassan, Lars Mathiassen, and Paul Benjamin Lowry. The Process of Information Systems Theorizing as a Discursive Practice. *Journal of Information Technology*, 34(3):198–220, 2019.

[525] Mohammad Irshad. A Systematic Review of Information Security Frameworks in the Internet of Things (IoT). *IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems*, pages 1270–1275, 2016.

[526] A Da Veiga and J H P Eloff. An Information Security Governance Framework. *Information Systems Management*, 24(4):361–372, 2007.

[527] Yosef Jabareen. Building a Conceptual Framework: Philosophy, Definitions, and Procedure. *International Journal of Qualitative Methods*, 8(4):49–62, 2009.

[528] John W Creswell and Cheryl N Poth. *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. SAGE Publications, London, UK, 2016.

[529] Mojtaba Khaghani Milani and Mahmoud Reza Hashemi. Extended Grounded Theory: A Methodology to Combine Multiple Disciplines. *Information Systems and e-Business Management*, 18:89–120, 2020.

[530] Sitwala Imenda. Is There a Conceptual Difference between Theoretical and Conceptual Frameworks? *Journal of Social Sciences*, 38(2):185–195, 2014.

[531] Theodosios Tsiakis and George Stephanides. The Economic Approach of Information Security. *Computers & Security*, 24(2):105–108, 2005.

[532] Daniel Schatz and Rabih Bashroush. Economic Valuation for Information Security Investment: A Systematic Literature Review. *Information Systems Frontiers*, 19(5):1205–1228, 2017.

[533] Constance E Helfat and Sidney G Winter. Untangling Dynamic and Operational Capabilities: Strategy for the (N)ever-Changing World. *Strategic Management Journal*, 32(11):1243–1250, 2011.

[534] Robert G Bowman. The Theoretical Relationship Between Systematic Risk and Financial (Accounting) Variables. *Journal of Finance*, 34(3):617–630, 1979.

[535] James M Gahlon. Operating Leverage as a Determinant of Systematic Risk. *Journal of Business Research*, 9(3):297–308, 1981.

[536] James M Gahlon and James A Gentry. On the Relationship Between Systematic Risk and the Degrees of Operating and Financial Leverage. *Financial Management*, 11(2):15–23, 1982.

[537] Armin Sarabi, Parinaz Naghizadeh, Yang Liu, and Mingyan Liu. Risky Business: Fine-Grained Data Breach Prediction Using Business Profiles. *Journal of Cybersecurity*, 2(1):15–28, 2016.

[538] Sanjai Bhagat and Brian Bolton. Corporate Governance and Firm Performance. *Journal of Corporate Finance*, 14(3):257–273, 2008.

[539] David F Larcker, Scott A Richardson, and Irem Tuna. Corporate Governance, Accounting Outcomes, and Organizational Performance. *The Accounting Review*, 82(4):963–1008, 2007.

[540] Richard Whittington, Basak Yakis-Douglas, and Kwangwon Ahn. Cheap Talk? Strategy Presentations as a Form of Chief Executive Officer Impression Management. *Strategic Management Journal*, 37(12):2413–2424, 2016.

Appendix A
Cyber Essentials (Plus) Certifications Sample

Table A.1: Cyber Essentials (Plus) Sample (1/2)

Event ID	Certifiee Name	Listed Company Name	Certificate Type
1	AA Drive-Tech	AA plc	CE
2	Aberforth Partners LLP	Aberforth Smaller Companies Trust Plc	CE
3	Aberforth Partners LLP	Aberforth Smaller Companies Trust Plc	Plus
4	Aberforth Partners LLP	Aberforth Smaller Companies Trust Plc	Plus
5	Aberforth Partners LLP	Aberforth Smaller Companies Trust Plc	Plus
6	Anglo American PLC	Anglo American plc	CE
7	Babcock International Group Plc	Babcock International Group plc	Plus
8	Babcock International Group plc.	Babcock International Group plc	Plus
9	Babcock Information Analytics and Security	Babcock International Group plc	CE
10	Babcock Information Analytics and Security	Babcock International Group plc	CE
11	BAE Systems Maritime - Submarines	BAE Systems plc	Plus
12	BAE Systems Maritime - Submarines	BAE Systems plc	CE
13	BAE Systems plc	BAE Systems plc	CE
14	BAE Systems Regional Aircraft	BAE Systems plc	CE
15	BAE Systems Saudi Arabia Limited	BAE Systems plc	CE
16	BAE Systems Saudi Arabia Limited	BAE Systems plc	Plus
17	BAE Systems, Inc. (BAE Systems USA)	BAE Systems plc	CE
18	Balfour Beatty plc	Balfour Beatty plc	CE
19	Barclays Bank plc	Barclays PLC	CE
20	Barclays Bank plc	Barclays PLC	CE
21	Brewin Dolphin Ltd	Brewin Dolphin Holdings PLC	Plus
22	BT Group plc	BT Group plc	CE
23	CAPITA	Capita plc	CE

Table A.1 continued from previous page

Event ID	Certifiee Name	Listed Company Name	Certificate Type
24	CAPITA	Capita plc	Plus
25	Trustmarque Solutions	Capita plc	CE
26	Capita Travel and Events	Capita plc	CE
27	Capita Translation and Interpreting	Capita plc	CE
28	Capita - Local Government Health and Property	Capita plc	CE
29	Capita Travel and Events	Capita plc	Plus
30	Capita Business Services Ltd	Capita plc	CE
31	Capita Transformation	Capita plc	CE
32	Capita - Real Estate and Infrastructure	Capita plc	Plus
33	Capita Property & Infrastructure Ltd	Capita plc	Plus
34	Trustmarque Solutions (part of Capita plc)	Capita plc	CE
35	Capita Customer Management	Capita plc	Plus
36	Capita Customer Management	Capita plc	Plus
37	Capita Business Services Ltd	Capita plc	CE
38	Capita Business Services	Capita plc	CE
39	Capita Business Services Ltd	Capita plc	CE
40	Capita Travel and Events	Capita plc	Plus
41	Capita Business Services Ltd (CBSL)	Capita plc	CE
42	Capita Travel and Events	Capita plc	Plus
43	Capita Business Services Ltd	Capita plc	CE
44	Capita Managing Agency Limited	Capita plc	CE
45	Fire Service College Ltd (Capita Group)	Capita plc	CE
46	Trustmarque Solutions Ltd	Capita plc	CE

Table A.1 continued from previous page

Event ID	Certifiee Name	Listed Company Name	Certificate Type
47	Capita Transformation.	Capita plc	CE
48	Capita ITPS	Capita plc	Plus
49	Capita Real Estate and Infrastructure	Capita plc	Plus
50	H. Clarkson & Co. Ltd	Clarkson PLC	CE
51	Cobham	Cobham plc	Plus
52	Computacenter (UK) Limited	Computacenter plc	CE
53	Computacenter PLC	Computacenter plc	CE
54	Cranswick Plc	Cranswick plc	CE
55	Cranswick Plc	Cranswick plc	Plus
56	DCC Energy Ltd	DCC plc	Plus
57	Experian Ltd	Experian plc	CE
58	Experian Ltd	Experian plc	CE
59	FDM Group (CES/00379)	FDM Group (Holdings) PLC	CE
60	G4S Fire & Security Systems UK	G4S plc	CE
61	G4S Regional Management Ltd	G4S plc	CE
62	Galliford Try Plc	Galliford Try plc	CE
63	GlaxoSmithKline	GlaxoSmithKline plc	CE
64	Grainger Plc	Grainger plc	CE
65	Greencoat Capital LLP	Greencoat UK Wind PLC	CE
66	Hargreaves Lansdown	Hargreaves Lansdown plc	CE
67	Hays Specialist Recruitment	Hays plc	CE
68	Hays PLC Subsidiaries	Hays plc	CE
69	Hiscox	Hiscox Ltd	Plus

Table A.1 continued from previous page

Event ID	Certifiee Name	Listed Company Name	Certificate Type
70	Howdens Joinery Plc	Howden Joinery Group Plc	CE
71	HSBC Holdings PLC	HSBC Holdings plc	Plus
72	Inchcape Fleet Solutions Ltd	Inchcape plc	CE
73	Inchcape Fleet Solutions Ltd	Inchcape plc	CE
74	Inchcape Fleet Solutions Ltd	Inchcape plc	CE
75	James Fisher Mimic	James Fisher and Sons plc	CE
76	James Fisher Nuclear Holdings Ltd	James Fisher and Sons plc	CE
77	Jupiter Asset Management Limited	Jupiter Fund Management Plc	Plus
78	Jupiter Asset Management Limited	Jupiter Fund Management Plc	Plus
79	Jupiter Asset Management Ltd	Jupiter Fund Management Plc	CE
80	KIER Group Ltd	Kier Group plc	CE
81	Kier Ltd	Kier Group plc	CE
82	Lloyds Banking Group	Lloyds Banking Group plc	CE
83	Lloyds Banking Group	Lloyds Banking Group plc	CE
84	Lloyds Banking Group	Lloyds Banking Group plc	CE
85	Meggitt PLC	Meggitt PLC	Plus
86	Meggitt PLC	Meggitt PLC	CE
87	MEGGITT TRAINING SYSTEMS LIMITED	Meggitt PLC	CE
88	Entcorp UK Ltd	Micro Focus International plc	CE
89	Morgan Advanced Materials	Morgan Advanced Materials plc	Plus
90	Morgan Advanced Materials	Morgan Advanced Materials plc	Plus
91	Morgan Advanced Materials	Morgan Advanced Materials plc	Plus
92	QinetiQ Ltd	QinetiQ Group plc	CE

Table A.1 continued from previous page

Event ID	Certifiee Name	Listed Company Name	Certificate Type
93	Redrow PLC	Redrow plc	Plus
94	Redrow PLC	Redrow plc	Plus
95	RELX (UK) Limited t/a LexisNexis	RELX PLC	CE
96	ROLLS-ROYCE POWER ENGINEERING plc	Rolls-Royce Holdings plc	Plus
97	Rolls-Royce Power Systems AG	Rolls-Royce Holdings plc	Plus
98	Royal Mail Group Ltd	Royal Mail plc	CE
99	Savills PLC	Savills plc	Plus
100	Savills PLC	Savills plc	Plus
101	Savills PLC	Savills plc	Plus
102	Serco Ltd	Serco Group plc	Plus
103	Serco Ltd	Serco Group plc	CE
104	Serco Regional Services Ltd	Serco Group plc	CE
105	Serco Ltd	Serco Group plc	Plus
106	Serco Ltd	Serco Group plc	Plus
107	Severn Trent Services Operations UK Limited	Severn Trent Plc	CE
108	Severn Trent Services Operations UK Limited	Severn Trent Plc	CE
109	Severn Trent Services UK Operations Ltd	Severn Trent Plc	CE
110	Shaftesbury Plc	Shaftesbury PLC	CE
111	Shaftesbury Plc	Shaftesbury PLC	CE
112	Shaftesbury PLC	Shaftesbury PLC	CE
113	Sky Betting and Gaming	Sky plc	Plus
114	Softcat plc	Softcat plc	CE
115	Sophos	Sophos Group plc	CE

Table A.1 continued from previous page

Event ID	Certifiee Name	Listed Company Name	Certificate Type
116	Sophos	Sophos Group plc	CE
117	Sophos	Sophos Group plc	CE
118	SSE Telecommunications Ltd	SSE plc	Plus
119	St James's Place Wealth Management	St. James's Place plc	Plus
120	St. Modwen Properties PLC	St. Modwen Properties PLC	CE
121	Aberdeen Asset Management Plc	Standard Life Aberdeen plc	CE
122	The Berkeley Group Holdings plc	The Berkeley Group Holdings plc	CE
123	The Berkeley Group Holdings plc	The Berkeley Group Holdings plc	Plus
124	Go Ahead London	The Go-Ahead Group plc	Plus
125	Go Ahead London	The Go-Ahead Group plc	Plus
126	Go-Ahead Group	The Go-Ahead Group plc	Plus
127	Go-Ahead Group plc	The Go-Ahead Group plc	Plus
128	Royal Bank of Scotland plc	The Royal Bank of Scotland Group plc	Plus
129	Sage Qualifications Ltd.	The Sage Group plc	CE
130	Weir Engineering Services Ltd	The Weir Group PLC	CE
131	Weir Valves and Controls UK Ltd	The Weir Group PLC	CE
132	Travis Perkins Plc	Travis Perkins plc	CE
133	Ultra Electronics AEP	Ultra Electronics Holdings plc	CE
134	Ultra Electronics CIS Sonar	Ultra Electronics Holdings plc	Plus
135	Ultra Electronics Command & Sonar Systems	Ultra Electronics Holdings plc	Plus
136	Ultra Electronics Command & Sonar Systems	Ultra Electronics Holdings plc	CE
137	Ultra Electronics Ocean Systems Inc	Ultra Electronics Holdings plc	CE
138	Ultra Electronics PMES	Ultra Electronics Holdings plc	CE

Table A.1 continued from previous page

Event ID	Certifiee Name	Listed Company Name	Certificate Type
139	Virgin Money Giving	Virgin Money Holdings (UK) plc	Plus
140	Vodafone	Vodafone Group Plc	Plus
141	Vodafone Limited	Vodafone Group Plc	Plus
142	Vodafone Limited (recertified)	Vodafone Group Plc	Plus
143	Whitbread PLC	Whitbread PLC	Plus
144	Whitbread PLC	Whitbread PLC	CE
145	Witan Investment Trust PLC	Witan Investment Trust plc	CE

Table A.2: Cyber Essentials (Plus) Sample (2/2)

Event ID	Primary Industry	Date	Certifiee Org Status	Source
1	Specialized Consumer Services	09/06/2017	Subsidiary	Auditor
2	Asset Management & Custody Banks	04/12/2017	Subsidiary	Both
3	Asset Management & Custody Banks	13/12/2017	Subsidiary	Both
4	Asset Management & Custody Banks	16/12/2016	Subsidiary	Both
5	Asset Management & Custody Banks	13/12/2017	Subsidiary	Both
6	Diversified Metals & Mining	20/11/2017	Parent/Holding Co	Auditor
7	Diversified Support Services	31/10/2017	Parent/Holding Co	Both
8	Diversified Support Services	05/04/2016	Parent/Holding Co	Auditor
9	Diversified Support Services	12/06/2017	Subsidiary	Auditor
10	Diversified Support Services	24/05/2016	Subsidiary	Auditor
11	Aerospace & Defense	01/11/2017	Subsidiary	NCSC
12	Aerospace & Defense	01/10/2017	Subsidiary	NCSC
13	Aerospace & Defense	25/05/2018	Parent/Holding Co	NCSC
14	Aerospace & Defense	18/06/2018	Subsidiary	NCSC
15	Aerospace & Defense	01/08/2017	Subsidiary	NCSC
16	Aerospace & Defense	01/08/2017	Subsidiary	NCSC
17	Aerospace & Defense	26/06/2018	Subsidiary	NCSC
18	Construction & Engineering	10/04/2018	Parent/Holding Co	NCSC
19	Diversified Banks	24/06/2014	Parent/Holding Co	Auditor
20	Diversified Banks	27/05/2016	Parent/Holding Co	Auditor
21	Asset Management & Custody Banks	22/03/2018	Parent/Holding Co	Both
22	Integrated Telco Services	27/04/2018	Parent/Holding Co	NCSC
23	HR & Employment Services	14/03/2018	Parent/Holding Co	NCSC

Table A.2 continued from previous page

Event ID	Primary Industry	Date	Certifiee Org Status	Source
24	HR & Employment Services	14/03/2018	Parent/Holding Co	NCSC
25	HR & Employment Services	10/04/2015	Subsidiary	Auditor
26	HR & Employment Services	30/06/2015	Subsidiary	Auditor
27	HR & Employment Services	22/03/2016	Subsidiary	Auditor
28	HR & Employment Services	18/04/2016	Subsidiary	Auditor
29	HR & Employment Services	08/11/2016	Subsidiary	Auditor
30	HR & Employment Services	18/11/2016	Subsidiary	Auditor
31	HR & Employment Services	02/02/2017	Subsidiary	Auditor
32	HR & Employment Services	22/03/2017	Subsidiary	Auditor
33	HR & Employment Services	22/03/2017	Subsidiary	Auditor
34	HR & Employment Services	15/06/2017	Subsidiary	Auditor
35	HR & Employment Services	08/09/2017	Subsidiary	Auditor
36	HR & Employment Services	30/09/2017	Subsidiary	NCSC
37	HR & Employment Services	01/10/2017	Subsidiary	NCSC
38	HR & Employment Services	01/11/2017	Subsidiary	NCSC
39	HR & Employment Services	30/11/2017	Subsidiary	NCSC
40	HR & Employment Services	30/11/2017	Subsidiary	NCSC
41	HR & Employment Services	06/12/2017	Subsidiary	NCSC
42	HR & Employment Services	04/01/2018	Subsidiary	NCSC
43	HR & Employment Services	24/01/2018	Subsidiary	NCSC
44	HR & Employment Services	07/02/2018	Subsidiary	NCSC
45	HR & Employment Services	19/03/2018	Subsidiary	NCSC
46	HR & Employment Services	26/04/2018	Subsidiary	Auditor

Table A.2 continued from previous page

Event ID	Primary Industry	Date	Certifiee Org Status	Source
47	HR & Employment Services	23/05/2018	Subsidiary	NCSC
48	HR & Employment Services	24/05/2018	Subsidiary	NCSC
49	HR & Employment Services	29/05/2018	Subsidiary	NCSC
50	Marine	01/09/2017	Subsidiary	NCSC
51	Aerospace & Defense	03/08/2016	Parent/Holding Co	Auditor
52	IT Consulting & Other Services	31/12/2017	Subsidiary	NCSC
53	IT Consulting & Other Services	09/01/2018	Parent/Holding Co	NCSC
54	Packaged Foods & Meats	13/04/2017	Parent/Holding Co	Auditor
55	Packaged Foods & Meats	28/03/2018	Parent/Holding Co	Both
56	Industrial Conglomerates	22/05/2017	Subsidiary	Auditor
57	Research & Consulting Services	11/01/2017	Subsidiary	Auditor
58	Research & Consulting Services	08/01/2018	Subsidiary	Both
59	IT Consulting & Other Services	01/09/2017	Parent/Holding Co	NCSC
60	Security & Alarm Services	27/02/2017	Subsidiary	Auditor
61	Security & Alarm Services	15/12/2015	Subsidiary	Auditor
62	Construction & Engineering	31/07/2017	Parent/Holding Co	Auditor
63	Pharmaceuticals	01/08/2016	Parent/Holding Co	Auditor
64	Real Estate Operating Companies	21/03/2018	Parent/Holding Co	NCSC
65	Renewable Electricity	01/11/2017	Parent/Holding Co	NCSC
66	Asset Management & Custody Banks	19/04/2018	Parent/Holding Co	NCSC
67	HR & Employment Services	10/07/2017	Parent/Holding Co	Auditor
68	HR & Employment Services	10/07/2016	Subsidiary	Auditor
69	Property & Casualty Insurance	29/05/2018	Parent/Holding Co	Both

Table A.2 continued from previous page

Event ID	Primary Industry	Date	Certifiee Org Status	Source
70	Trading Companies & Distributors	28/11/2017	Parent/Holding Co	Both
71	Diversified Banks	08/03/2016	Parent/Holding Co	Auditor
72	Distributors	06/08/2015	Subsidiary	Auditor
73	Distributors	05/08/2015	Subsidiary	Auditor
74	Distributors	09/08/2016	Subsidiary	Auditor
75	Marine Ports & Services	22/12/2017	Subsidiary	NCSC
76	Marine Ports & Services	28/02/2018	Subsidiary	NCSC
77	Asset Management & Custody Banks	31/10/2017	Parent/Holding Co	NCSC
78	Asset Management & Custody Banks	06/10/2016	Parent/Holding Co	Auditor
79	Asset Management & Custody Banks	24/04/2015	Parent/Holding Co	Auditor
80	Construction & Engineering	01/10/2017	Parent/Holding Co	NCSC
81	Construction & Engineering	27/06/2018	Parent/Holding Co	NCSC
82	Diversified Banks	19/12/2017	Parent/Holding Co	NCSC
83	Diversified Banks	16/02/2016	Parent/Holding Co	Auditor
84	Diversified Banks	16/03/2016	Parent/Holding Co	Auditor
85	Aerospace & Defense	21/02/2018	Parent/Holding Co	NCSC
86	Aerospace & Defense	03/12/2017	Parent/Holding Co	NCSC
87	Aerospace & Defense	21/11/2017	Subsidiary	NCSC
88	Application SW	26/03/2018	Subsidiary	NCSC
89	Industrial Machinery	10/09/2015	Parent/Holding Co	Auditor
90	Industrial Machinery	09/09/2016	Parent/Holding Co	Auditor
91	Industrial Machinery	01/09/2017	Parent/Holding Co	Both
92	Aerospace & Defense	14/05/2018	Parent/Holding Co	NCSC

Table A.2 continued from previous page

Event ID	Primary Industry	Date	Certifiee Org Status	Source
93	Homebuilding	26/05/2016	Parent/Holding Co	Auditor
94	Homebuilding	01/06/2017	Parent/Holding Co	Auditor
95	Research & Consulting Services	06/06/2018	Subsidiary	NCSC
96	Aerospace & Defense	31/07/2017	Subsidiary	Both
97	Aerospace & Defense	03/12/2017	Subsidiary	Both
98	Air Freight & Logistics	29/06/2018	Parent/Holding Co	NCSC
99	Real Estate Services	04/03/2016	Parent/Holding Co	Auditor
100	Real Estate Services	26/04/2017	Parent/Holding Co	Auditor
101	Real Estate Services	09/05/2018	Parent/Holding Co	Both
102	Environment & Facilities Services	29/01/2018	Subsidiary	NCSC
103	Environment & Facilities Services	22/01/2018	Subsidiary	NCSC
104	Environment & Facilities Services	30/08/2017	Subsidiary	NCSC
105	Environment & Facilities Services	16/12/2015	Subsidiary	Auditor
106	Environment & Facilities Services	30/01/2017	Subsidiary	Auditor
107	Water Utilities	13/01/2016	Subsidiary	Auditor
108	Water Utilities	27/03/2018	Subsidiary	Both
109	Water Utilities	23/02/2017	Subsidiary	Auditor
110	Retail REITs	07/04/2016	Parent/Holding Co	Auditor
111	Retail REITs	19/04/2017	Parent/Holding Co	Auditor
112	Retail REITs	18/08/2014	Parent/Holding Co	Auditor
113	Cable & Satellite	08/07/2016	Subsidiary	Auditor
114	IT Consulting & Other Services	29/06/2018	Parent/Holding Co	NCSC
115	Systems Software	31/03/2017	Parent/Holding Co	Auditor

Table A.2 continued from previous page

Event ID	Primary Industry	Date	Certifiee Org Status	Source
116	Systems Software	26/03/2018	Parent/Holding Co	Both
117	Systems Software	31/03/2017	Parent/Holding Co	Auditor
118	Electric Utilities	15/05/2018	Subsidiary	NCSC
119	Asset Management & Custody Banks	21/06/2018	Parent/Holding Co	Both
120	Real Estate Development	01/11/2017	Parent/Holding Co	NCSC
121	Other Diversified Financial Services	01/12/2017	Subsidiary	Auditor
122	Homebuilding	10/04/2015	Parent/Holding Co	Auditor
123	Homebuilding	10/04/2015	Parent/Holding Co	Auditor
124	Railroads	22/09/2016	Subsidiary	Auditor
125	Railroads	06/12/2017	Subsidiary	Auditor
126	Railroads	26/06/2015	Parent/Holding Co	Both
127	Railroads	01/07/2016	Parent/Holding Co	Auditor
128	Diversified Banks	06/02/2018	Parent/Holding Co	Both
129	Application SW	28/01/2018	Subsidiary	Both
130	Industrial Machinery	30/11/2017	Subsidiary	NCSC
131	Industrial Machinery	18/12/2017	Subsidiary	NCSC
132	Trading Companies & Distributors	11/04/2018	Parent/Holding Co	NCSC
133	Aerospace & Defense	27/03/2015	Subsidiary	Auditor
134	Aerospace & Defense	24/07/2015	Subsidiary	Auditor
135	Aerospace & Defense	29/03/2018	Subsidiary	NCSC
136	Aerospace & Defense	11/12/2017	Subsidiary	NCSC
137	Aerospace & Defense	22/05/2018	Subsidiary	NCSC
138	Aerospace & Defense	21/06/2018	Subsidiary	NCSC

Table A.2 continued from previous page

Event ID	Primary Industry	Date	Certifiee Org Status	Source
139	Diversified Banks	04/01/2018	Subsidiary	NCSC
140	Wireless Telecommunication Services	01/08/2016	Parent/Holding Co	Auditor
141	Wireless Telecommunication Services	14/07/2014	Parent/Holding Co	Auditor
142	Wireless Telecommunication Services	26/06/2015	Parent/Holding Co	Auditor
143	Restaurants	05/02/2018	Parent/Holding Co	NCSC
144	Restaurants	03/01/2018	Parent/Holding Co	NCSC
145	Asset Management & Custody Banks	26/03/2018	Parent/Holding Co	NCSC

Appendix B
ISO/IEC 27001 Certifications Sample

Table B.1: ISO/IEC 27001 Sample (1/2)

Event ID	Certifiee Name	Listed Company Name
1	AAI Limited	Suncorp Group Limited
2	Agility Applications Pty Ltd	HUB24 Limited
3	Covata Australia Pty Ltd	Covata Limited
4	Dynamiq Strategy Pty Ltd	Insurance Australia Group Limited
5	GBST Holdings Pty Ltd	GBST Holdings Limited
6	Grand United Corporate Health Limited	nib holdings limited
7	Hansen Corporation Pty Ltd	Hansen Technologies Ltd
8	Infomedia Ltd	Infomedia Ltd.
9	Link Administration Holdings Limited	Link Administration Holdings Limited
10	Macquarie Telecom Pty Ltd	Macquarie Telecom Group Limited
11	NEXTDC Limited	NEXTDC Limited
12	Nextgen Networks Pty Ltd	Vocus Group Limited
13	Sydney Airport Corporation Limited	Sydney Airport Limited
14	Tabcorp Holdings Limited	Tabcorp Holdings Limited
15	Telstra Corporation Ltd	Telstra Corporation Limited
16	TELSTRA INTERNATIONAL LIMITED	Telstra Corporation Limited
17	Vocus Group	Vocus Group Limited
18	TBI Info Ltd	Vienna Insurance Group AG
19	DONGFANG ELECTRONICS PRIVATE LIMITED	Dongfang Electronics Co., Ltd.
20	Ingram Micro Inc.	HNA Technology Co., Ltd.
21	Wridgways Pty Ltd	Santa Fe Group A/S
22	Razorfish (a Div. of TLG India Pvt. Ltd.)	Publicis Groupe S.A.
23	Allianz Australia Insurance Limited	Allianz SE

Table B.1 continued from previous page

Event ID	Certifiee Name	Listed Company Name
24	PCCW Global (Australia) Pty Limited	PCCW Limited
25	8KMiles Software Services Ltd	8K Miles Software Services Limited
26	Adroit Infosystems (P) Ltd.	Adroit Infotech Limited
27	Elitecore Technologies Pvt. Ltd.	Sterlite Technologies Limited
28	Incessant Technologies	NIIT Technologies Limited
29	JEEVANSATHI INTERNET SERVICES	Info Edge (India) Limited
30	POWERGRID CORPORATION OF INDIA LIMITED	Power Grid Corporation of India Limited
31	POWERGRID CORPORATION OF INDIA LIMITED	Power Grid Corporation of India Limited
32	The Hi-Tech Robotic Systemz Ltd.	The Hi-Tech Gears Limited
33	Trigyn Technologies Limited	Trigyn Technologies Limited
34	Betfair Pty Limited	Paddy Power Betfair plc
35	Elbit Systems of Australia Pty Ltd	Elbit Systems Ltd.
36	Chiyoda Singapore (Pte.) Limited	Chiyoda Corporation
37	Converga Pty Ltd	Canon Inc.
38	Fuji Xerox Asia Pacific Pte Ltd	FUJIFILM Holdings Corporation
39	Fuji Xerox Australia Pty Limited	FUJIFILM Holdings Corporation
40	Fujitsu Australia Limited	Fujitsu Limited
41	INFORMATION SERVICES INTERNATIONAL-DENTSU, LTD	Information Services International-Dentsu, Ltd.
42	Kowamex Co., Ltd.	Mamezou Holdings Co.,Ltd.
43	KYOCERA Document Solutions Australia Pty Ltd	Kyocera Corporation
44	NEC Australia Pty Ltd (ABN 86 001 217 527)	NEC Corporation
45	Neutral Co., Ltd	Mamezou Holdings Co.,Ltd.
46	NTT DATA Figtree Systems Pty Ltd	Nippon Telegraph and Telephone Corporation

Table B.1 continued from previous page

Event ID	Certifiee Name	Listed Company Name
47	Panasonic Appliances Vietnam Co., Ltd.	Panasonic Corporation
48	PANASONIC SYSTEM NETWORKS VIETNAM CO., LTD	Panasonic Corporation
49	WACOM-IT Co., Ltd.	Wacom Co., Ltd.
50	Bank Audi SAL - CISBC Department	Bank Audi S.A.L.
51	Fugro Australia Land Pty Ltd	Fugro N.V.
52	Freightways Information Services	Freightways Limited
53	Shred-X Pty Ltd	Freightways Limited
54	The Information Management Group Pty Ltd	Freightways Limited
55	FBNQuest Merchant Bank Limited	FBN Holdings Plc
56	National Bank of Oman	National Bank of Oman SAOG
57	ASSECO SEE EOOD	Asseco South Eastern Europe S.A.
58	Wataniya Telecom Algerie S.P.A - Ooredoo	Ooredoo Q.P.S.C.
59	Optus Networks Pty Limited	Singapore Telecommunications Limited
60	MTN Nigeria Communications Limited	MTN Group Limited
61	Recoveries Corporation Pty Ltd	Transaction Capital Limited
62	SGS India Private Limited	SGS SA
63	VMLabs Ltd	STMicroelectronics N.V.
64	Aldar Properties PJSC	Aldar Properties PJSC
65	PT. Technip Indonesia	TechnipFMC plc
66	Vix Verify Pty Ltd	GB Group plc
67	3M Company	3M Company
68	CA Technologies	Broadcom Inc.
69	Cubic Transportation Systems (Australia) Pty Limited	Cubic Corporation

Table B.1 continued from previous page

Event ID	Certifiee Name	Listed Company Name
70	MONG DUONG THERMAL POWER COMPANY	The AES Corporation
71	Motorola Solutions Australia Pty Limited	Motorola Solutions, Inc.
72	NetApp Australia Pty Ltd	NetApp, Inc.
73	OPTUM TECHNOLOGY CENTER	UnitedHealth Group Incorporated
74	Perceptive Group Ltd	Omnicom Group Inc.
75	ReachTEL Pty Ltd	Equifax Inc.
76	CMC SOFTWARE SOLUTION COMPANY LIMITED	CMC Corporation
77	PETROLEUM IT TELECOM	PetroVietnam Technical Services Corporation

Table B.2: ISO/IEC 27001 Sample (2/2)

Event ID	Certificate Type	Primary Industry	Date	Certifiee Org Status
1	ISO/IEC 27001	Property & Casualty Insurance	06/01/2016	Subsidiary
2	ISO/IEC 27001	Investment Banking & Brokerage	11/06/2018	Subsidiary
3	ISO/IEC 27001	Systems Software	26/05/2016	Subsidiary
4	ISO/IEC 27001	Property & Casualty Insurance	25/11/2015	Subsidiary
5	ISO/IEC 27001	Data Processing & Outsourced Services	30/08/2016	Subsidiary
6	ISO/IEC 27001	Life & Health Insurance	21/12/2016	Parent/Holding Co
7	ISO/IEC 27001	Application Software	22/10/2018	Subsidiary
8	ISO/IEC 27001	Application Software	08/08/2018	Parent/Holding Co
9	ISO/IEC 27001	Data Processing & Outsourced Services	04/07/2018	Parent/Holding Co
10	ISO/IEC 27001	Integrated Telecommunication Services	21/12/2017	Subsidiary
11	ISO/IEC 27001	Internet Services & Infrastructure	21/11/2018	Parent/Holding Co
12	ISO/IEC 27001	Integrated Telecommunication Services	11/10/2017	Subsidiary
13	ISO/IEC 27001	Airport Services	21/03/2018	Subsidiary
14	ISO/IEC 27001	Casinos & Gaming	27/07/2018	Parent/Holding Co
15	ISO/IEC 27001	Integrated Telecommunication Services	10/02/2017	Parent/Holding Co
16	ISO/IEC 27001	Integrated Telecommunication Services	26/10/2017	Subsidiary
17	ISO/IEC 27001	Integrated Telecommunication Services	23/01/2018	Parent/Holding Co
18	ISO/IEC 27001	Multi-line Insurance	23/03/2018	Subsidiary
19	ISO/IEC 27001	Electrical Components & Equipment	06/11/2018	Parent/Holding Co
20	ISO/IEC 27001	Technology Distributors	15/09/2017	Subsidiary
21	ISO/IEC 27001	Air Freight & Logistics	21/12/2017	Subsidiary
22	ISO/IEC 27001	Advertising	17/10/2016	Subsidiary
23	ISO/IEC 27001	Multi-line Insurance	07/05/2018	Subsidiary

Table B.2 continued from previous page

Event ID	Certificate Type	Primary Industry	Date	Certifiee Org Status
24	ISO/IEC 27001	Integrated Telecommunication Services	03/08/2018	Subsidiary
25	ISO/IEC 27001	Application Software	31/05/2018	Parent/Holding Co
26	ISO/IEC 27001	IT Consulting & Other Services	26/03/2018	Parent/Holding Co
27	ISO/IEC 27001	Communications Equipment	12/04/2016	Subsidiary
28	ISO/IEC 27001	IT Consulting & Other Services	01/10/2018	Subsidiary
29	ISO/IEC 27001	Interactive Media & Services	30/03/2017	Subsidiary
30	ISO/IEC 27001	Electric Utilities	01/11/2017	Parent/Holding Co
31	ISO/IEC 27001	Electric Utilities	23/08/2018	Parent/Holding Co
32	ISO/IEC 27001	Auto Parts & Equipment	26/12/2015	Subsidiary
33	ISO/IEC 27001	IT Consulting & Other Services	31/07/2018	Parent/Holding Co
34	ISO/IEC 27001	Casinos & Gaming	28/09/2018	Subsidiary
35	ISO/IEC 27001	Aerospace & Defense	07/09/2018	Subsidiary
36	ISO/IEC 27001	Construction & Engineering	28/03/2018	Subsidiary
37	ISO/IEC 27001	Technology Hardware Storage & Peripherals	01/03/2016	Subsidiary
38	ISO/IEC 27001	Technology Hardware Storage & Peripherals	12/12/2017	Subsidiary
39	ISO/IEC 27001	Technology Hardware Storage & Peripherals	30/11/2017	Subsidiary
40	ISO/IEC 27001	IT Consulting & Other Services	12/10/2017	Subsidiary
41	ISO/IEC 27001	IT Consulting & Other Services	06/11/2017	Parent/Holding Co
42	ISO/IEC 27001	IT Consulting & Other Services	09/01/2018	Subsidiary
43	ISO/IEC 27001	Electronic Components	30/10/2017	Subsidiary
44	ISO/IEC 27001	Technology Hardware Storage & Peripherals	17/08/2015	Subsidiary
45	ISO/IEC 27001	IT Consulting & Other Services	19/12/2016	Subsidiary
46	ISO/IEC 27001	Integrated Telecommunication Services	17/04/2018	Subsidiary

Table B.2 continued from previous page

Event ID	Certificate Type	Primary Industry	Date	Certifiee Org Status
47	ISO/IEC 27001	Consumer Electronics	22/02/2016	Subsidiary
48	ISO/IEC 27001	Consumer Electronics	26/03/2018	Subsidiary
49	ISO/IEC 27001	Technology Hardware Storage & Peripherals	21/09/2016	Subsidiary
50	ISO/IEC 27001	Diversified Banks	28/09/2018	Parent/Holding Co
51	ISO/IEC 27001	Oil & Gas Equipment & Services	16/04/2018	Subsidiary
52	ISO/IEC 27001	Air Freight & Logistics	17/10/2018	Subsidiary
53	ISO/IEC 27001	Air Freight & Logistics	10/06/2016	Subsidiary
54	ISO/IEC 27001	Air Freight & Logistics	05/09/2011	Subsidiary
55	ISO/IEC 27001	Diversified Banks	08/01/2018	Subsidiary
56	ISO/IEC 27001	Diversified Banks	12/01/2016	Parent/Holding Co
57	ISO/IEC 27001	IT Consulting & Other Services	02/11/2018	Subsidiary
58	ISO/IEC 27001	Integrated Telecommunication Services	15/10/2015	Subsidiary
59	ISO/IEC 27001	Integrated Telecommunication Services	22/12/2017	Subsidiary
60	ISO/IEC 27001	Wireless Telecommunication Services	01/06/2018	Subsidiary
61	ISO/IEC 27001	Consumer Finance	07/12/2017	Subsidiary
62	ISO/IEC 27001	Research & Consulting Services	09/04/2018	Subsidiary
63	ISO/IEC 27001	Semiconductors	18/06/2018	Subsidiary
64	ISO/IEC 27001	Diversified Real Estate Activities	13/11/2017	Parent/Holding Co
65	ISO/IEC 27001	Oil & Gas Equipment & Services	03/07/2018	Subsidiary
66	ISO/IEC 27001	Application Software	20/03/2018	Subsidiary
67	ISO/IEC 27001	Industrial Conglomerates	05/12/2016	Parent/Holding Co
68	ISO/IEC 27001	Semiconductors	07/12/2017	Subsidiary
69	ISO/IEC 27001	Aerospace & Defense	17/07/2017	Subsidiary

Table B.2 continued from previous page

Event ID	Certificate Type	Primary Industry	Date	Certifiee Org Status
70	ISO/IEC 27001	Independent Power Producers & Energy Traders	22/08/2018	Subsidiary
71	ISO/IEC 27001	Communications Equipment	22/11/2018	Subsidiary
72	ISO/IEC 27001	Technology Hardware Storage & Peripherals	19/10/2018	Subsidiary
73	ISO/IEC 27001	Managed Health Care	29/05/2018	Subsidiary
74	ISO/IEC 27001	Advertising	08/12/2016	Subsidiary
75	ISO/IEC 27001	Research & Consulting Services	19/12/2016	Subsidiary
76	ISO/IEC 27001	IT Consulting & Other Services	18/09/2018	Subsidiary
77	ISO/IEC 27001	Oil & Gas Equipment & Services	26/07/2017	Subsidiary

Appendix C
Severe Security Breaches Sample

Table C.1: Severe Security Breaches Sample

Event	Date (Adj.)	Company	MCap ($m)	Industry Sector	Country
1	09/02/2006	OfficeMax	1,975.29	Consumer Disc	USA
2	01/08/2006	Dollar Tree	2,734.14	Consumer Disc	USA
3	28/08/2006	Copart	2,485.42	Industrials	USA
4	22/09/2006	North Fork Bank	13,145.98	Financials	USA
5	20/12/2006	Deb Shops	373.96	Consumer Disc	USA
6	12/01/2007	MoneyGram International	2,450.91	IT	USA
7	17/01/2007	TJ stores (TJX)	13,484.58	Consumer Disc	USA
8	16/02/2007	Brunswick Corp.	3,070.05	Consumer Disc	USA
9	21/02/2007	Fidelity National Information Services	8,945.43	IT	USA
10	23/07/2007	Fox News	73,140.71	Communication	USA
11	23/08/2007	Monster.com	4,412.59	Communication	USA
12	12/09/2007	Hartford Life Insurance	27,771.67	Financials	USA
13	14/09/2007	TD Ameritrade Holding	10,714.96	Financials	USA
14	10/10/2007	Commerce Bank	3,258.36	Financials	USA
15	31/03/2008	Advance Auto Parts	3,372.99	Consumer Disc	USA
16	10/06/2008	1st Source Bank	460.16	Financials	USA
17	19/06/2008	Citibank	113,728.31	Financials	USA
18	12/08/2008	Wells Fargo	34,541.68	Financials	USA
19	10/09/2008	Franklin Savings and Loan	13.55	Financials	USA
20	06/11/2008	Express Scripts	14,335.30	Health Care	USA
21	20/01/2009	Heartland Payment Systems	533.65	IT	USA
22	23/01/2009	Monster.com	1,149.05	Communication	USA
23	03/02/2009	SRA International	913.76	IT	USA
24	11/03/2009	Sprint	9,849.17	Communication	USA
25	16/03/2009	Comcast	45,130.05	Communication	USA

Table C.1 continued from previous page

Event	Date (Adj.)	Company	MCap ($m)	Industry Sector	Country
26	28/05/2009	Aetna	11,976.92	Health Care	USA
27	23/11/2009	Hancock Fabrics	25.95	Consumer Disc	USA
28	09/04/2010	Charles Schwab	22,943.69	Financials	USA
29	04/06/2010	Digital River	1,033.75	IT	USA
30	09/06/2010	Apple, AT&T	147,134.10	Communication	USA
31	23/06/2010	Anthem Blue Cross, WellPoint	22,653.73	Health Care	USA
32	09/07/2010	Cisco Live 2010	129,643.13	IT	USA
33	02/09/2010	Sprint	12,800.94	Communication	USA
34	10/12/2010	Genesco	882.10	Consumer Disc	USA
35	10/12/2010	Walgreens	33,725.58	Consumer Staples	USA
36	01/04/2011	iTunes (Apple)	317,435.55	IT	USA
37	06/04/2011	Hartford Life Insurance Company	12,439.21	Financials	USA
38	10/05/2011	Fox.com	47,443.97	Communication	USA
39	25/05/2011	Bank of America	115,313.12	Financials	USA
40	27/05/2011	Lockheed Martin	27,004.14	Industrials	USA
41	09/06/2011	Citibank	110,379.11	Financials	USA
42	08/07/2011	Capital Grille	7,260.81	Consumer Disc	USA
43	26/08/2011	Fidelity National Information Services	8,375.17	IT	USA
44	23/09/2011	Hewlett-Packard Enterprise Services	44,349.11	IT	USA
45	02/02/2012	VeriSign	5,871.51	IT	USA
46	10/02/2012	Intel	135,930.94	IT	USA
47	22/02/2012	DHI Mortgage Company	4,413.94	Consumer Disc	USA
48	30/03/2012	Global Payments	3,722.11	IT	USA
49	25/04/2012	Cryptic Studios, Perfect World	595.98	Communication	USA
50	04/05/2012	Ford-Motor Websites	40,720.64	Consumer Disc	USA
51	18/05/2012	Comcast	92,220.86	Communication	USA
52	06/06/2012	LinkedIn.com	9,615.30	Communication	USA
53	13/07/2012	Nvidia	7,769.08	IT	USA
54	09/08/2012	Blizzard Entertainment	12,944.15	Communication	USA
55	04/09/2012	Apple	632,720.92	IT	USA
56	10/10/2012	Equifax	5,850.56	Industrials	USA

Table C.1 continued from previous page

Event	Date (Adj.)	Company	MCap ($m)	Industry Sector	Country
57	12/10/2012	Korn/Ferry International	672.52	Industrials	USA
58	24/10/2012	Barnes & Noble	911.93	Consumer Disc	USA
59	14/11/2012	Adobe	15,958.09	IT	USA
60	11/01/2013	Advanced Micro Devices, Nvidia	1,900.90	IT	USA
61	30/01/2013	The New York Times	1,287.46	Communication	USA
62	19/02/2013	Apple	431,957.29	IT	USA
63	19/02/2013	Express Scripts, Ernst & Young	45,461.82	Health Care	USA
64	22/02/2013	Microsoft	232,524.56	IT	USA
65	27/02/2013	Information Handling Services	6,981.78	Industrials	USA
66	28/03/2013	American Express	74,339.99	Financials	USA
67	28/03/2013	JPMorgan Chase	180,537.84	Financials	USA
68	12/06/2013	comScore	765.78	Communication	USA
69	22/07/2013	Apple	400,329.81	IT	USA
70	26/07/2013	NASDAQ OMX	5,457.94	Financials	USA
71	08/08/2013	US Airways	3,644.48	Industrials	USA
72	09/08/2013	Northrop Grunman	21,978.46	Industrials	USA
73	04/10/2013	Adobe	25,779.19	IT	USA
74	22/10/2013	Aaron's	2,203.58	Consumer Disc	USA
75	28/10/2013	Dun & Bradstreet	4,232.36	Industrials	USA
76	07/11/2013	CME Group, CME ClearPort	24,958.60	Financials	USA
77	25/11/2013	Crown Castle International Corp	24,278.99	Real Estate	USA
78	05/12/2013	JPMorgan Chase	209,599.53	Financials	USA
79	06/12/2013	B&G Foods North America, Maple Grove Farms	1,804.87	Consumer Staples	USA
80	13/12/2013	Target Corp	39,416.99	Consumer Disc	USA
81	27/12/2013	American Express Company	95,546.64	Financials	USA
82	07/02/2014	Boston Scientific	17,491.40	Health Care	USA
83	07/02/2014	Medtronic	55,498.29	Health Care	USA
84	12/02/2014	Las Vegas Sands Hotels and Casinos	64,389.40	Consumer Disc	USA
85	20/02/2014	Alaska Communications	106.87	Communication	USA
86	26/02/2014	Apple	461,470.50	IT	USA

Table C.1 continued from previous page

Event	Date (Adj.)	Company	MCap ($m)	Industry Sector	Country
87	27/02/2014	J.M. Smucker Company	10,331.57	Consumer Staples	USA
88	04/03/2014	Capital One	42,199.12	Financials	USA
89	25/04/2014	Federal Home Loan Mortgage Corporation (Freddie Mac)	12,562.82	Financials	USA
90	28/04/2014	AOL	3,334.73	Communication	USA
91	21/05/2014	Ebay	65,749.74	Consumer Disc	USA
92	12/06/2014	Fidelity National Financial	9,021.45	Financials	USA
93	08/07/2014	Aecom	3,164.09	Industrials	USA
94	11/07/2014	Boeing	93,406.37	Industrials	USA
95	11/07/2014	Lockheed Martin	50,590.16	Industrials	USA
96	21/07/2014	Dominion Resources	40,724.19	Utilities	USA
97	15/08/2014	Supervalue	2,427.82	Consumer Staples	USA
98	18/08/2014	Community Health Systems	5,967.57	Health Care	USA
99	18/08/2014	MeetMe	104.65	Communication	USA
100	28/08/2014	J.P Morgan Chase	222,489.40	Financials	USA
101	02/09/2014	Apple	613,756.37	IT	USA
102	02/09/2014	The Home Depot	122,680.79	Consumer Disc	USA
103	06/10/2014	AT&T	184,051.14	Communication	USA
104	10/10/2014	Sears Holding Company / K-Mart	2,638.38	Consumer Disc	USA
105	20/10/2014	Staples	7,923.67	Consumer Disc	USA
106	03/11/2014	Fidelity National Financial	8,268.75	Financials	USA
107	04/11/2014	Hilton/Hilton Honors Program	24,221.58	Consumer Disc	USA
108	26/11/2014	Shutterfly/Tiny Prints/ Treats/Wedding Divas	1,685.19	Consumer Disc	USA
109	26/12/2014	Microsoft xBox	394,667.79	IT	USA
110	02/01/2015	United Airlines	24,687.14	Industrials	USA
111	05/01/2015	Morgan Stanley	73,402.62	Financials	USA
112	06/01/2015	NVIDIA Corporation	10,430.48	IT	USA
113	05/02/2015	Anthem	37,044.00	Health Care	USA
114	02/03/2015	Natural Grocers	664.06	Consumer Staples	USA
115	02/04/2015	Microsoft/Xbox One	330,530.50	IT	USA
116	08/04/2015	AT&T	169,458.99	Communication	USA
117	12/05/2015	Starbucks	74,545.12	Consumer Disc	USA
118	12/06/2015	Fred's	724.26	Consumer Disc	USA

Table C.1 continued from previous page

Event	Date (Adj.)	Company	MCap ($m)	Industry Sector	Country
119	29/07/2015	United Airlines	21,611.78	Industrials	USA
120	07/08/2015	Ubiquiti Networks	2,784.36	IT	USA
121	19/08/2015	Web.com	1,102.07	IT	USA
122	25/09/2015	Hilton Hotels	22,800.24	Consumer Disc	USA
123	09/10/2015	E-Trade	7,589.87	Financials	USA
124	12/10/2015	Dow Jones & Company	8,126.08	Communication	USA
125	09/11/2015	Comcast	171,805.69	Communication	USA
126	20/11/2015	Starwood Hotels	12,333.58	Consumer Disc	USA
127	21/12/2015	Juniper Network	10,514.47	IT	USA
128	11/01/2016	Blucora (TaxAct)	369.34	Financials	USA
129	15/01/2016	Hyatt Hotels	5,135.17	Consumer Disc	USA
130	27/01/2016	Wendy's	2,630.87	Consumer Disc	USA
131	01/03/2016	Central Concrete Supply Company	778.46	Materials	USA
132	04/03/2016	Seagate	10,235.45	IT	USA
133	08/03/2016	1-800-Flowers	512.47	Consumer Disc	USA
134	28/03/2016	Sprouts Farmers Market	4,345.30	Consumer Staples	USA
135	03/05/2016	Charles Schwab	36,999.20	Financials	USA
136	05/05/2016	ADP	39,380.98	IT	USA
137	16/05/2016	Noodles and Company	281.77	Consumer Disc	USA
138	13/06/2016	Twitter	10,135.05	Communication	USA
139	16/06/2016	Advanced Auto Parts	11,323.83	Consumer Disc	USA
140	29/07/2016	Disney Consumer Products and Interactive Media	155,673.12	Communication	USA
141	23/09/2016	Jive Software/Producteev	333.37	IT	USA
142	12/10/2016	Vera Bradley	527.93	Consumer Disc	USA
143	22/11/2016	The Madison Square Garden Company	4,143.55	Communication	USA
144	23/11/2016	Hewlett Packard Enterprise Services	39,234.30	IT	USA
145	30/11/2016	Google Android	528,611.61	Communication	USA
146	12/12/2016	Quest Diagnostics	12,714.67	Health Care	USA
147	27/01/2017	eHealth Insurance	227.25	Financials	USA
148	27/01/2017	WellCare Health Plans	6,436.22	Health Care	USA
149	02/02/2017	Sunrun	572.03	Industrials	USA
150	06/02/2017	Capital One	42,075.12	Financials	USA

Table C.1 continued from previous page

Event	Date (Adj.)	Company	MCap ($m)	Industry Sector	Country
151	07/03/2017	Verifone	2,242.76	IT	USA
152	15/03/2017	Dunn and Bradstreet	3,986.97	Industrials	USA
153	26/04/2017	Chipotle Mexican Grill	13,843.96	Consumer Disc	USA
154	02/05/2017	Sabre Corporation	6,860.51	IT	USA
155	04/05/2017	Gannett Co	954.54	Communication	USA
156	17/05/2017	Rite Aid	3,849.21	Consumer Staples	USA
157	02/06/2017	Game Stop	2,295.56	Consumer Disc	USA
158	19/06/2017	Bed Bath & Beyond	5,065.82	Consumer Disc	USA
159	20/06/2017	The Buckle	819.71	Consumer Disc	USA
160	31/07/2017	Anthem	48,895.89	Health Care	USA
161	30/08/2017	Instagram	493,481.08	Communication	USA
162	07/09/2017	Equifax Corporation	17,179.56	Industrials	USA
163	29/09/2017	Briggs & Stratton Corp.	1,004.76	Industrials	USA
164	14/11/2017	ABM Industries	2,613.25	Industrials	USA
165	16/11/2017	Hyatt Hotels	8,322.74	Consumer Disc	USA
166	22/01/2018	The Coca-Cola Company	201,870.42	Consumer Staples	USA
167	16/02/2018	Marriott International	49,505.06	Consumer Disc	USA
168	29/03/2018	Under Armour	6,790.71	Consumer Disc	USA
169	06/04/2018	Delta Air Lines	37,363.67	Industrials	USA
170	17/04/2018	Inogen	3,040.36	Health Care	USA
171	20/04/2018	SunTrust Banks	31,301.17	Financials	USA
172	12/06/2018	HealthEquity	4,962.44	Health Care	USA
173	12/06/2018	Nuance Communications	4,171.50	IT	USA
174	06/07/2018	Coty	10,627.61	Consumer Staples	USA
175	28/09/2018	Facebook	474,831.98	Communication	USA
176	01/10/2018	Chegg	3,124.79	Consumer Disc	USA
177	05/10/2018	Five below	6,552.92	Consumer Disc	USA
178	09/10/2018	Roadrunner Transportation Systems	29.23	Industrials	USA
179	25/10/2018	CNO Financial Group	3,092.20	Financials	USA
180	05/11/2018	Nordstrom	11,352.88	Consumer Disc	USA
181	16/11/2018	HealthEquity	5,310.88	Health Care	USA
182	01/03/2017	Autoneum North America	1,255.56	Consumer Disc	CHE
183	11/09/2017	ABB	51,723.53	Industrials	CHE
184	09/10/2018	Givaudan Flavors Corp.	21,918.17	Materials	CHE
185	14/06/2016	Acer Service Corp.	1,467.36	IT	TWN

Table C.1 continued from previous page

Event	Date (Adj.)	Company	MCap ($m)	Industry Sector	Country
186	28/06/2018	Adidas	43,246.28	Consumer Disc	DEU
187	12/03/2007	Dai Nippon	10,456.02	Industrials	JAP
188	04/09/2009	Mitsubishi	32,628.55	Industrials	JAP
189	27/12/2010	American Honda Motor	71,622.71	Consumer Disc	JAP
190	17/06/2011	Sega	4,900.28	Consumer Disc	JAP
191	02/03/2012	Epson America	2,449.03	IT	JAP
192	02/05/2012	Emerson (Funai Corp.)	629.12	Consumer Disc	JAP
193	03/06/2009	Aviva	15,023.03	Financials	GBR
194	26/09/2013	LexisNexis	30,041.68	Industrials	GBR
195	01/10/2015	Experian	15,581.94	Industrials	GBR
196	26/07/2016	Kimpton Hotels	7,787.42	Consumer Disc	GBR
197	28/12/2016	InterContinental Hotels Group	8,548.59	Consumer Disc	GBR
198	16/04/2013	Iberdola USA, Central Maine Power	30,454.70	Utilities	ESP
199	04/03/2015	Mandarin Oriental Hotel Group	1,766.55	Consumer Disc	SGP
200	28/12/2017	Miracle-Ear and Amplifon (USA)	3,437.16	Health Care	ITA
201	30/11/2015	VTech	2,814.59	IT	HKG
202	22/10/2015	Xero	1,452.39	IT	AUS
		Mean	52,019.92		

Note: Date (Adj.) is the PRC breach announcement date, potentially adjusted as described in Section 3.5. MCap ($m) is the market capitalisation at the (adjusted) breach announcement date. Consumer Disc = Consumer Discretionary; Communication = Communication Services; IT = Information Technology.

Appendix D
Indices Used To Establish Abnormal Investment Returns

Table D.1 shows the indices used to proxy country market portfolios for Contribution **C1**.

Table D.1: Indices Used to Proxy Country Market Portfolios

Country	Index Name	Country	Index Name
Australia	S&P/ASX All Australian 200	New Zealand	S&P/NZX 50 Index Gross
Austria	Austria ATX	Nigeria	Nigeria SE All Shares
China	S&P China BMI	Oman	OMSCI Oman
Denmark	OMX Copenhagen 20	Poland	FTSE Poland
France	FTSE France	Qatar	OMSCI Qatar
Germany	Germany DAX	Singapore	OMSCI Singapore
Hong Kong	Hang Seng	South Africa	FTSE South Africa
India	OMSCI India	Switzerland	FTSE Switzerland
Ireland	FTSE Ireland	UAE	OMSCI All UAE
Israel	OMSCI Israel	UK	FTSE 350 and MSCI UK
Japan	TOPIX 100	USA	NASDAQ Composite
Lebanon	S&P Lebanon BMI	Vietnam	STOXX Vietnam Total SE
Netherlands	FTSE Netherlands		

Appendix E
Indices Used To Proxy The Market Portfolio

Table E.1 shows the indices used to proxy country market portfolios for Contributions **C2** and **C4**.

Table E.1: Indices Used to Proxy Country Market Portfolios

Country	Index Name
USA - United States of America	S&P 500
CHE - Switzerland	FTSE Switzerland
TWN - Taiwan	Taiwan TAIEX
DEU - Germany	Germany DAX
JAP - Japan	Nikkei 225
GBR - United Kingdom	FTSE 350
ESP - Spain	Madrid Ibex 35
SGP - Singapore	FTSE Straits Times
ITA - Italy	FTSE MIB
HKG - Hong Kong	Hang Seng
AUS - Australia	S&P/ASX 200

Appendix F
Descriptive Statistics: Regular Beta per Event

All descriptive statistics presented in the appendix are based on 60 daily one-year betas. For each event, across 60 daily betas, Min and Max demonstrate the lowest and greatest value, respectively. Mean (M), Median (Mdn), and Standard Deviation (SD) are based on each event's respective 60 daily values.

	Regular Pre-Breach					Regular Post-Breach				
Event	Min	Max	M	Mdn	SD	Min	Max	M	Mdn	SD
1	0.756	0.919	0.835	0.802	0.063	0.877	1.092	0.997	0.997	0.054
2	0.713	0.828	0.770	0.773	0.027	0.786	0.954	0.843	0.842	0.044
3	1.012	1.129	1.071	1.070	0.031	0.800	0.988	0.890	0.879	0.068
4	0.814	0.873	0.844	0.844	0.015	0.789	0.836	0.812	0.813	0.013
5	0.917	1.161	1.042	1.059	0.066	1.187	1.438	1.359	1.376	0.060
6	1.485	1.832	1.720	1.727	0.067	1.522	1.805	1.651	1.623	0.099
7	0.962	1.111	1.031	1.023	0.042	1.046	1.133	1.086	1.080	0.027
8	1.051	1.184	1.104	1.098	0.041	1.151	1.218	1.182	1.181	0.018
9	1.097	1.170	1.129	1.125	0.017	1.094	1.175	1.147	1.149	0.017
10	0.929	1.054	0.989	0.993	0.031	0.938	1.064	1.022	1.027	0.031
11	1.302	2.085	1.715	1.737	0.221	1.163	1.248	1.202	1.198	0.025
12	1.073	1.255	1.161	1.145	0.059	1.199	1.260	1.220	1.217	0.017
13	1.290	1.584	1.394	1.385	0.070	1.150	1.310	1.238	1.258	0.053
14	0.719	0.825	0.781	0.783	0.030	0.780	0.914	0.844	0.836	0.042
15	0.890	1.021	0.965	0.964	0.034	0.972	1.022	0.992	0.991	0.014
16	2.068	2.140	2.101	2.106	0.017	2.087	2.278	2.195	2.221	0.064
17	1.670	1.802	1.757	1.756	0.031	1.797	2.181	1.985	2.006	0.124
18	1.660	2.264	1.814	1.686	0.212	2.326	4.651	3.077	2.934	0.685

Table F.1 continued from previous page

	Regular Pre-Breach					Regular Post-Breach				
19	-0.527	-0.320	-0.409	-0.404	0.076	-0.583	1.434	0.253	0.411	0.604
20	0.702	1.000	0.827	0.757	0.108	0.946	0.976	0.957	0.957	0.006
21	0.806	0.956	0.897	0.913	0.048	0.895	0.992	0.954	0.966	0.030
22	1.058	1.113	1.086	1.085	0.014	1.096	1.180	1.129	1.115	0.027
23	0.617	0.762	0.731	0.737	0.024	0.676	0.739	0.698	0.701	0.012
24	1.734	1.809	1.784	1.793	0.021	1.740	1.791	1.759	1.757	0.009
25	1.158	1.203	1.180	1.184	0.013	1.203	1.224	1.215	1.217	0.006
26	1.024	1.121	1.086	1.087	0.026	1.037	1.071	1.057	1.057	0.007
27	0.926	1.217	1.103	1.104	0.064	0.456	1.486	1.066	1.140	0.280
28	1.369	1.586	1.487	1.495	0.061	1.107	1.286	1.176	1.147	0.059
29	0.969	1.076	1.026	1.023	0.028	0.976	1.059	1.019	1.021	0.022
30	0.525	0.631	0.570	0.571	0.024	0.549	0.609	0.577	0.573	0.016
31	0.625	0.750	0.690	0.693	0.026	0.671	0.834	0.763	0.742	0.053
32	0.979	1.124	1.054	1.049	0.041	1.063	1.100	1.085	1.086	0.010
33	1.283	1.403	1.354	1.358	0.027	1.232	1.441	1.325	1.334	0.054
34	1.226	1.271	1.253	1.253	0.009	1.210	1.314	1.261	1.251	0.032
35	0.777	0.890	0.852	0.862	0.033	0.880	0.912	0.893	0.892	0.007
36	0.992	1.058	1.013	1.006	0.019	0.886	1.023	0.957	0.950	0.043
37	1.805	1.874	1.851	1.866	0.025	1.866	1.999	1.926	1.933	0.035
38	1.478	1.514	1.494	1.492	0.008	1.431	1.555	1.503	1.512	0.038
39	1.489	1.593	1.550	1.562	0.030	1.412	1.945	1.561	1.515	0.168
40	0.620	0.696	0.677	0.685	0.020	0.589	0.704	0.636	0.629	0.034
41	1.277	1.420	1.334	1.325	0.044	1.296	1.708	1.453	1.351	0.170
42	0.848	0.918	0.886	0.884	0.019	0.803	0.897	0.856	0.849	0.026
43	0.817	1.018	0.912	0.920	0.063	0.949	1.060	1.012	1.009	0.028
44	0.768	1.003	0.857	0.815	0.083	0.944	1.123	1.059	1.072	0.056
45	0.976	1.007	0.988	0.988	0.008	0.969	0.992	0.983	0.985	0.007
46	0.769	0.858	0.832	0.843	0.027	0.833	0.859	0.849	0.851	0.007
47	1.228	1.276	1.256	1.258	0.013	1.240	1.309	1.279	1.277	0.018
48	1.029	1.044	1.037	1.037	0.004	1.021	1.045	1.033	1.034	0.006
49	1.155	1.252	1.189	1.178	0.027	1.246	1.307	1.275	1.280	0.019
50	1.341	1.358	1.350	1.350	0.004	1.282	1.361	1.336	1.353	0.026
51	0.970	1.002	0.981	0.977	0.009	0.929	0.970	0.957	0.957	0.007
52	1.289	1.339	1.317	1.319	0.014	1.151	1.346	1.282	1.298	0.046

Table F.1 continued from previous page

	Regular Pre-Breach					Regular Post-Breach				
53	1.466	1.508	1.488	1.488	0.015	1.378	1.501	1.453	1.453	0.031
54	0.619	0.677	0.645	0.640	0.016	0.639	0.775	0.675	0.663	0.035
55	0.750	0.806	0.787	0.796	0.017	0.769	1.145	0.921	0.877	0.113
56	1.056	1.100	1.081	1.082	0.013	0.891	1.050	0.957	0.940	0.055
57	1.930	2.219	2.068	2.063	0.097	1.399	1.992	1.641	1.549	0.197
58	0.601	1.099	0.822	0.813	0.124	0.491	0.937	0.684	0.678	0.096
59	1.145	1.309	1.215	1.221	0.045	1.162	1.277	1.205	1.188	0.041
60	2.147	2.338	2.241	2.235	0.057	2.124	2.258	2.185	2.190	0.036
61	1.452	1.661	1.535	1.511	0.063	1.400	1.537	1.453	1.443	0.034
62	1.084	1.276	1.221	1.245	0.062	1.182	1.278	1.237	1.237	0.020
63	0.911	0.977	0.939	0.938	0.017	0.863	0.953	0.907	0.911	0.017
64	1.000	1.132	1.094	1.107	0.036	1.038	1.096	1.077	1.080	0.016
65	0.790	0.866	0.832	0.830	0.019	0.755	0.821	0.796	0.796	0.017
66	1.067	1.156	1.104	1.112	0.024	1.014	1.089	1.055	1.060	0.021
67	1.338	1.498	1.401	1.405	0.031	1.248	1.349	1.304	1.305	0.030
68	0.653	0.899	0.763	0.707	0.088	0.738	1.160	0.939	0.849	0.167
69	1.083	1.268	1.136	1.109	0.054	0.982	1.133	1.073	1.084	0.041
70	0.992	1.086	1.028	1.027	0.026	0.988	1.055	1.024	1.028	0.019
71	0.714	0.956	0.830	0.834	0.059	0.855	1.101	1.007	1.038	0.074
72	0.835	0.888	0.860	0.863	0.016	0.815	0.898	0.854	0.856	0.027
73	0.867	0.974	0.915	0.907	0.037	0.976	1.171	1.060	1.067	0.058
74	0.780	0.861	0.819	0.821	0.016	0.730	0.846	0.780	0.783	0.028
75	0.779	0.923	0.852	0.866	0.039	0.936	1.085	0.986	0.957	0.055
76	0.719	0.785	0.759	0.761	0.019	0.799	0.889	0.848	0.849	0.023
77	0.728	0.819	0.777	0.776	0.019	0.716	0.830	0.769	0.774	0.027
78	1.191	1.260	1.229	1.229	0.017	1.190	1.261	1.222	1.217	0.020
79	0.987	1.068	1.029	1.034	0.021	0.877	1.050	0.969	0.990	0.056
80	0.536	0.599	0.562	0.561	0.017	0.554	0.660	0.631	0.636	0.022
81	1.045	1.101	1.079	1.080	0.013	1.128	1.208	1.165	1.158	0.026
82	1.088	1.155	1.124	1.132	0.020	1.113	1.263	1.165	1.133	0.054
83	0.903	0.947	0.919	0.920	0.011	0.883	0.938	0.920	0.927	0.016
84	1.258	1.429	1.330	1.330	0.046	1.419	1.577	1.507	1.501	0.039
85	1.146	1.382	1.255	1.236	0.069	1.344	1.592	1.464	1.457	0.083
86	0.491	0.767	0.618	0.606	0.084	0.390	0.523	0.468	0.488	0.048

Table F.1 continued from previous page

	Regular Pre-Breach					Regular Post-Breach				
87	0.831	0.895	0.859	0.856	0.017	0.790	0.843	0.814	0.816	0.017
88	1.075	1.173	1.138	1.148	0.030	1.127	1.188	1.164	1.164	0.015
89	0.810	1.392	1.122	1.188	0.165	0.374	1.144	0.800	0.766	0.193
90	0.964	1.203	1.054	1.039	0.072	1.102	1.199	1.142	1.138	0.022
91	1.027	1.078	1.052	1.052	0.010	0.968	1.046	1.016	1.019	0.018
92	0.897	0.972	0.943	0.945	0.022	0.615	0.949	0.735	0.764	0.094
93	1.415	1.561	1.460	1.454	0.033	1.370	1.573	1.430	1.397	0.064
94	1.130	1.167	1.148	1.149	0.009	1.031	1.146	1.080	1.081	0.035
95	0.960	1.012	0.981	0.975	0.017	0.983	1.055	1.013	1.015	0.014
96	0.546	0.717	0.645	0.656	0.052	0.549	0.612	0.576	0.577	0.015
97	1.249	1.441	1.335	1.304	0.057	1.182	1.364	1.277	1.276	0.057
98	0.857	1.050	0.933	0.906	0.058	0.977	1.191	1.067	1.043	0.075
99	1.999	2.688	2.251	2.122	0.225	2.103	2.278	2.185	2.183	0.042
100	1.171	1.216	1.193	1.192	0.011	1.097	1.171	1.146	1.142	0.017
101	0.432	0.584	0.502	0.494	0.043	0.537	0.707	0.642	0.631	0.048
102	0.741	0.790	0.770	0.771	0.010	0.773	0.873	0.819	0.814	0.036
103	0.637	0.669	0.655	0.656	0.008	0.523	0.616	0.564	0.559	0.025
104	1.234	1.567	1.404	1.381	0.075	1.146	1.474	1.276	1.266	0.081
105	0.915	1.302	1.120	1.105	0.092	0.618	0.895	0.771	0.820	0.098
106	0.585	0.687	0.640	0.636	0.029	0.565	0.678	0.615	0.598	0.039
107	0.830	1.014	0.882	0.853	0.057	1.005	1.168	1.068	1.074	0.054
108	1.215	1.504	1.354	1.335	0.098	1.012	1.274	1.146	1.149	0.068
109	0.900	0.985	0.947	0.954	0.024	0.930	1.188	1.097	1.150	0.098
110	1.473	1.634	1.561	1.567	0.042	1.285	1.462	1.390	1.402	0.047
111	1.293	1.408	1.329	1.325	0.025	1.326	1.408	1.371	1.376	0.023
112	1.153	1.289	1.208	1.207	0.034	1.221	1.381	1.299	1.302	0.049
113	0.936	1.048	0.973	0.969	0.023	1.053	1.127	1.086	1.082	0.026
114	0.696	1.222	0.946	0.949	0.193	0.358	0.700	0.532	0.511	0.106
115	0.930	1.188	1.106	1.150	0.093	1.102	1.173	1.145	1.152	0.020
116	0.488	0.566	0.526	0.533	0.021	0.592	0.633	0.619	0.622	0.011
117	0.773	0.845	0.815	0.818	0.019	0.796	0.845	0.822	0.821	0.013
118	0.683	0.798	0.720	0.706	0.032	0.633	0.845	0.727	0.734	0.043
119	1.090	1.190	1.139	1.137	0.025	0.861	1.153	0.992	0.951	0.087
120	1.123	1.258	1.181	1.176	0.032	0.705	1.129	0.847	0.786	0.129

Table F.1 continued from previous page

	Regular Pre-Breach					Regular Post-Breach				
121	1.276	1.478	1.362	1.324	0.078	1.017	1.211	1.060	1.054	0.032
122	1.043	1.201	1.144	1.169	0.050	1.021	1.143	1.069	1.057	0.036
123	1.349	1.444	1.394	1.388	0.029	1.416	1.479	1.440	1.432	0.018
124	1.046	1.160	1.113	1.117	0.029	1.117	1.206	1.162	1.158	0.025
125	0.930	0.996	0.964	0.963	0.017	0.929	0.999	0.968	0.973	0.018
126	1.039	1.121	1.093	1.098	0.021	1.030	1.090	1.057	1.053	0.018
127	0.925	1.009	0.975	0.981	0.022	0.944	1.001	0.977	0.976	0.014
128	0.758	0.884	0.844	0.844	0.030	0.833	1.003	0.899	0.900	0.045
129	0.963	1.015	0.978	0.976	0.013	0.965	1.030	1.007	1.009	0.015
130	0.694	0.741	0.721	0.720	0.011	0.694	0.769	0.721	0.719	0.015
131	0.890	1.199	1.045	1.032	0.096	1.147	1.240	1.184	1.176	0.026
132	1.088	1.321	1.182	1.150	0.078	1.294	1.358	1.323	1.324	0.013
133	0.749	0.897	0.822	0.821	0.037	0.792	0.876	0.833	0.832	0.020
134	0.581	0.755	0.672	0.663	0.048	0.765	0.866	0.821	0.840	0.034
135	1.379	1.541	1.458	1.477	0.056	1.560	1.716	1.634	1.598	0.063
136	1.020	1.047	1.033	1.033	0.009	1.012	1.032	1.023	1.023	0.005
137	0.576	0.678	0.643	0.653	0.027	0.632	0.725	0.683	0.685	0.026
138	1.109	1.172	1.146	1.148	0.017	1.158	1.392	1.227	1.208	0.053
139	0.862	0.916	0.887	0.877	0.018	0.858	1.009	0.899	0.871	0.049
140	0.928	0.960	0.943	0.944	0.010	0.899	0.945	0.919	0.915	0.013
141	0.820	1.185	0.935	0.836	0.140	1.198	1.295	1.259	1.269	0.029
142	0.768	0.987	0.890	0.921	0.059	0.687	0.943	0.819	0.819	0.069
143	0.551	0.663	0.601	0.587	0.037	0.528	0.673	0.609	0.610	0.028
144	1.615	1.700	1.652	1.649	0.022	1.484	1.630	1.569	1.578	0.031
145	0.930	0.977	0.952	0.952	0.011	0.915	1.033	0.972	0.967	0.031
146	0.841	0.934	0.885	0.886	0.022	0.850	0.937	0.903	0.900	0.019
147	1.111	1.345	1.239	1.233	0.058	1.174	1.381	1.289	1.305	0.058
148	0.780	0.966	0.873	0.887	0.046	0.588	0.845	0.691	0.694	0.069
149	0.633	1.256	0.902	0.884	0.181	1.039	1.679	1.467	1.562	0.194
150	1.425	1.577	1.465	1.451	0.036	1.522	1.620	1.568	1.555	0.030
151	1.251	1.397	1.322	1.323	0.045	1.130	1.231	1.168	1.157	0.030
152	1.031	1.292	1.174	1.191	0.072	0.997	1.082	1.043	1.053	0.028
153	0.448	0.623	0.551	0.550	0.049	0.544	0.746	0.653	0.660	0.058
154	0.908	1.026	0.950	0.944	0.031	1.013	1.091	1.057	1.058	0.017

Table F.1 continued from previous page

	Regular Pre-Breach					Regular Post-Breach				
155	1.099	1.391	1.300	1.327	0.076	1.327	1.651	1.480	1.417	0.105
156	0.293	0.554	0.429	0.440	0.080	0.582	2.050	1.384	1.680	0.566
157	1.349	1.449	1.397	1.394	0.026	1.368	1.624	1.462	1.439	0.064
158	1.195	1.351	1.274	1.274	0.051	1.111	1.391	1.246	1.248	0.057
159	1.021	1.191	1.114	1.123	0.045	1.082	1.416	1.195	1.178	0.069
160	0.997	1.214	1.099	1.070	0.073	0.949	1.193	1.102	1.112	0.045
161	1.005	1.145	1.085	1.100	0.046	1.140	1.391	1.272	1.279	0.064
162	0.954	1.066	1.003	0.996	0.026	0.728	0.897	0.814	0.820	0.042
163	1.360	1.794	1.579	1.457	0.156	1.725	1.938	1.858	1.862	0.054
164	1.203	1.325	1.274	1.286	0.032	0.953	1.329	1.224	1.261	0.095
165	0.911	1.085	0.972	0.959	0.051	0.840	1.002	0.922	0.924	0.035
166	0.127	0.360	0.248	0.275	0.085	0.114	0.542	0.460	0.508	0.121
167	1.151	1.244	1.192	1.191	0.025	1.031	1.121	1.058	1.052	0.022
168	1.166	1.631	1.440	1.428	0.103	1.216	1.344	1.268	1.265	0.031
169	1.141	1.885	1.431	1.310	0.261	1.056	1.179	1.102	1.089	0.039
170	0.997	1.625	1.157	1.068	0.207	0.991	1.134	1.067	1.063	0.034
171	1.261	1.622	1.360	1.309	0.103	1.132	1.206	1.168	1.164	0.020
172	0.748	0.879	0.808	0.809	0.024	0.763	0.846	0.802	0.801	0.022
173	0.903	1.126	1.030	1.057	0.073	0.878	0.946	0.913	0.909	0.017
174	0.316	0.381	0.350	0.351	0.016	0.342	0.432	0.387	0.392	0.027
175	1.272	1.351	1.320	1.331	0.025	1.228	1.324	1.280	1.282	0.028
176	0.828	0.927	0.872	0.875	0.028	0.892	1.271	1.162	1.230	0.120
177	0.672	0.719	0.694	0.691	0.011	0.693	1.066	0.897	0.868	0.099
178	1.341	1.538	1.442	1.453	0.052	0.680	1.448	1.034	0.993	0.200
179	0.892	0.937	0.921	0.922	0.010	0.902	1.020	0.965	0.955	0.039
180	0.825	0.914	0.873	0.871	0.021	0.796	0.873	0.829	0.827	0.021
181	0.751	1.062	0.837	0.782	0.093	1.101	1.577	1.343	1.353	0.132
182	0.991	1.057	1.029	1.036	0.018	0.967	1.080	1.024	1.030	0.027
183	0.665	0.808	0.718	0.719	0.029	0.652	0.737	0.684	0.678	0.025
184	0.811	0.849	0.830	0.830	0.010	0.776	0.822	0.797	0.797	0.010
185	1.584	1.672	1.610	1.601	0.021	1.507	1.705	1.661	1.675	0.042
186	0.784	0.858	0.817	0.813	0.018	0.862	0.945	0.904	0.905	0.030
187	0.725	0.817	0.779	0.777	0.024	0.713	0.763	0.739	0.741	0.012
188	1.055	1.080	1.067	1.066	0.008	1.041	1.225	1.122	1.131	0.061

Table F.1 continued from previous page

	Regular Pre-Breach					Regular Post-Breach				
189	0.867	0.899	0.883	0.885	0.008	0.699	0.884	0.829	0.838	0.055
190	0.835	0.934	0.883	0.869	0.024	0.935	1.066	1.009	1.025	0.038
191	0.861	0.902	0.887	0.889	0.008	0.877	1.119	1.037	1.057	0.074
192	0.743	0.923	0.819	0.762	0.073	0.894	1.001	0.958	0.962	0.025
193	1.808	1.998	1.922	1.914	0.047	2.002	2.049	2.029	2.030	0.012
194	0.757	0.956	0.821	0.814	0.053	0.738	0.802	0.768	0.762	0.016
195	0.883	0.983	0.947	0.947	0.022	0.973	1.055	1.014	1.012	0.018
196	1.070	1.198	1.121	1.085	0.051	1.167	1.227	1.202	1.205	0.019
197	1.184	1.248	1.213	1.220	0.018	1.231	1.336	1.277	1.276	0.028
198	1.349	1.390	1.364	1.368	0.013	1.311	1.386	1.357	1.362	0.023
199	0.391	0.523	0.467	0.467	0.033	0.434	0.509	0.480	0.483	0.017
200	0.204	0.380	0.259	0.238	0.048	0.348	0.524	0.451	0.461	0.046
201	0.278	0.319	0.300	0.300	0.009	0.294	0.376	0.329	0.334	0.022
202	0.338	0.611	0.501	0.527	0.087	0.525	0.808	0.630	0.618	0.083
Mean	0.980	1.137	1.055	1.050	0.045	0.986	1.173	1.077	1.077	0.054

Appendix G
Descriptive Statistics: Upside Beta per Event

All descriptive statistics presented in the appendix are based on 60 daily one-year betas. For each event, across 60 daily betas, Min and Max demonstrate the lowest and greatest value, respectively. Mean (M), Median (Mdn), and Standard Deviation (SD) are based on each event's respective 60 daily values.

	Upside Pre-Breach					Upside Post-Breach				
Event	Min	Max	M	Mdn	SD	Min	Max	M	Mdn	SD
1	0.704	1.148	0.962	1.070	0.164	0.555	0.783	0.695	0.732	0.072
2	0.389	0.849	0.634	0.661	0.133	0.413	0.713	0.480	0.465	0.057
3	0.862	1.012	0.969	0.976	0.037	0.525	0.908	0.689	0.620	0.149
4	0.500	0.595	0.555	0.562	0.032	0.464	0.590	0.523	0.521	0.024
5	1.671	1.864	1.767	1.767	0.043	1.673	2.001	1.867	1.869	0.064
6	0.752	1.306	0.915	0.871	0.141	1.145	1.288	1.194	1.191	0.032
7	0.899	1.228	1.025	1.002	0.092	1.013	1.203	1.126	1.147	0.065
8	0.698	1.011	0.827	0.786	0.112	0.943	1.091	1.014	1.013	0.033
9	1.115	1.280	1.213	1.211	0.037	0.936	1.220	1.078	1.088	0.083
10	0.939	1.114	1.039	1.058	0.059	0.892	1.108	1.043	1.054	0.057
11	0.822	2.462	1.785	1.918	0.508	0.715	0.907	0.783	0.779	0.045
12	1.075	1.215	1.108	1.099	0.032	1.076	1.390	1.194	1.165	0.106
13	1.206	1.706	1.400	1.386	0.135	0.882	1.225	1.076	1.066	0.109
14	0.870	1.098	0.969	0.981	0.062	0.996	1.241	1.135	1.149	0.079
15	0.771	1.030	0.915	0.920	0.077	0.742	0.943	0.865	0.889	0.066
16	2.637	2.954	2.736	2.724	0.068	2.672	3.296	3.024	3.117	0.223
17	2.396	2.535	2.466	2.470	0.037	2.432	2.778	2.590	2.587	0.095
18	2.337	3.270	2.588	2.412	0.304	3.288	7.744	4.514	3.644	1.543

Table G.1 continued from previous page

	Upside Pre-Breach					Upside Post-Breach				
19	-0.300	0.019	-0.072	-0.043	0.070	-0.006	2.785	1.235	1.652	0.972
20	0.578	1.107	0.822	0.766	0.154	0.960	1.004	0.978	0.978	0.010
21	0.678	0.893	0.807	0.823	0.055	0.646	0.824	0.743	0.722	0.061
22	1.010	1.122	1.071	1.072	0.033	1.083	1.251	1.154	1.134	0.052
23	0.478	0.610	0.565	0.577	0.038	0.511	0.587	0.559	0.570	0.025
24	1.853	1.944	1.885	1.884	0.016	1.868	1.959	1.928	1.931	0.021
25	1.278	1.367	1.308	1.304	0.024	1.379	1.424	1.405	1.406	0.009
26	0.828	1.013	0.979	0.994	0.047	0.969	1.048	1.016	1.026	0.024
27	-0.866	0.070	-0.318	-0.266	0.373	-0.539	-0.043	-0.251	-0.161	0.176
28	1.610	1.915	1.767	1.761	0.083	1.027	1.499	1.239	1.195	0.149
29	1.290	1.619	1.461	1.476	0.082	1.165	1.367	1.260	1.263	0.050
30	0.486	0.720	0.580	0.562	0.064	0.605	0.732	0.664	0.658	0.034
31	0.631	0.894	0.742	0.705	0.096	0.572	0.687	0.611	0.604	0.025
32	0.968	1.294	1.125	1.068	0.104	0.966	1.104	1.041	1.047	0.044
33	0.979	1.215	1.074	1.057	0.080	0.981	1.398	1.146	1.163	0.099
34	1.007	1.082	1.048	1.048	0.020	1.058	1.255	1.167	1.158	0.056
35	0.689	0.745	0.724	0.727	0.015	0.687	0.750	0.720	0.724	0.021
36	1.107	1.195	1.151	1.150	0.021	1.046	1.243	1.158	1.177	0.065
37	1.578	1.718	1.654	1.655	0.048	1.670	1.836	1.715	1.717	0.032
38	1.520	1.611	1.556	1.547	0.025	1.290	1.570	1.463	1.517	0.097
39	1.592	1.649	1.619	1.618	0.014	1.642	2.335	1.787	1.690	0.223
40	0.535	0.605	0.574	0.574	0.018	0.557	0.672	0.608	0.604	0.035
41	1.091	1.230	1.153	1.155	0.030	1.154	1.804	1.403	1.230	0.263
42	0.916	1.147	0.964	0.947	0.049	0.874	1.116	0.989	1.032	0.081
43	0.802	1.073	0.927	0.923	0.087	0.921	1.023	0.983	0.994	0.030
44	0.685	0.960	0.831	0.791	0.076	0.760	1.033	0.945	0.971	0.069
45	1.118	1.281	1.192	1.187	0.063	1.132	1.166	1.150	1.152	0.009
46	0.806	0.885	0.833	0.827	0.023	0.764	0.823	0.803	0.809	0.017
47	1.053	1.165	1.118	1.121	0.027	1.005	1.174	1.099	1.121	0.055
48	1.141	1.168	1.159	1.160	0.006	1.203	1.228	1.217	1.217	0.005
49	1.126	1.480	1.294	1.345	0.116	1.135	1.280	1.211	1.219	0.039
50	1.432	1.518	1.477	1.486	0.027	1.344	1.515	1.439	1.458	0.060
51	0.835	0.871	0.856	0.857	0.008	0.811	0.921	0.837	0.829	0.030
52	1.451	1.573	1.519	1.508	0.031	1.301	1.488	1.380	1.370	0.057

Table G.1 continued from previous page

	Upside Pre-Breach					Upside Post-Breach				
53	1.796	1.903	1.852	1.850	0.026	1.412	1.833	1.621	1.592	0.141
54	0.564	0.629	0.600	0.608	0.018	0.555	0.698	0.632	0.636	0.041
55	0.631	0.791	0.733	0.747	0.044	0.651	1.179	0.812	0.769	0.141
56	0.949	1.119	1.058	1.070	0.058	0.628	1.039	0.830	0.843	0.130
57	1.892	2.489	2.223	2.294	0.193	1.380	2.170	1.704	1.564	0.270
58	0.791	1.127	1.000	1.028	0.091	0.403	0.952	0.669	0.733	0.156
59	1.100	1.259	1.166	1.163	0.045	1.126	1.262	1.183	1.180	0.042
60	1.667	1.927	1.802	1.802	0.061	1.633	1.922	1.735	1.737	0.058
61	1.485	1.890	1.678	1.649	0.132	1.276	1.462	1.345	1.332	0.041
62	1.006	1.671	1.372	1.408	0.185	1.469	1.803	1.680	1.734	0.106
63	0.816	1.028	0.897	0.876	0.054	0.800	0.930	0.867	0.868	0.037
64	0.927	1.202	1.108	1.111	0.072	1.132	1.241	1.170	1.169	0.020
65	0.890	0.997	0.935	0.940	0.027	0.846	0.939	0.903	0.899	0.023
66	1.119	1.197	1.157	1.158	0.018	1.081	1.151	1.118	1.116	0.014
67	1.095	1.408	1.216	1.226	0.061	1.023	1.207	1.102	1.095	0.049
68	-0.133	0.160	-0.010	-0.078	0.111	0.027	1.158	0.552	0.247	0.492
69	1.368	1.678	1.451	1.447	0.057	1.476	1.790	1.640	1.604	0.104
70	1.069	1.242	1.178	1.180	0.058	1.341	1.479	1.402	1.390	0.036
71	0.604	0.853	0.744	0.724	0.065	0.705	1.376	1.123	1.213	0.214
72	0.530	0.778	0.663	0.713	0.094	0.502	0.728	0.598	0.569	0.077
73	0.905	1.238	1.032	1.013	0.107	1.186	1.566	1.289	1.269	0.092
74	1.020	1.225	1.109	1.114	0.047	0.781	1.049	0.921	0.940	0.068
75	0.819	1.150	0.979	0.996	0.088	1.063	1.425	1.188	1.120	0.138
76	0.765	0.925	0.822	0.793	0.052	0.981	1.379	1.188	1.113	0.133
77	0.919	1.077	1.007	1.006	0.045	0.788	1.031	0.894	0.886	0.074
78	0.975	1.185	1.071	1.079	0.066	1.169	1.396	1.308	1.329	0.074
79	0.966	1.125	1.060	1.075	0.036	0.800	1.094	0.992	1.036	0.086
80	0.306	0.408	0.360	0.363	0.027	0.261	0.566	0.445	0.487	0.083
81	1.115	1.293	1.206	1.196	0.049	1.281	1.428	1.336	1.321	0.040
82	0.564	0.747	0.641	0.637	0.045	0.501	0.857	0.654	0.599	0.127
83	0.732	0.931	0.827	0.812	0.071	0.856	0.950	0.896	0.892	0.023
84	0.882	1.279	1.081	1.128	0.146	1.049	1.313	1.158	1.146	0.066
85	-0.288	0.201	-0.101	-0.103	0.105	-0.511	0.151	-0.039	-0.058	0.140
86	0.284	1.289	0.692	0.653	0.326	-0.043	0.305	0.159	0.200	0.121

Table G.1 continued from previous page

	Upside Pre-Breach					Upside Post-Breach				
87	0.804	1.047	0.937	0.924	0.062	0.612	0.828	0.707	0.715	0.068
88	1.114	1.414	1.237	1.190	0.104	1.204	1.312	1.251	1.247	0.024
89	0.286	1.361	0.771	0.630	0.358	-0.475	0.635	0.151	0.182	0.392
90	1.237	1.617	1.411	1.409	0.077	1.391	1.617	1.526	1.541	0.061
91	0.699	0.995	0.798	0.777	0.064	0.608	0.781	0.689	0.692	0.059
92	0.425	0.656	0.537	0.526	0.062	0.426	0.711	0.519	0.496	0.079
93	0.924	1.006	0.969	0.971	0.021	0.942	1.027	0.984	0.987	0.021
94	1.001	1.113	1.051	1.044	0.029	1.073	1.261	1.192	1.205	0.051
95	1.059	1.171	1.113	1.113	0.029	1.113	1.341	1.217	1.217	0.059
96	0.639	0.752	0.688	0.689	0.028	0.692	0.924	0.833	0.844	0.056
97	1.716	2.037	1.888	1.866	0.087	1.624	1.996	1.759	1.760	0.066
98	0.252	1.006	0.615	0.596	0.241	0.204	0.673	0.430	0.354	0.161
99	1.528	3.473	2.266	2.114	0.557	1.670	2.036	1.869	1.862	0.104
100	1.332	1.515	1.442	1.462	0.056	1.213	1.420	1.319	1.329	0.054
101	0.025	0.159	0.079	0.079	0.032	-0.113	0.388	0.136	0.059	0.198
102	0.580	0.691	0.634	0.627	0.025	0.494	0.722	0.605	0.575	0.088
103	0.587	0.707	0.647	0.668	0.041	0.460	0.610	0.536	0.519	0.041
104	-1.155	-0.337	-0.670	-0.627	0.201	-1.598	-0.176	-1.002	-1.094	0.356
105	0.837	1.160	1.032	1.046	0.063	0.526	0.846	0.718	0.774	0.106
106	0.410	0.697	0.500	0.472	0.078	0.596	0.746	0.690	0.700	0.035
107	0.619	1.013	0.742	0.708	0.110	0.926	1.151	1.018	1.028	0.065
108	0.307	1.017	0.700	0.600	0.265	0.112	0.705	0.447	0.402	0.134
109	0.970	1.269	1.136	1.146	0.072	1.247	1.393	1.326	1.320	0.049
110	1.092	1.498	1.319	1.334	0.069	1.119	1.566	1.376	1.374	0.112
111	1.123	1.390	1.224	1.211	0.040	1.148	1.303	1.218	1.223	0.032
112	1.556	1.833	1.691	1.697	0.076	1.396	1.653	1.524	1.509	0.076
113	1.012	1.246	1.137	1.109	0.063	1.282	1.362	1.312	1.310	0.019
114	0.122	0.613	0.308	0.308	0.141	-0.215	0.190	-0.036	-0.036	0.086
115	1.229	1.393	1.324	1.320	0.051	1.095	1.260	1.189	1.181	0.049
116	0.489	0.623	0.563	0.562	0.038	0.496	0.664	0.571	0.561	0.048
117	0.411	0.548	0.491	0.491	0.040	0.438	0.534	0.492	0.501	0.028
118	0.767	1.101	0.965	1.011	0.101	0.215	0.801	0.612	0.686	0.173
119	0.720	1.007	0.855	0.871	0.080	0.504	0.899	0.664	0.597	0.142
120	1.199	1.545	1.376	1.403	0.099	1.012	1.449	1.141	1.092	0.125

Table G.1 continued from previous page

	Upside Pre-Breach					Upside Post-Breach				
121	1.508	1.653	1.577	1.578	0.036	1.008	1.547	1.172	1.138	0.104
122	1.019	1.252	1.147	1.163	0.074	0.923	1.098	0.999	0.998	0.053
123	1.023	1.425	1.211	1.143	0.135	1.441	1.592	1.547	1.548	0.026
124	0.824	0.977	0.908	0.900	0.035	0.902	1.146	0.993	0.970	0.061
125	0.871	1.071	0.962	0.964	0.052	0.841	0.952	0.901	0.914	0.030
126	0.780	0.966	0.842	0.810	0.064	0.847	1.009	0.929	0.927	0.039
127	0.684	0.903	0.810	0.798	0.062	0.769	1.045	0.918	0.974	0.102
128	0.798	1.118	0.946	0.953	0.098	0.251	0.811	0.495	0.401	0.216
129	0.981	1.077	1.029	1.025	0.026	0.886	1.017	0.965	0.966	0.034
130	0.577	0.719	0.688	0.700	0.033	0.598	0.746	0.667	0.664	0.028
131	0.839	1.613	1.183	1.115	0.274	1.322	1.487	1.413	1.401	0.051
132	1.414	1.703	1.535	1.518	0.097	1.583	1.860	1.733	1.802	0.110
133	0.062	0.490	0.268	0.293	0.139	0.409	0.544	0.464	0.459	0.036
134	0.518	0.929	0.741	0.708	0.146	0.889	0.997	0.934	0.934	0.020
135	1.209	1.475	1.384	1.417	0.084	1.388	1.479	1.437	1.451	0.029
136	1.029	1.090	1.064	1.069	0.016	1.018	1.093	1.061	1.060	0.010
137	0.686	0.907	0.806	0.824	0.053	0.707	1.136	0.842	0.781	0.134
138	1.277	1.520	1.473	1.476	0.039	1.226	1.614	1.465	1.500	0.125
139	0.777	0.875	0.819	0.815	0.027	0.829	1.062	0.910	0.878	0.080
140	0.997	1.062	1.022	1.022	0.016	0.930	0.999	0.971	0.972	0.017
141	0.185	0.506	0.335	0.311	0.103	0.260	0.679	0.436	0.397	0.128
142	0.564	1.152	0.957	1.062	0.167	0.350	0.720	0.560	0.651	0.142
143	0.391	0.602	0.479	0.487	0.069	0.415	0.793	0.532	0.502	0.090
144	0.914	1.153	1.007	0.988	0.067	0.708	1.102	0.958	1.027	0.124
145	0.972	1.069	1.018	1.018	0.029	1.019	1.189	1.082	1.059	0.053
146	0.741	0.982	0.857	0.847	0.053	0.540	0.808	0.750	0.766	0.058
147	1.695	2.071	1.911	1.912	0.096	1.755	2.435	2.169	2.257	0.218
148	0.804	1.003	0.890	0.890	0.039	0.489	0.924	0.613	0.582	0.109
149	-0.861	-0.219	-0.567	-0.575	0.211	-0.804	0.654	0.092	0.386	0.495
150	1.410	1.559	1.455	1.441	0.039	1.494	1.727	1.571	1.543	0.069
151	1.355	1.786	1.659	1.721	0.119	1.137	1.361	1.228	1.227	0.055
152	1.002	1.253	1.172	1.179	0.056	0.749	1.036	0.918	0.975	0.097
153	0.447	0.947	0.690	0.677	0.138	0.548	0.857	0.732	0.730	0.090
154	0.907	1.254	1.032	1.023	0.089	0.924	1.050	0.986	0.981	0.038

Table G.1 continued from previous page

	Upside Pre-Breach					Upside Post-Breach				
155	0.850	1.481	1.283	1.293	0.147	1.338	1.746	1.566	1.553	0.128
156	0.087	0.267	0.187	0.184	0.048	-0.216	0.449	0.237	0.226	0.138
157	0.955	1.257	1.068	1.065	0.061	1.259	1.670	1.421	1.434	0.081
158	1.128	1.279	1.212	1.226	0.047	1.074	1.509	1.321	1.309	0.113
159	1.067	1.377	1.214	1.212	0.084	0.624	1.557	1.211	1.249	0.272
160	0.809	1.183	1.024	1.024	0.119	1.038	1.191	1.135	1.143	0.039
161	0.647	0.785	0.745	0.744	0.024	0.798	1.391	1.007	0.922	0.190
162	0.875	1.216	0.982	0.948	0.102	0.492	0.843	0.632	0.602	0.080
163	1.580	1.940	1.770	1.796	0.112	1.416	1.798	1.663	1.674	0.093
164	1.072	1.280	1.167	1.163	0.055	0.696	1.403	1.183	1.260	0.194
165	0.720	0.936	0.876	0.898	0.051	0.475	0.798	0.611	0.615	0.083
166	0.115	0.521	0.300	0.295	0.146	0.118	0.378	0.270	0.285	0.072
167	0.940	1.219	1.045	1.037	0.073	0.719	1.007	0.837	0.825	0.064
168	1.896	2.519	2.212	2.209	0.173	2.142	2.344	2.213	2.204	0.056
169	1.056	1.798	1.375	1.221	0.257	0.850	1.007	0.896	0.882	0.041
170	0.871	1.828	1.205	0.961	0.354	0.825	0.977	0.914	0.917	0.034
171	1.259	1.603	1.426	1.384	0.089	1.134	1.302	1.209	1.208	0.054
172	0.852	1.223	0.929	0.905	0.087	0.737	0.981	0.856	0.850	0.073
173	0.578	0.815	0.707	0.717	0.067	0.444	0.586	0.533	0.541	0.041
174	0.234	0.483	0.322	0.337	0.050	0.193	0.470	0.333	0.375	0.110
175	1.230	1.328	1.292	1.298	0.020	1.154	1.335	1.260	1.260	0.047
176	0.462	0.690	0.568	0.551	0.073	0.553	1.307	0.943	1.028	0.226
177	0.571	0.698	0.652	0.669	0.038	0.678	1.235	0.971	0.973	0.138
178	0.018	0.862	0.332	0.197	0.275	-0.255	0.856	0.228	0.329	0.296
179	0.719	0.849	0.800	0.805	0.033	0.624	1.044	0.811	0.734	0.154
180	0.775	1.084	0.886	0.876	0.064	0.720	0.948	0.834	0.839	0.052
181	0.737	1.353	0.951	0.909	0.178	1.318	1.516	1.425	1.422	0.040
182	0.913	1.029	0.972	0.971	0.023	0.767	0.968	0.860	0.863	0.049
183	0.755	1.075	0.971	0.995	0.087	0.813	0.916	0.854	0.844	0.028
184	0.675	0.765	0.716	0.712	0.022	0.695	0.876	0.800	0.791	0.046
185	1.633	1.749	1.681	1.673	0.033	1.143	1.611	1.504	1.505	0.099
186	0.796	0.970	0.884	0.881	0.057	0.591	0.904	0.732	0.680	0.090
187	0.737	0.869	0.787	0.778	0.034	0.775	0.836	0.806	0.805	0.015
188	0.983	1.004	0.996	0.999	0.006	0.783	1.023	0.962	0.960	0.048

Table G.1 continued from previous page

	Upside Pre-Breach					Upside Post-Breach				
189	0.877	0.988	0.949	0.961	0.032	0.673	0.970	0.842	0.838	0.091
190	0.434	0.683	0.551	0.544	0.045	0.694	0.932	0.818	0.791	0.085
191	0.838	0.997	0.920	0.902	0.050	0.905	1.223	1.126	1.141	0.092
192	0.225	0.670	0.594	0.629	0.096	0.633	0.974	0.869	0.886	0.079
193	1.703	1.862	1.762	1.758	0.038	1.633	1.698	1.660	1.661	0.019
194	0.702	1.099	0.815	0.797	0.099	0.733	0.852	0.793	0.802	0.035
195	0.938	1.082	1.022	1.041	0.043	0.929	1.077	1.010	1.021	0.038
196	1.139	1.343	1.219	1.195	0.056	1.185	1.275	1.223	1.215	0.027
197	1.192	1.275	1.241	1.250	0.023	1.158	1.392	1.257	1.244	0.058
198	1.263	1.307	1.282	1.280	0.011	1.233	1.296	1.267	1.267	0.017
199	0.546	0.800	0.659	0.629	0.063	0.748	0.919	0.813	0.807	0.041
200	0.184	0.538	0.294	0.243	0.107	0.356	0.518	0.446	0.457	0.044
201	0.219	0.402	0.359	0.370	0.044	0.348	0.438	0.400	0.404	0.025
202	-0.595	-0.068	-0.346	-0.338	0.178	-0.300	0.103	-0.099	-0.077	0.113
Mean	0.868	1.161	1.009	1.004	0.084	0.855	1.182	1.013	1.010	0.097

Appendix H
Descriptive Statistics: Downside Beta per Event

All descriptive statistics presented in the appendix are based on 60 daily one-year betas. For each event, across 60 daily betas, Min and Max demonstrate the lowest and greatest value, respectively. Mean (M), Median (Mdn), and Standard Deviation (SD) are based on each event's respective 60 daily values.

	Downside Pre-Breach					Downside Post-Breach				
Event	Min	Max	M	Mdn	SD	Min	Max	M	Mdn	SD
1	0.627	1.145	0.908	0.876	0.161	1.003	1.157	1.096	1.100	0.031
2	0.488	0.819	0.646	0.653	0.102	0.461	0.709	0.601	0.627	0.069
3	0.465	0.790	0.645	0.657	0.085	0.494	0.658	0.554	0.559	0.049
4	0.431	0.585	0.514	0.508	0.047	0.372	0.634	0.524	0.558	0.081
5	-0.362	0.243	-0.020	0.032	0.179	-0.078	0.717	0.289	0.280	0.268
6	1.278	2.141	1.995	2.045	0.176	1.672	2.204	1.897	1.708	0.229
7	0.967	1.135	1.069	1.070	0.042	0.981	1.153	1.069	1.065	0.050
8	1.203	1.516	1.403	1.452	0.108	1.276	1.516	1.380	1.368	0.061
9	1.022	1.225	1.168	1.178	0.052	1.148	1.320	1.217	1.204	0.038
10	0.864	1.150	1.003	1.008	0.070	0.944	1.104	1.037	1.034	0.034
11	1.071	1.512	1.209	1.161	0.123	1.044	1.383	1.166	1.110	0.100
12	1.065	1.378	1.223	1.199	0.102	1.308	1.385	1.345	1.335	0.023
13	1.018	1.321	1.148	1.135	0.080	1.059	1.244	1.133	1.122	0.052
14	0.642	0.781	0.700	0.698	0.025	0.655	0.863	0.755	0.763	0.060
15	1.256	1.425	1.366	1.367	0.038	1.262	1.330	1.292	1.289	0.019
16	1.536	1.623	1.561	1.553	0.023	1.477	1.808	1.583	1.573	0.077
17	1.397	1.530	1.458	1.459	0.039	1.493	2.112	1.711	1.749	0.157
18	1.035	1.553	1.209	1.177	0.145	1.509	5.363	2.980	2.988	1.196

Table H.1 continued from previous page

	Downside Pre-Breach					Downside Post-Breach				
19	0.047	0.893	0.538	0.650	0.224	0.209	2.151	1.009	1.029	0.494
20	0.822	1.180	0.983	0.916	0.118	1.052	1.091	1.065	1.062	0.011
21	0.724	0.857	0.808	0.835	0.043	0.777	0.917	0.857	0.874	0.042
22	0.922	1.022	0.951	0.955	0.015	0.931	0.974	0.952	0.952	0.009
23	0.561	0.868	0.722	0.704	0.059	0.640	0.728	0.688	0.692	0.022
24	2.105	2.274	2.191	2.210	0.055	2.220	2.291	2.253	2.252	0.020
25	1.119	1.162	1.142	1.146	0.013	1.064	1.121	1.101	1.105	0.016
26	1.299	1.392	1.340	1.336	0.025	1.340	1.425	1.379	1.377	0.021
27	1.309	2.270	1.745	1.634	0.341	1.245	3.127	2.678	2.858	0.467
28	1.161	1.359	1.284	1.287	0.048	1.051	1.245	1.143	1.127	0.059
29	0.907	1.110	1.040	1.058	0.046	1.137	1.228	1.191	1.198	0.022
30	0.545	0.740	0.621	0.599	0.062	0.550	0.653	0.617	0.618	0.025
31	0.427	0.700	0.578	0.553	0.086	0.563	0.908	0.752	0.681	0.124
32	0.952	1.045	0.992	0.986	0.027	1.010	1.109	1.052	1.040	0.032
33	1.038	1.261	1.204	1.217	0.048	1.055	1.268	1.164	1.164	0.057
34	0.989	1.113	1.032	1.026	0.029	1.064	1.201	1.144	1.159	0.042
35	0.757	0.981	0.883	0.875	0.052	0.969	1.079	1.028	1.050	0.039
36	1.116	1.231	1.163	1.150	0.038	0.993	1.186	1.081	1.078	0.055
37	1.615	1.740	1.670	1.646	0.045	1.598	1.706	1.650	1.661	0.031
38	1.354	1.439	1.392	1.386	0.023	1.397	1.582	1.483	1.488	0.049
39	1.399	1.496	1.454	1.448	0.025	1.297	2.167	1.587	1.545	0.270
40	0.885	0.945	0.914	0.914	0.012	0.734	0.923	0.816	0.818	0.051
41	1.417	1.631	1.517	1.514	0.048	1.370	1.959	1.599	1.515	0.226
42	0.859	1.042	0.982	1.008	0.051	0.863	1.033	0.933	0.942	0.039
43	0.726	0.978	0.850	0.838	0.085	0.941	1.066	1.012	1.006	0.035
44	0.751	1.121	0.921	0.877	0.136	0.930	1.060	0.999	1.004	0.047
45	0.865	0.927	0.886	0.883	0.016	0.880	0.918	0.896	0.896	0.010
46	0.784	0.814	0.796	0.795	0.010	0.757	0.800	0.778	0.779	0.011
47	1.191	1.259	1.228	1.228	0.013	1.186	1.256	1.214	1.217	0.017
48	1.015	1.066	1.043	1.045	0.014	0.965	1.014	0.980	0.980	0.010
49	1.067	1.299	1.206	1.228	0.069	0.938	1.071	0.987	0.972	0.038
50	1.297	1.363	1.331	1.335	0.021	1.308	1.351	1.338	1.339	0.007
51	1.085	1.111	1.099	1.098	0.007	1.050	1.116	1.080	1.073	0.017
52	1.316	1.501	1.432	1.437	0.050	0.810	1.424	1.270	1.382	0.178

Table H.1 continued from previous page

	Downside Pre-Breach					Downside Post-Breach				
53	1.354	1.441	1.397	1.398	0.024	1.350	1.582	1.474	1.490	0.045
54	0.742	0.823	0.777	0.779	0.019	0.742	1.048	0.848	0.781	0.101
55	0.767	0.883	0.826	0.823	0.037	0.816	1.218	0.977	0.911	0.143
56	1.044	1.109	1.075	1.072	0.020	0.993	1.116	1.057	1.063	0.042
57	1.996	2.432	2.204	2.197	0.131	1.488	2.223	1.788	1.800	0.238
58	0.412	1.206	0.722	0.675	0.227	0.281	2.023	1.450	1.530	0.433
59	0.852	1.325	1.061	1.116	0.143	1.115	1.303	1.209	1.213	0.051
60	1.645	2.051	1.897	1.891	0.115	1.894	2.064	1.966	1.973	0.042
61	1.233	1.602	1.392	1.345	0.114	1.324	1.751	1.487	1.443	0.114
62	1.175	1.354	1.284	1.301	0.055	1.178	1.384	1.297	1.297	0.054
63	1.097	1.228	1.166	1.184	0.047	0.950	1.105	1.059	1.075	0.046
64	0.880	1.044	0.979	0.995	0.047	0.856	1.063	0.970	1.009	0.077
65	0.227	0.402	0.306	0.300	0.038	0.276	0.399	0.337	0.325	0.035
66	1.033	1.175	1.120	1.132	0.042	0.814	1.081	0.954	0.985	0.079
67	1.323	1.431	1.394	1.399	0.032	1.133	1.375	1.290	1.306	0.056
68	0.993	1.172	1.072	1.071	0.046	0.728	1.074	0.857	0.837	0.082
69	1.292	1.448	1.389	1.389	0.037	1.456	1.576	1.511	1.508	0.035
70	0.913	1.289	1.128	1.208	0.130	0.814	0.910	0.862	0.861	0.031
71	1.006	1.416	1.234	1.247	0.114	1.300	1.541	1.459	1.474	0.061
72	0.867	0.990	0.936	0.930	0.022	0.874	1.037	0.985	0.989	0.026
73	0.434	0.578	0.524	0.525	0.036	0.349	0.657	0.481	0.474	0.094
74	0.819	0.941	0.898	0.908	0.029	0.731	1.002	0.818	0.791	0.074
75	0.672	0.840	0.755	0.758	0.040	0.759	0.988	0.912	0.929	0.065
76	0.603	0.699	0.657	0.660	0.030	0.556	0.660	0.617	0.623	0.022
77	0.191	0.335	0.286	0.298	0.041	0.305	0.574	0.433	0.407	0.091
78	1.048	1.248	1.167	1.195	0.068	1.101	1.158	1.126	1.125	0.016
79	0.712	0.836	0.766	0.761	0.025	0.721	1.020	0.869	0.824	0.093
80	0.474	0.562	0.517	0.520	0.020	0.413	0.651	0.514	0.500	0.078
81	0.836	0.960	0.892	0.888	0.026	0.979	1.146	1.073	1.076	0.057
82	1.409	1.552	1.476	1.482	0.038	1.435	1.650	1.520	1.496	0.069
83	0.824	1.020	0.889	0.885	0.033	0.966	1.085	1.012	0.999	0.035
84	1.590	1.833	1.700	1.696	0.053	1.684	1.833	1.751	1.760	0.035
85	0.857	1.644	1.332	1.439	0.249	1.621	1.840	1.735	1.726	0.056
86	0.973	1.393	1.231	1.270	0.135	0.781	1.058	0.910	0.952	0.092

Table H.1 continued from previous page

	Downside Pre-Breach					Downside Post-Breach				
87	0.506	0.689	0.593	0.585	0.040	0.506	0.596	0.560	0.561	0.018
88	0.884	1.047	0.968	0.967	0.044	1.042	1.189	1.120	1.133	0.044
89	1.577	2.850	2.335	2.409	0.329	1.587	2.724	2.086	2.100	0.410
90	1.114	1.737	1.250	1.228	0.133	1.189	1.455	1.336	1.330	0.086
91	0.972	1.079	1.033	1.033	0.027	0.697	1.066	0.859	0.865	0.092
92	1.189	1.515	1.372	1.365	0.080	0.793	1.184	0.951	1.043	0.119
93	1.258	1.607	1.375	1.311	0.107	1.326	1.589	1.414	1.382	0.077
94	1.110	1.165	1.137	1.139	0.014	0.996	1.176	1.083	1.071	0.054
95	0.846	0.889	0.870	0.870	0.012	0.779	0.907	0.828	0.827	0.024
96	0.274	0.573	0.445	0.487	0.095	0.368	0.533	0.461	0.477	0.042
97	1.614	1.979	1.797	1.766	0.091	1.271	1.511	1.421	1.444	0.064
98	0.997	1.201	1.140	1.149	0.046	1.091	1.323	1.186	1.176	0.060
99	1.821	2.791	2.168	2.103	0.243	1.474	2.045	1.778	1.832	0.184
100	1.232	1.410	1.347	1.360	0.053	1.228	1.376	1.299	1.282	0.046
101	0.713	0.832	0.768	0.749	0.039	0.594	0.752	0.652	0.639	0.038
102	0.920	1.146	1.068	1.098	0.075	0.760	0.874	0.813	0.806	0.031
103	0.597	0.710	0.667	0.677	0.034	0.629	0.691	0.663	0.662	0.013
104	1.754	2.272	2.039	2.030	0.099	1.643	1.991	1.760	1.754	0.068
105	0.772	1.426	1.056	1.065	0.147	0.500	0.905	0.719	0.751	0.130
106	0.719	0.850	0.804	0.810	0.034	0.696	0.895	0.812	0.833	0.058
107	1.193	1.325	1.284	1.301	0.039	1.157	1.338	1.269	1.288	0.051
108	0.662	1.198	1.012	1.030	0.121	0.587	1.004	0.787	0.791	0.092
109	0.645	0.757	0.724	0.740	0.033	0.747	1.344	1.140	1.269	0.220
110	2.163	2.559	2.371	2.372	0.095	1.832	2.085	1.967	1.983	0.077
111	1.391	1.557	1.472	1.470	0.027	1.358	1.551	1.458	1.454	0.052
112	1.347	1.462	1.389	1.389	0.019	1.254	1.572	1.411	1.394	0.092
113	0.661	0.948	0.758	0.769	0.065	0.939	1.140	1.057	1.043	0.046
114	-0.448	0.764	0.141	0.202	0.448	-0.769	-0.094	-0.385	-0.347	0.197
115	0.768	1.344	1.169	1.272	0.206	1.329	1.381	1.351	1.350	0.013
116	0.515	0.718	0.594	0.582	0.068	0.695	0.779	0.730	0.729	0.024
117	0.828	0.963	0.904	0.910	0.040	0.899	0.995	0.943	0.939	0.030
118	-0.028	0.336	0.096	0.052	0.094	0.160	0.888	0.455	0.394	0.232
119	1.379	1.768	1.492	1.440	0.130	1.051	1.471	1.223	1.143	0.153
120	1.056	1.402	1.260	1.287	0.094	0.348	1.113	0.638	0.611	0.203

Table H.1 continued from previous page

	Downside Pre-Breach					Downside Post-Breach				
121	1.137	1.558	1.275	1.216	0.138	0.929	1.108	0.971	0.961	0.029
122	0.999	1.317	1.191	1.269	0.121	1.092	1.172	1.138	1.140	0.021
123	1.534	1.726	1.617	1.598	0.061	1.478	1.625	1.559	1.576	0.043
124	1.302	1.614	1.458	1.502	0.079	1.452	1.536	1.503	1.497	0.019
125	0.998	1.097	1.027	1.016	0.027	0.883	1.033	0.984	0.977	0.030
126	1.260	1.357	1.314	1.314	0.030	1.302	1.494	1.386	1.380	0.050
127	0.899	1.065	0.955	0.939	0.042	0.891	1.071	0.983	0.991	0.057
128	0.454	0.775	0.584	0.563	0.078	0.846	1.052	0.929	0.925	0.048
129	0.982	1.107	1.057	1.066	0.031	1.093	1.208	1.154	1.153	0.030
130	0.535	0.637	0.579	0.578	0.026	0.515	0.647	0.554	0.545	0.032
131	1.171	1.417	1.312	1.312	0.057	1.381	1.469	1.431	1.437	0.022
132	0.741	0.952	0.837	0.808	0.073	0.828	0.917	0.868	0.868	0.025
133	0.499	0.749	0.650	0.652	0.050	0.569	0.775	0.706	0.710	0.046
134	0.500	0.702	0.612	0.621	0.055	0.531	0.706	0.612	0.573	0.062
135	1.663	1.823	1.770	1.792	0.051	1.709	2.057	1.873	1.813	0.132
136	1.090	1.120	1.107	1.109	0.008	1.034	1.090	1.070	1.075	0.016
137	0.465	0.607	0.528	0.522	0.040	0.332	0.620	0.470	0.468	0.082
138	1.136	1.260	1.193	1.194	0.034	1.099	1.516	1.242	1.212	0.106
139	1.102	1.197	1.152	1.166	0.027	0.775	1.148	0.930	0.940	0.077
140	1.012	1.060	1.036	1.037	0.013	0.922	1.058	1.026	1.036	0.028
141	0.524	1.254	0.772	0.572	0.286	1.326	1.550	1.419	1.383	0.084
142	0.660	1.038	0.832	0.792	0.135	0.861	1.127	1.006	1.007	0.058
143	0.580	0.676	0.634	0.633	0.025	0.375	0.708	0.610	0.634	0.078
144	1.977	2.153	2.048	2.021	0.050	1.931	2.217	2.056	2.043	0.064
145	0.923	1.046	0.996	1.013	0.038	0.758	0.933	0.869	0.869	0.047
146	0.831	0.966	0.887	0.875	0.040	0.922	1.100	0.999	1.007	0.053
147	0.889	1.268	1.014	0.983	0.105	0.791	1.094	0.924	0.937	0.063
148	0.786	1.027	0.911	0.902	0.072	0.583	0.755	0.649	0.654	0.039
149	0.242	1.641	1.000	1.255	0.462	1.353	1.833	1.611	1.583	0.140
150	1.416	1.645	1.515	1.527	0.041	1.420	1.553	1.497	1.498	0.028
151	1.541	1.848	1.709	1.711	0.075	1.723	1.916	1.810	1.791	0.057
152	1.104	1.431	1.232	1.211	0.103	1.163	1.348	1.262	1.246	0.049
153	0.692	0.886	0.801	0.842	0.071	0.752	1.144	0.907	0.917	0.091
154	1.023	1.301	1.109	1.103	0.054	1.141	1.406	1.313	1.307	0.045

Table H.1 continued from previous page

	Downside Pre-Breach					Downside Post-Breach				
155	0.975	1.231	1.110	1.114	0.070	1.088	1.877	1.489	1.400	0.247
156	0.584	0.759	0.687	0.695	0.045	0.524	2.042	1.311	1.805	0.636
157	0.970	1.334	1.102	1.060	0.120	0.931	1.239	1.085	1.103	0.080
158	0.838	1.075	0.964	0.971	0.080	0.943	1.429	1.226	1.233	0.084
159	0.655	1.099	0.793	0.758	0.117	0.638	1.124	0.837	0.824	0.119
160	0.682	1.121	0.889	0.788	0.158	0.962	1.356	1.136	1.143	0.077
161	1.010	1.270	1.192	1.230	0.087	1.225	1.439	1.370	1.370	0.051
162	0.965	1.074	1.032	1.043	0.033	0.565	0.806	0.685	0.688	0.073
163	1.250	2.340	1.753	1.443	0.399	2.296	2.475	2.394	2.393	0.049
164	1.006	1.410	1.221	1.196	0.102	0.861	1.233	1.047	1.038	0.092
165	1.091	1.393	1.220	1.196	0.082	0.864	1.207	1.119	1.168	0.100
166	0.184	0.284	0.230	0.219	0.031	0.228	0.805	0.688	0.735	0.160
167	1.151	1.493	1.343	1.365	0.081	1.096	1.167	1.136	1.135	0.018
168	0.938	2.021	1.333	1.208	0.261	0.805	0.955	0.885	0.889	0.045
169	1.020	1.968	1.352	1.178	0.343	1.017	1.094	1.066	1.070	0.021
170	0.775	1.390	0.957	0.936	0.177	0.828	0.916	0.879	0.883	0.021
171	1.298	2.227	1.505	1.395	0.274	1.262	1.357	1.315	1.320	0.028
172	-0.145	0.053	-0.003	0.005	0.033	0.002	0.132	0.064	0.075	0.029
173	1.050	1.127	1.086	1.085	0.018	1.082	1.211	1.128	1.106	0.045
174	-0.082	-0.016	-0.050	-0.053	0.019	-0.223	-0.040	-0.138	-0.161	0.050
175	1.160	1.316	1.216	1.190	0.056	1.069	1.219	1.145	1.157	0.038
176	0.560	0.668	0.615	0.616	0.025	0.679	1.172	1.000	1.047	0.127
177	0.580	0.764	0.658	0.648	0.061	0.711	1.197	1.003	0.989	0.111
178	1.242	1.678	1.468	1.481	0.130	0.504	1.291	0.840	0.794	0.209
179	1.037	1.170	1.127	1.125	0.025	1.116	1.204	1.157	1.158	0.022
180	0.736	0.890	0.820	0.818	0.050	0.570	0.748	0.657	0.643	0.045
181	0.079	0.633	0.265	0.156	0.179	0.735	1.622	1.091	1.064	0.245
182	1.279	1.477	1.373	1.360	0.055	1.258	1.333	1.298	1.298	0.019
183	0.588	1.158	0.695	0.659	0.137	0.505	0.626	0.559	0.554	0.034
184	0.740	0.871	0.780	0.781	0.025	0.759	0.863	0.800	0.798	0.029
185	1.395	1.489	1.450	1.449	0.024	1.430	2.074	1.671	1.635	0.168
186	0.976	1.069	1.028	1.031	0.024	0.837	1.004	0.920	0.923	0.043
187	0.610	0.735	0.666	0.657	0.037	0.580	0.645	0.614	0.612	0.013
188	0.885	0.927	0.909	0.908	0.012	0.898	1.401	1.126	1.150	0.194

Table H.1 continued from previous page

	Downside Pre-Breach					Downside Post-Breach				
189	0.749	0.899	0.834	0.848	0.042	0.529	0.788	0.702	0.733	0.083
190	1.156	1.241	1.181	1.177	0.019	1.224	1.337	1.291	1.297	0.034
191	0.725	0.788	0.750	0.743	0.017	0.744	1.212	1.059	1.093	0.139
192	0.377	0.545	0.492	0.515	0.045	0.397	0.568	0.469	0.463	0.043
193	1.411	1.534	1.499	1.493	0.021	1.457	1.491	1.475	1.474	0.008
194	0.877	0.995	0.919	0.908	0.037	0.848	0.954	0.901	0.906	0.030
195	0.707	0.928	0.797	0.758	0.079	0.923	1.064	0.984	0.974	0.047
196	1.034	1.261	1.132	1.060	0.093	1.289	1.551	1.458	1.495	0.086
197	1.298	1.551	1.392	1.376	0.078	1.335	1.576	1.460	1.460	0.071
198	1.322	1.452	1.357	1.353	0.035	1.389	1.442	1.422	1.423	0.013
199	0.470	0.855	0.707	0.704	0.087	0.602	0.734	0.680	0.680	0.027
200	0.248	0.554	0.445	0.482	0.096	0.333	0.796	0.538	0.520	0.142
201	0.426	0.501	0.470	0.474	0.022	0.294	0.429	0.357	0.360	0.039
202	1.091	1.666	1.348	1.318	0.178	0.901	1.182	1.017	1.025	0.073
Mean	0.932	1.207	1.066	1.062	0.078	0.951	1.246	1.097	1.099	0.084

Appendix I
Descriptive Statistics: Changes in Regular, Upside, and Downside Beta per Event

All changes in beta per event presented are based on 60 daily one-year betas. The differences between aggregated (i.e., mean) pre- and post-breach betas are shown in absolute (Abs) and percentage (%) terms. n.m. = not meaningful.

	Regular			Upside			Downside		
Event	Pre	Abs	%	Pre	Abs	%	Pre	Abs	%
1	0.835	0.163	19.47	0.962	-0.267	-27.74	0.908	0.189	20.78
2	0.770	0.073	9.50	0.634	-0.154	-24.35	0.646	-0.045	-7.00
3	1.071	-0.181	-16.88	0.969	-0.280	-28.88	0.645	-0.092	-14.24
4	0.844	-0.032	-3.80	0.555	-0.032	-5.73	0.514	0.010	1.94
5	1.042	0.317	30.38	1.767	0.100	5.68	-0.020	0.309	n.m.
6	1.720	-0.069	-4.02	0.915	0.278	30.42	1.995	-0.099	-4.94
7	1.031	0.055	5.32	1.025	0.100	9.80	1.069	0.000	-0.04
8	1.104	0.078	7.04	0.827	0.187	22.56	1.403	-0.023	-1.63
9	1.129	0.018	1.57	1.213	-0.135	-11.13	1.168	0.049	4.22
10	0.989	0.032	3.28	1.039	0.004	0.39	1.003	0.035	3.47
11	1.715	-0.513	-29.93	1.785	-1.002	-56.13	1.209	-0.044	-3.61
12	1.161	0.060	5.13	1.108	0.085	7.70	1.223	0.122	10.00
13	1.394	-0.156	-11.19	1.400	-0.324	-23.12	1.148	-0.015	-1.28
14	0.781	0.063	8.12	0.969	0.166	17.08	0.700	0.055	7.84
15	0.965	0.027	2.79	0.915	-0.050	-5.49	1.366	-0.074	-5.38
16	2.101	0.094	4.48	2.736	0.288	10.53	1.561	0.022	1.39
17	1.757	0.228	13.00	2.466	0.124	5.01	1.458	0.253	17.35

Table I.1 continued from previous page

	Regular			Upside			Downside		
18	1.814	1.262	69.57	2.588	1.926	74.39	1.209	1.772	146.56
19	-0.409	0.662	n.m.	-0.072	1.306	n.m.	0.538	0.471	87.49
20	0.827	0.130	15.78	0.822	0.156	18.97	0.983	0.082	8.33
21	0.897	0.057	6.40	0.807	-0.064	-7.94	0.808	0.049	6.11
22	1.086	0.043	3.95	1.071	0.083	7.76	0.951	0.000	0.04
23	0.731	-0.033	-4.45	0.565	-0.005	-0.93	0.722	-0.034	-4.68
24	1.784	-0.025	-1.42	1.885	0.043	2.30	2.191	0.062	2.84
25	1.180	0.036	3.01	1.308	0.097	7.41	1.142	-0.041	-3.56
26	1.086	-0.029	-2.68	0.979	0.037	3.80	1.340	0.039	2.94
27	1.103	-0.038	-3.41	-0.318	0.067	21.14	1.745	0.933	53.47
28	1.487	-0.312	-20.96	1.767	-0.528	-29.87	1.284	-0.141	-10.97
29	1.026	-0.008	-0.77	1.461	-0.201	-13.74	1.040	0.151	14.51
30	0.570	0.007	1.23	0.580	0.084	14.56	0.621	-0.004	-0.67
31	0.690	0.073	10.61	0.742	-0.131	-17.68	0.578	0.175	30.23
32	1.054	0.031	2.97	1.125	-0.084	-7.47	0.992	0.059	5.99
33	1.354	-0.030	-2.19	1.074	0.072	6.74	1.204	-0.040	-3.30
34	1.253	0.009	0.69	1.048	0.119	11.35	1.032	0.112	10.85
35	0.852	0.040	4.72	0.724	-0.004	-0.50	0.883	0.145	16.44
36	1.013	-0.056	-5.48	1.151	0.007	0.59	1.163	-0.082	-7.07
37	1.851	0.075	4.07	1.654	0.061	3.67	1.670	-0.019	-1.16
38	1.494	0.009	0.63	1.556	-0.093	-5.96	1.392	0.091	6.55
39	1.550	0.011	0.70	1.619	0.168	10.38	1.454	0.133	9.16
40	0.677	-0.040	-5.98	0.574	0.034	5.96	0.914	-0.098	-10.69
41	1.334	0.119	8.93	1.153	0.250	21.65	1.517	0.083	5.44
42	0.886	-0.030	-3.37	0.964	0.026	2.65	0.982	-0.049	-4.95
43	0.912	0.100	10.92	0.927	0.057	6.10	0.850	0.162	19.03
44	0.857	0.202	23.58	0.831	0.114	13.72	0.921	0.077	8.39
45	0.988	-0.005	-0.54	1.192	-0.043	-3.57	0.886	0.009	1.05
46	0.832	0.017	2.05	0.833	-0.030	-3.62	0.796	-0.018	-2.29
47	1.256	0.023	1.84	1.118	-0.019	-1.73	1.228	-0.014	-1.13
48	1.037	-0.004	-0.40	1.159	0.059	5.05	1.043	-0.063	-6.00
49	1.189	0.086	7.20	1.294	-0.083	-6.39	1.206	-0.219	-18.15
50	1.350	-0.013	-1.00	1.477	-0.038	-2.59	1.331	0.007	0.51
51	0.981	-0.024	-2.40	0.856	-0.019	-2.20	1.099	-0.018	-1.66

Table I.1 continued from previous page

	Regular			Upside			Downside		
52	1.317	-0.035	-2.65	1.519	-0.139	-9.18	1.432	-0.162	-11.33
53	1.488	-0.035	-2.36	1.852	-0.231	-12.49	1.397	0.077	5.49
54	0.645	0.030	4.68	0.600	0.031	5.24	0.777	0.071	9.17
55	0.787	0.134	17.00	0.733	0.079	10.75	0.826	0.151	18.28
56	1.081	-0.124	-11.50	1.058	-0.228	-21.57	1.075	-0.018	-1.66
57	2.068	-0.427	-20.63	2.223	-0.519	-23.34	2.204	-0.416	-18.89
58	0.822	-0.138	-16.76	1.000	-0.331	-33.09	0.722	0.727	100.72
59	1.215	-0.011	-0.90	1.166	0.017	1.43	1.061	0.149	14.03
60	2.241	-0.056	-2.48	1.802	-0.067	-3.72	1.897	0.069	3.63
61	1.535	-0.083	-5.38	1.678	-0.333	-19.85	1.392	0.095	6.84
62	1.221	0.016	1.29	1.372	0.308	22.41	1.284	0.013	1.02
63	0.939	-0.033	-3.46	0.897	-0.030	-3.35	1.166	-0.106	-9.12
64	1.094	-0.017	-1.56	1.108	0.061	5.55	0.979	-0.009	-0.92
65	0.832	-0.036	-4.35	0.935	-0.032	-3.44	0.306	0.031	10.01
66	1.104	-0.049	-4.47	1.157	-0.039	-3.38	1.120	-0.166	-14.82
67	1.401	-0.097	-6.91	1.216	-0.115	-9.42	1.394	-0.105	-7.51
68	0.763	0.176	23.02	-0.010	0.562	n.m.	1.072	-0.215	-20.06
69	1.136	-0.063	-5.54	1.451	0.190	13.07	1.389	0.122	8.77
70	1.028	-0.004	-0.43	1.178	0.224	19.05	1.128	-0.266	-23.55
71	0.830	0.176	21.26	0.744	0.379	50.92	1.234	0.225	18.27
72	0.860	-0.006	-0.70	0.663	-0.066	-9.89	0.936	0.049	5.28
73	0.915	0.144	15.76	1.032	0.258	24.96	0.524	-0.043	-8.18
74	0.819	-0.039	-4.74	1.109	-0.188	-16.92	0.898	-0.080	-8.96
75	0.852	0.135	15.79	0.979	0.210	21.42	0.755	0.157	20.73
76	0.759	0.088	11.65	0.822	0.366	44.50	0.657	-0.039	-5.96
77	0.777	-0.008	-1.00	1.007	-0.113	-11.27	0.286	0.148	51.71
78	1.229	-0.007	-0.61	1.071	0.238	22.18	1.167	-0.042	-3.57
79	1.029	-0.060	-5.79	1.060	-0.068	-6.42	0.766	0.103	13.51
80	0.562	0.069	12.34	0.360	0.086	23.76	0.517	-0.003	-0.54
81	1.079	0.086	7.96	1.206	0.130	10.75	0.892	0.181	20.33
82	1.124	0.041	3.64	0.641	0.014	2.15	1.476	0.044	3.00
83	0.919	0.001	0.08	0.827	0.069	8.29	0.889	0.123	13.85
84	1.330	0.177	13.32	1.081	0.077	7.08	1.700	0.052	3.04
85	1.255	0.209	16.65	-0.101	0.062	61.76	1.332	0.403	30.24

Table I.1 continued from previous page

	Regular			Upside			Downside		
86	0.618	-0.150	-24.29	0.692	-0.533	-77.00	1.231	-0.321	-26.07
87	0.859	-0.045	-5.24	0.937	-0.230	-24.51	0.593	-0.033	-5.52
88	1.138	0.026	2.33	1.237	0.013	1.06	0.968	0.152	15.71
89	1.122	-0.322	-28.73	0.771	-0.620	-80.43	2.335	-0.249	-10.66
90	1.054	0.088	8.37	1.411	0.114	8.11	1.250	0.086	6.89
91	1.052	-0.037	-3.47	0.798	-0.109	-13.63	1.033	-0.175	-16.91
92	0.943	-0.208	-22.07	0.537	-0.018	-3.43	1.372	-0.421	-30.67
93	1.460	-0.029	-2.00	0.969	0.015	1.52	1.375	0.040	2.87
94	1.148	-0.068	-5.89	1.051	0.141	13.43	1.137	-0.054	-4.72
95	0.981	0.032	3.25	1.113	0.104	9.33	0.870	-0.042	-4.78
96	0.645	-0.068	-10.62	0.688	0.145	21.07	0.445	0.015	3.43
97	1.335	-0.058	-4.31	1.888	-0.128	-6.81	1.797	-0.376	-20.91
98	0.933	0.134	14.35	0.615	-0.185	-30.06	1.140	0.046	4.00
99	2.251	-0.066	-2.91	2.266	-0.397	-17.52	2.168	-0.390	-17.98
100	1.193	-0.047	-3.92	1.442	-0.124	-8.56	1.347	-0.048	-3.55
101	0.502	0.140	27.78	0.079	0.057	71.51	0.768	-0.116	-15.09
102	0.770	0.050	6.48	0.634	-0.029	-4.52	1.068	-0.254	-23.83
103	0.655	-0.090	-13.81	0.647	-0.111	-17.16	0.667	-0.004	-0.55
104	1.404	-0.128	-9.10	-0.670	-0.332	-49.49	2.039	-0.278	-13.65
105	1.120	-0.349	-31.18	1.032	-0.314	-30.45	1.056	-0.337	-31.88
106	0.640	-0.025	-3.83	0.500	0.190	37.91	0.804	0.008	1.03
107	0.882	0.186	21.06	0.742	0.275	37.07	1.284	-0.016	-1.21
108	1.354	-0.209	-15.41	0.700	-0.252	-36.03	1.012	-0.225	-22.25
109	0.947	0.150	15.88	1.136	0.190	16.72	0.724	0.416	57.43
110	1.561	-0.170	-10.92	1.319	0.056	4.28	2.371	-0.403	-17.02
111	1.329	0.042	3.15	1.224	-0.006	-0.47	1.472	-0.014	-0.92
112	1.208	0.091	7.55	1.691	-0.167	-9.88	1.389	0.022	1.59
113	0.973	0.114	11.70	1.137	0.174	15.33	0.758	0.300	39.57
114	0.946	-0.414	-43.80	0.308	-0.344	n.m.	0.141	-0.526	n.m.
115	1.106	0.040	3.60	1.324	-0.134	-10.16	1.169	0.183	15.63
116	0.526	0.092	17.53	0.563	0.008	1.40	0.594	0.136	22.90
117	0.815	0.006	0.77	0.491	0.001	0.29	0.904	0.039	4.30
118	0.720	0.007	1.03	0.965	-0.353	-36.55	0.096	0.359	374.65
119	1.139	-0.148	-12.95	0.855	-0.192	-22.39	1.492	-0.269	-18.04

Table I.1 continued from previous page

	Regular			Upside			Downside		
120	1.181	-0.335	-28.33	1.376	-0.235	-17.07	1.260	-0.622	-49.38
121	1.362	-0.302	-22.17	1.577	-0.404	-25.66	1.275	-0.304	-23.82
122	1.144	-0.075	-6.58	1.147	-0.148	-12.88	1.191	-0.053	-4.46
123	1.394	0.047	3.35	1.211	0.336	27.71	1.617	-0.057	-3.55
124	1.113	0.050	4.47	0.908	0.086	9.44	1.458	0.045	3.10
125	0.964	0.004	0.45	0.962	-0.062	-6.43	1.027	-0.042	-4.13
126	1.093	-0.036	-3.27	0.842	0.087	10.35	1.314	0.072	5.51
127	0.975	0.002	0.21	0.810	0.108	13.39	0.955	0.028	2.95
128	0.844	0.055	6.55	0.946	-0.451	-47.71	0.584	0.344	58.93
129	0.978	0.029	2.93	1.029	-0.064	-6.21	1.057	0.097	9.20
130	0.721	0.000	0.01	0.688	-0.021	-3.10	0.579	-0.026	-4.42
131	1.045	0.138	13.25	1.183	0.230	19.41	1.312	0.118	9.02
132	1.182	0.141	11.93	1.535	0.198	12.91	0.837	0.031	3.76
133	0.822	0.011	1.34	0.268	0.196	73.07	0.650	0.056	8.64
134	0.672	0.150	22.31	0.741	0.193	26.09	0.612	0.001	0.13
135	1.458	0.176	12.08	1.384	0.053	3.86	1.770	0.103	5.82
136	1.033	-0.010	-1.01	1.064	-0.003	-0.25	1.107	-0.037	-3.33
137	0.643	0.040	6.16	0.806	0.037	4.55	0.528	-0.057	-10.88
138	1.146	0.081	7.08	1.473	-0.008	-0.56	1.193	0.049	4.10
139	0.887	0.012	1.36	0.819	0.091	11.11	1.152	-0.222	-19.30
140	0.943	-0.024	-2.50	1.022	-0.051	-5.01	1.036	-0.010	-0.93
141	0.935	0.324	34.66	0.335	0.101	30.18	0.772	0.647	83.84
142	0.890	-0.071	-7.97	0.957	-0.397	-41.46	0.832	0.174	20.88
143	0.601	0.008	1.26	0.479	0.053	11.10	0.634	-0.024	-3.77
144	1.652	-0.083	-5.01	1.007	-0.049	-4.83	2.048	0.008	0.37
145	0.952	0.020	2.08	1.018	0.065	6.35	0.996	-0.127	-12.78
146	0.885	0.018	2.01	0.857	-0.106	-12.41	0.887	0.112	12.58
147	1.239	0.050	4.01	1.911	0.258	13.47	1.014	-0.090	-8.88
148	0.873	-0.182	-20.81	0.890	-0.278	-31.20	0.911	-0.262	-28.74
149	0.902	0.565	62.68	-0.567	0.659	n.m.	1.000	0.611	61.06
150	1.465	0.102	6.98	1.455	0.116	7.95	1.515	-0.019	-1.23
151	1.322	-0.154	-11.66	1.659	-0.431	-25.97	1.709	0.101	5.91
152	1.174	-0.131	-11.15	1.172	-0.254	-21.64	1.232	0.029	2.39
153	0.551	0.102	18.46	0.690	0.042	6.08	0.801	0.106	13.29

Table I.1 continued from previous page

	Regular			Upside			Downside		
154	0.950	0.108	11.33	1.032	-0.046	-4.43	1.109	0.204	18.44
155	1.300	0.181	13.91	1.283	0.283	22.02	1.110	0.379	34.13
156	0.429	0.955	222.48	0.187	0.050	26.99	0.687	0.624	90.80
157	1.397	0.065	4.68	1.068	0.353	33.02	1.102	-0.017	-1.55
158	1.274	-0.027	-2.15	1.212	0.109	8.96	0.964	0.262	27.19
159	1.114	0.081	7.24	1.214	-0.003	-0.26	0.793	0.044	5.60
160	1.099	0.003	0.26	1.024	0.111	10.88	0.889	0.247	27.73
161	1.085	0.187	17.28	0.745	0.262	35.19	1.192	0.179	14.98
162	1.003	-0.189	-18.85	0.982	-0.350	-35.66	1.032	-0.347	-33.65
163	1.579	0.279	17.63	1.770	-0.106	-6.01	1.753	0.640	36.52
164	1.274	-0.050	-3.96	1.167	0.016	1.33	1.221	-0.174	-14.27
165	0.972	-0.050	-5.17	0.876	-0.265	-30.26	1.220	-0.101	-8.27
166	0.248	0.212	85.61	0.300	-0.029	-9.75	0.230	0.458	198.62
167	1.192	-0.134	-11.25	1.045	-0.208	-19.87	1.343	-0.207	-15.44
168	1.440	-0.172	-11.93	2.212	0.002	0.09	1.333	-0.448	-33.63
169	1.431	-0.329	-23.02	1.375	-0.479	-34.86	1.352	-0.286	-21.17
170	1.157	-0.090	-7.78	1.205	-0.291	-24.15	0.957	-0.078	-8.11
171	1.360	-0.193	-14.16	1.426	-0.217	-15.23	1.505	-0.189	-12.59
172	0.808	-0.005	-0.63	0.929	-0.073	-7.85	-0.003	0.067	n.m.
173	1.030	-0.116	-11.29	0.707	-0.174	-24.60	1.086	0.042	3.83
174	0.350	0.037	10.70	0.322	0.011	3.44	-0.050	-0.089	-179.00
175	1.320	-0.040	-3.02	1.292	-0.031	-2.44	1.216	-0.071	-5.83
176	0.872	0.291	33.34	0.568	0.375	66.03	0.615	0.385	62.60
177	0.694	0.202	29.14	0.652	0.319	48.88	0.658	0.344	52.32
178	1.442	-0.408	-28.30	0.332	-0.104	-31.22	1.468	-0.628	-42.76
179	0.921	0.043	4.72	0.800	0.010	1.29	1.127	0.030	2.65
180	0.873	-0.044	-5.09	0.886	-0.053	-5.94	0.820	-0.164	-19.97
181	0.837	0.506	60.45	0.951	0.475	49.94	0.265	0.826	311.31
182	1.029	-0.004	-0.42	0.972	-0.112	-11.50	1.373	-0.075	-5.46
183	0.718	-0.034	-4.76	0.971	-0.118	-12.10	0.695	-0.135	-19.50
184	0.830	-0.033	-3.94	0.716	0.084	11.76	0.780	0.020	2.62
185	1.610	0.051	3.20	1.681	-0.177	-10.56	1.450	0.221	15.26
186	0.817	0.088	10.75	0.884	-0.152	-17.23	1.028	-0.108	-10.47
187	0.779	-0.040	-5.17	0.787	0.019	2.36	0.666	-0.052	-7.77

Table I.1 continued from previous page

	Regular			Upside			Downside		
188	1.067	0.056	5.24	0.996	-0.034	-3.45	0.909	0.218	23.96
189	0.883	-0.055	-6.19	0.949	-0.107	-11.28	0.834	-0.131	-15.73
190	0.883	0.126	14.24	0.551	0.267	48.51	1.181	0.110	9.35
191	0.887	0.150	16.92	0.920	0.206	22.37	0.750	0.309	41.14
192	0.819	0.139	17.00	0.594	0.275	46.28	0.492	-0.023	-4.59
193	1.922	0.107	5.58	1.762	-0.102	-5.80	1.499	-0.024	-1.61
194	0.821	-0.054	-6.54	0.815	-0.022	-2.68	0.919	-0.018	-1.96
195	0.947	0.067	7.07	1.022	-0.012	-1.19	0.797	0.187	23.50
196	1.121	0.081	7.26	1.219	0.004	0.34	1.132	0.326	28.78
197	1.213	0.064	5.31	1.241	0.016	1.30	1.392	0.068	4.90
198	1.364	-0.007	-0.51	1.282	-0.015	-1.14	1.357	0.065	4.76
199	0.467	0.013	2.80	0.659	0.154	23.45	0.707	-0.026	-3.72
200	0.259	0.192	73.98	0.294	0.152	51.72	0.445	0.093	20.92
201	0.300	0.029	9.70	0.359	0.041	11.32	0.470	-0.113	-24.06
202	0.501	0.129	25.69	-0.346	0.247	71.31	1.348	-0.331	-24.53
Mean	1.055	0.022	2.07	1.009	0.004	0.38	1.066	0.031	2.92

Appendix J
Overview Matched CDS Control Portfolios

Table J.1: Overview Rating- and Industry-Matched CDS Control Portfolios

Event	Company	Index	Industry	No. comps CDS
7	TJ stores (TJX)	CDX NA IG	Specialty Retail	18
8	Brunswick Corp.	CDX NA IG	Leisure Products	2
12	Hartford Life Insurance	CDX NA IG	Insurance	69
17	Citibank	CDX NA IG	Banks	198
18	Wells Fargo	CDX NA IG	Banks	208
25	Comcast	CDX NA IG	Media	58
26	Aetna	CDX NA IG	Health Care Providers and Services	25
28	Charles Schwab	CDX NA IG	Capital Markets	39
30	AT&T	CDX NA IG	Diversified Telecommunication Services	60
31	Anthem Blue Cross, WellPoint	CDX NA IG	Health Care Providers and Services	24
32	Cisco Live 2010	CDX NA IG	Communications Equipment	8
37	Hartford Life Insurance Company	CDX NA IG	Insurance	76
39	Bank of America	CDX NA IG	Banks	213
40	Lockheed Martin	CDX NA IG	Aerospace and Defense	19
41	Citibank	CDX NA IG	Banks	212
42	Capital Grille	CDX NA IG	Hotels, Restaurants and Leisure	27
44	Hewlett-Packard Enterprise Services	CDX NA IG	Technology Hardware, Storage and Peripherals	11

Table J.1 continued from previous page

Event	Company	Index	Industry	No. comps CDS
46	Intel	CDX NA IG	Semiconductors and Semiconductor Equipment	12
47	DHI Mortgage Company	CDX NA non-IG	Household Durables	27
50	Ford-Motor Websites	CDX NA IG	Automobiles	20
51	Comcast	CDX NA IG	Media	50
60	Advanced Micro Devices, Nvidia	CDX NA non-IG	Semiconductors and Semiconductor Equipment	11
61	The New York Times	CDX NA non-IG	Media	48
64	Microsoft	CDX NA IG	Software	6
66	American Express	CDX NA IG	Consumer Finance	18
67	JPMorgan Chase	CDX NA IG	Banks	216
69	Apple	CDX NA IG	Technology Hardware, Storage and Peripherals	23
72	Northrop Grumman	CDX NA IG	Aerospace and Defense	17
77	Crown Castle International Corp	CDX NA non-IG	Equity Real Estate Investment Trusts	44
78	JPMorgan Chase	CDX NA IG	Banks	225
80	Target Corp	CDX NA IG	Multiline Retail	17
81	American Express	CDX NA IG	Consumer Finance	18
82	Boston Scientific	CDX NA IG	Health Care Equipment and Supplies	14
86	Apple	CDX NA IG	Technology Hardware, Storage and Peripherals	23
88	Capital One	CDX NA IG	Consumer Finance	20
94	Boeing	CDX NA IG	Aerospace and Defense	22
95	Lockheed Martin	CDX NA IG	Aerospace and Defense	20
96	Dominion Resources	CDX NA IG	Multi-Utilities	22
97	Supervalue	CDX NA non-IG	Food and Staples Retailing	22
98	Community Health Systems	CDX NA non-IG	Health Care Providers and Services	28
100	JPMorgan Chase	CDX NA IG	Banks	234
101	Apple	CDX NA IG	Technology Hardware, Storage and Peripherals	23
102	The Home Depot	CDX NA IG	Specialty Retail	19

Table J.1 continued from previous page

Event	Company	Index	Industry	No. comps CDS
103	AT&T	CDX NA IG	Diversified Telecommunication Services	63
104	Sears HoldCo/ K-Mart	CDX NA non-IG	Multiline Retail	16
105	Staples	CDX NA IG	Specialty Retail	20
109	Microsoft xBox	CDX NA IG	Software	8
110	United Airlines	CDX NA non-IG	Airlines	12
111	Morgan Stanley	CDX NA IG	Capital Markets	40
113	Anthem	CDX NA IG	Health Care Providers and Services	26
115	Microsoft/Xbox One	CDX NA IG	Software	8
116	AT&T	CDX NA IG	Diversified Telecommunication Services	64
119	United Airlines	CDX NA non-IG	Airlines	13
125	Comcast	CDX NA IG	Media	51
126	Starwood Hotels	CDX NA IG	Hotels, Restaurants and Leisure	35
127	Juniper Networks	CDX NA IG	Communications Equipment	6
135	Charles Schwab	CDX NA IG	Capital Markets	42
136	ADP	CDX NA IG	IT Services	13
146	Quest Diagnostics	CDX NA IG	Health Care Providers and Services	25
150	Capital One	CDX NA IG	Consumer Finance	22
156	Rite Aid	CDX NA IG	Food and Staples Retailing	28
160	Anthem	CDX NA IG	Health Care Providers and Services	25
166	Coca-Cola	CDX NA IG	Beverages	21
167	Marriott International	CDX NA IG	Hotels, Restaurants and Leisure	38
169	Delta Air Lines	CDX NA IG	Airlines	16
171	SunTrust Banks	CDX NA IG	Banks	248
180	Nordstrom	CDX NA IG	Multiline Retail	15
183	ABB	iTraxx Europe IG	Electrical Equipment	7
186	adidas	iTraxx Europe IG	Textiles, Apparel and Luxury Goods	9
188	Mitsubishi	iTraxx Japan IG	Trading Companies and Distributors	22

Table J.1 continued from previous page

Event	Company	Index	Industry	No. comps CDS
189	American Honda Motor	iTraxx Japan IG	Automobiles	19
191	Epson America	iTraxx Japan IG	Technology Hardware, Storage and Peripherals	11
193	Aviva	iTraxx Europe IG	Insurance	78
194	LexisNexis	iTraxx Europe IG	Professional Services	3
198	Iberdola USA, Central Maine Power	iTraxx Europe IG	Electric Utilities	48

Note: Index refers to the CDS index, where CDX NA IG is the Markit CDX North American Investment Grade Index, CDX NA non-IG is the Markit CDX North American High Yield Index, iTraxx Europe IG is the iTraxx Europe Main Investment Grade Index, and iTraxx Japan IG is the iTraxx Asia Japan Investment Grade Index. Industry is the *S&P Capital IQ* Primary Industry in which the breached firm operates. No. comps CDS is the number of competitors' CDS contracts averaged to yield daily industry-specific changes in CDS premia.

Appendix K
CDS Competitor Portfolios

Event	Date (Adj.)	S&P CIQ CDS contracts							
7	17/01/2007	IQT46203137	IQT539599493	IQT46193836	IQT46195359	IQT46195869	IQT79635437	IQT46210519	IQT46201339
		IQT79636815	IQT46208360	IQT46209775	IQT46209672	IQT49751066	IQT46216933	IQT46218917	IQT46204804
		IQT46205518	IQT46221292						
8	16/02/2007	IQT46898995	IQT46210169						
12	12/09/2007	IQT46193721	IQT46198775	IQT579299842	IQT46193556	IQT46193586	IQT79639183	IQT46194263	IQT46194233
		IQT46193185	IQT46193175	IQT46193990	IQT46194573	IQT46224846	IQT46224866	IQT46194032	IQT46203802
		IQT106833211	IQT46195131	IQT46195161	IQT46195266	IQT46195246	IQT46198222	IQT46193330	IQT46199166
		IQT46203234	IQT46302616	IQT46204682	IQT46225319	IQT46225299	IQT79639832	IQT46209211	IQT46209241
		IQT88648731	IQT88648721	IQT46209617	IQT46209786	IQT46211181	IQT46210265	IQT46210275	IQT46210495
		IQT46225755	IQT46225775	IQT79639304	IQT79639314	IQT46213913	IQT46213768	IQT46213738	IQT46875110
		IQT46215264	IQT46215244	IQT46215520	IQT46216893	IQT46216873	IQT46217123	IQT46226090	IQT46226070
		IQT46217623	IQT49751106	IQT46219208	IQT46219188	IQT83051483	IQT46194102	IQT46219178	IQT51023605
		IQT51023600	IQT46222488	IQT46224381	IQT46224622	IQT46224642			
17	19/06/2008	IQT323680451	IQT46225354	IQT313313245	IQT46261982	IQT46193940	IQT46262002	IQT46261992	IQT51023258
		IQT60387142	IQT46194523	IQT46194543	IQT79640200	IQT46211367	IQT46211397	IQT46208954	IQT46208924
		IQT51023497	IQT51023496	IQT46195910	IQT46195940	IQT51023287	IQT46196922	IQT60387202	IQT79639264
		IQT46302585	IQT79639473	IQT52023890	IQT52023880	IQT79634427	IQT79634417	IQT51023522	IQT51023512
		IQT46226030	IQT46226010	IQT46636340	IQT46195491	IQT79639852	IQT46196077	IQT79636605	IQT46224986
		IQT46224976	IQT46205397	IQT46205357	IQT79639422	IQT46898760	IQT46195560	IQT46195580	IQT46197653
		IQT46197623	IQT79639344	IQT79639334	IQT46225006	IQT46225026	IQT79636475	IQT46197792	IQT46199344
		IQT263205692	IQT79634317	IQT79634327	IQT46531429	IQT46198882	IQT46225103	IQT46225083	IQT46198242
		IQT46198272	IQT46225888	IQT46225908	IQT46224740	IQT46224760	IQT79634047	IQT46198666	IQT46200394
		IQT46200364	IQT46200504	IQT46200474	IQT79639213	IQT46200725	IQT51023323	IQT79634307	IQT79634296
		IQT46201319	IQT46201289	IQT46201716	IQT46202628	IQT46202896	IQT46204477	IQT46204507	IQT79634397
		IQT79634077	IQT79634087	IQT46225394	IQT46225374	IQT46206772	IQT46206790	IQT49750965	IQT46206992
		IQT106833134	IQT106833144	IQT46207440	IQT46207410	IQT46224815	IQT46224805	IQT62270069	IQT79640104
		IQT46196009	IQT46205219	IQT46216976	IQT79636635	IQT46207892	IQT46207872	IQT46208393	IQT46198904
		IQT46302646	IQT46302656	IQT51023395	IQT51023405	IQT46208242	IQT46208862	IQT46208882	IQT46209464
		IQT46209484	IQT46211551	IQT60388494	IQT46210205	IQT46210195	IQT46195600	IQT46195620	IQT46225677
		IQT46225657	IQT106833271	IQT106833261	IQT79634901	IQT79634891	IQT46225735	IQT46225715	IQT46211878
		IQT46211858	IQT46224699	IQT46224719	IQT46875219	IQT46875229	IQT46196336	IQT46196296	IQT46213563
		IQT46213533	IQT46302636	IQT46207195	IQT46215397	IQT46217039	IQT313313741	IQT79640014	IQT46206679
		IQT46206649	IQT46193103	IQT46193083	IQT46217375	IQT49751126	IQT79635832	IQT263207246	IQT51649278
		IQT46262247	IQT46262257	IQT46226152	IQT46226132	IQT46219301	IQT79639892	IQT46226224	IQT46226204
		IQT254955233	IQT46217425	IQT46219703	IQT46219673	IQT79636257	IQT46219740	IQT49751166	IQT49751156
		IQT49751186	IQT49896508	IQT106490915	IQT46206453	IQT46206423	IQT51532171	IQT51611338	IQT51649277
		IQT79634506	IQT46222559	IQT46222579	IQT46223228	IQT46223646	IQT46223666	IQT46223350	IQT46223370
		IQT79635962	IQT46224202	IQT51532178	IQT51532188	IQT79636044	IQT79636034		
18	12/08/2008	IQT46193455	IQT46261982	IQT46193940	IQT46262002	IQT46261992	IQT51023258	IQT60387142	IQT46194523
		IQT46194543	IQT79640200	IQT46211397	IQT46211367	IQT46208954	IQT46208924	IQT51023497	IQT51023496
		IQT46195910	IQT46195940	IQT51023287	IQT79639264	IQT46196922	IQT60387202	IQT79639473	IQT46302585
		IQT52023890	IQT52023880	IQT79634417	IQT79634427	IQT51023490	IQT51991422	IQT51023522	IQT51023512
		IQT46226010	IQT46226030	IQT46636340	IQT46195491	IQT79639852	IQT46196077	IQT79636605	IQT46224976
		IQT46224986	IQT46205397	IQT46205357	IQT46898760	IQT79639422	IQT46195580	IQT46195560	IQT46197653
		IQT46197623	IQT79639344	IQT79639334	IQT46225026	IQT46225006	IQT79636475	IQT46197792	IQT46199344
		IQT263205692	IQT79634327	IQT79634317	IQT46531429	IQT46198882	IQT46197694	IQT46197714	IQT46225083
		IQT46198272	IQT46225908	IQT46225888	IQT46224760	IQT46224740	IQT79634047	IQT46198666	IQT46200364
		IQT46200394	IQT46200474	IQT46200504	IQT79639213	IQT46200725	IQT51023323	IQT79634296	IQT79634307

Table K.1 continued from previous page

Event	Date (Adj.)	S&P CIQ CDS contracts							
		IQT46201289	IQT46201319	IQT79640300	IQT51023343	IQT46201716	IQT46202628	IQT51023359	IQT46202896
		IQT46211987	IQT60387122	IQT46204507	IQT46204477	IQT79634397	IQT79634077	IQT79634087	IQT46225374
		IQT46225394	IQT46206772	IQT46206790	IQT49750965	IQT46206992	IQT106833144	IQT106833134	IQT46207410
		IQT46207440	IQT46224805	IQT46224815	IQT62270069	IQT79640104	IQT46196009	IQT46205219	IQT46216976
		IQT79636635	IQT46207892	IQT46207872	IQT46208393	IQT46198904	IQT46302646	IQT46302656	IQT51023395
		IQT51023405	IQT46208242	IQT49751006	IQT46208882	IQT46208862	IQT46209484	IQT46209464	IQT60388494
		IQT46211551	IQT46210195	IQT46210205	IQT46210109	IQT46195600	IQT46195620	IQT46225677	IQT46225657
		IQT106833261	IQT106833271	IQT79634891	IQT79634901	IQT46225715	IQT46225735	IQT46211858	IQT46211878
		IQT46224719	IQT46224699	IQT46875229	IQT46875219	IQT46196336	IQT46196296	IQT46213563	IQT46213533
		IQT46207195	IQT46302636	IQT46215397	IQT46217059	IQT46217039	IQT79640014	IQT313313741	IQT46216365
		IQT46217158	IQT46206649	IQT46206679	IQT46193083	IQT46193103	IQT46217375	IQT49751126	IQT79635832
		IQT263207246	IQT51649278	IQT46262247	IQT46262257	IQT46226132	IQT46226152	IQT46219301	IQT79639892
		IQT46226204	IQT46226224	IQT254955233	IQT46217425	IQT46219703	IQT46219673	IQT46219740	IQT79636257
		IQT49751166	IQT49751156	IQT49751176	IQT49751186	IQT51023303	IQT46199472	IQT46212072	IQT49896508
		IQT106490915	IQT46206423	IQT46206453	IQT51532171	IQT51611338	IQT79634506	IQT51649277	IQT46222559
		IQT46222579	IQT46223228	IQT79635962	IQT46224202	IQT51532178	IQT51532188	IQT79636034	IQT79636044
25	16/03/2009	IQT46217355	IQT46199947	IQT81859700	IQT46200286	IQT46204180	IQT46222762	IQT79634872	IQT46196520
		IQT46196274	IQT79639355	IQT46200009	IQT79639153	IQT46199619	IQT79636848	IQT46200019	IQT46201472
		IQT46200923	IQT79640084	IQT46204005	IQT46220647	IQT46205259	IQT46224512	IQT46206260	IQT46198430
		IQT46470865	IQT79636405	IQT46210288	IQT79639234	IQT46213799	IQT46215275	IQT46215190	IQT46215375
		IQT79636766	IQT46215155	IQT46217917	IQT46531439	IQT46217385	IQT81859720	IQT46197353	IQT46206585
		IQT313312430	IQT46220562	IQT46219118	IQT46207217	IQT46211253	IQT46213465	IQT46200688	IQT46216312
		IQT79636247	IQT46221440	IQT79636017	IQT79634585	IQT46222529	IQT46206812	IQT46222839	IQT46198346
		IQT46207989	IQT46224107						
26	28/05/2009	IQT46193123	IQT46223889	IQT46197768	IQT46198775	IQT46200195	IQT46200059	IQT46200090	IQT46201533
		IQT79636625	IQT46205770	IQT46225248	IQT79635660	IQT46205914	IQT46206320	IQT79635752	IQT46209261
		IQT46205508	IQT46210360	IQT46210687	IQT46213573	IQT79635782	IQT46200788	IQT46220857	IQT46222425
		IQT46222242							
28	09/04/2010	IQT313305671	IQT46470877	IQT46217561	IQT60388107	IQT46262077	IQT46875079	IQT106833201	IQT46195642
		IQT79636565	IQT46199841	IQT46199861	IQT46200317	IQT46200432	IQT46200412	IQT46875109	IQT46205104
		IQT46209742	IQT102286632	IQT84609938	IQT46202260	IQT46202230	IQT46210462	IQT46262097	IQT46262087
		IQT46225948	IQT46225968	IQT46212786	IQT62270106	IQT46223596	IQT46223626	IQT46210657	IQT46220667
		IQT46197292	IQT46204987	IQT46204957	IQT46222188	IQT46222168	IQT46223289	IQT46223159	
30	09/06/2010	IQT46194493	IQT323679950	IQT46220237	IQT46226245	IQT644701487	IQT263207493	IQT46197228	IQT46200009
		IQT217703455	IQT46200019	IQT46200923	IQT79636815	IQT46210288	IQT46196015	IQT46196575	IQT46200124
		IQT46199947	IQT46201372	IQT46898887	IQT46875103	IQT46196107	IQT46200286	IQT46213991	IQT106833231
		IQT46207093	IQT46208685	IQT46208665	IQT46209833	IQT46213157	IQT46213841	IQT109027089	IQT79634236
		IQT46203750	IQT46214136	IQT60387242	IQT46215566	IQT46215546	IQT79635812	IQT46218241	IQT79639812
		IQT46226266	IQT79635882	IQT49751096	IQT46220521	IQT46226296	IQT46220769	IQT46220923	IQT46220614
		IQT46220634	IQT46220961	IQT46220541	IQT46220309	IQT79639406	IQT46223278	IQT79636665	IQT79636675
		IQT79640270	IQT79636685	IQT46223743	IQT46223793				
31	23/06/2010	IQT46193699	IQT46193123	IQT46197768	IQT46198775	IQT46200195	IQT46200059	IQT46200090	IQT46201533
		IQT79636625	IQT46205770	IQT46225248	IQT79635660	IQT46205914	IQT46206320	IQT46209261	IQT46205508
		IQT46210360	IQT46210687	IQT46213573	IQT79635782	IQT46200788	IQT46220857	IQT46222425	IQT46222242
32	09/07/2010	IQT46899379	IQT263213059	IQT323680401	IQT46194211	IQT46211478	IQT46212776	IQT46194201	IQT46209576

Table K.1 continued from previous page

Event	Date (Adj.)	S&P CIQ CDS contracts							
37	06/04/2011	IQT46193721	IQT46198775	IQT579299842	IQT46193586	IQT46193556	IQT79639193	IQT79639183	IQT46194263
		IQT46194233	IQT46193990	IQT46194573	IQT46224846	IQT46224866	IQT46193815	IQT46203802	IQT106833211
		IQT46195131	IQT46195161	IQT46195266	IQT46195246	IQT46195318	IQT46198177	IQT46198222	IQT46193330
		IQT46199166	IQT46215898	IQT46203234	IQT46204682	IQT46225319	IQT46225299	IQT79639832	IQT46209211
		IQT46209241	IQT88648731	IQT88648721	IQT46209617	IQT46209786	IQT46211181	IQT46210265	IQT46210275
		IQT46210495	IQT46302708	IQT46225775	IQT46225755	IQT79639314	IQT79639304	IQT46213913	IQT46213768
		IQT46213738	IQT46875110	IQT46215244	IQT46215264	IQT46215520	IQT46216580	IQT46216873	IQT46216893
		IQT46217123	IQT46226090	IQT46226070	IQT46217623	IQT49751106	IQT46302727	IQT46219208	IQT46219188
		IQT54590857	IQT46194102	IQT46210567	IQT46214580	IQT46219178	IQT46210831	IQT51023605	IQT51023600
		IQT46222488	IQT46224381	IQT46224642	IQT46224622				
39	25/05/2011	IQT323680451	IQT46207150	IQT60388494	IQT102286632	IQT46214601	IQT46195905	IQT46193455	IQT46193940
		IQT46261982	IQT46262002	IQT46261992	IQT51649271	IQT51649261	IQT46193135	IQT46194543	IQT46194523
		IQT46211397	IQT46211367	IQT46208954	IQT46208924	IQT51023496	IQT51023497	IQT46195910	IQT46195940
		IQT51023287	IQT137102612	IQT79639264	IQT46196922	IQT60387202	IQT46302585	IQT79639473	IQT52023890
		IQT52023880	IQT79634417	IQT79634427	IQT51023490	IQT51991422	IQT51023522	IQT51023512	IQT46226010
		IQT46226030	IQT46195899	IQT46196077	IQT79636605	IQT46224976	IQT46224986	IQT46205397	IQT46205357
		IQT62119234	IQT113995175	IQT46898760	IQT79639422	IQT46195560	IQT46195580	IQT51023261	IQT51023262
		IQT46197653	IQT46197623	IQT79639344	IQT79639334	IQT46225026	IQT46225006	IQT46197792	IQT51023314
		IQT99877909	IQT46200144	IQT263205692	IQT46199344	IQT46531429	IQT46198882	IQT46197694	IQT46197714
		IQT46225083	IQT46225103	IQT46198242	IQT46198272	IQT46225888	IQT46225908	IQT46224740	IQT46224760
		IQT46198666	IQT46200364	IQT46200394	IQT46200474	IQT46200504	IQT79639213	IQT81952228	IQT50061992
		IQT46200725	IQT51023323	IQT79634296	IQT79634307	IQT46201289	IQT46201319	IQT51023343	IQT46201716
		IQT46202628	IQT51023359	IQT79634644	IQT60516149	IQT46202896	IQT111873228	IQT46211987	IQT79634397
		IQT79634077	IQT79634087	IQT46225374	IQT46225394	IQT46206772	IQT46206790	IQT49750965	IQT61533550
		IQT46206992	IQT106833144	IQT106833134	IQT46207440	IQT46207410	IQT62270069	IQT79640104	IQT46205219
		IQT46216976	IQT79636635	IQT46207892	IQT46207872	IQT46208393	IQT46198904	IQT46302646	IQT46302656
		IQT51023395	IQT51023405	IQT46208242	IQT49751006	IQT106833163	IQT46209464	IQT46209484	IQT46211551
		IQT46210205	IQT46210109	IQT46195600	IQT46195620	IQT106833261	IQT106833271	IQT79634891	IQT79634901
		IQT46225735	IQT46225715	IQT46211878	IQT46211858	IQT60388534	IQT217327837	IQT46224719	IQT46224699
		IQT46531419	IQT46875219	IQT46875229	IQT46196336	IQT46196296	IQT46213563	IQT46213533	IQT46207195
		IQT46302636	IQT79633891	IQT60389288	IQT46215397	IQT46217039	IQT46217059	IQT79640014	IQT313313741
		IQT46217158	IQT46193103	IQT46193083	IQT46217375	IQT49751126	IQT79635832	IQT51649278	IQT263207246
		IQT46262247	IQT46262257	IQT46226152	IQT46226132	IQT46226224	IQT46226204	IQT254955233	IQT46217425
		IQT46219703	IQT46219673	IQT46219740	IQT79636257	IQT49751166	IQT49751156	IQT49751176	IQT49751186
		IQT46199472	IQT46212072	IQT49896508	IQT108848440	IQT46217092	IQT106490915	IQT46206453	IQT46206423
		IQT51532171	IQT51611338	IQT51649277	IQT79634506	IQT46222579	IQT46223228	IQT46223646	IQT46223666
		IQT46223350	IQT46224202	IQT79635962	IQT51532178	IQT51532188			
40	27/05/2011	IQT46201656	IQT313310897	IQT46205935	IQT600184961	IQT313305470	IQT46193028	IQT46195733	IQT46196785
		IQT46204207	IQT46204814	IQT79636325	IQT46203342	IQT46212734	IQT46214216	IQT46216944	IQT46222809
		IQT46216688	IQT46221943	IQT46195429					
41	09/06/2011	IQT323680451	IQT46225354	IQT313313245	IQT46193455	IQT46193940	IQT46261982	IQT46262002	IQT46261992
		IQT51649261	IQT51649271	IQT46193135	IQT46194523	IQT46194543	IQT46211367	IQT46211397	IQT46208924
		IQT46208954	IQT51023497	IQT51023496	IQT46195940	IQT46195910	IQT51023287	IQT137102612	IQT79639264
		IQT60387202	IQT46196922	IQT46302585	IQT79639473	IQT52023880	IQT52023890	IQT79634417	IQT79634427
		IQT51991422	IQT51023490	IQT51023512	IQT51023522	IQT46226010	IQT46226030	IQT46636340	IQT46195491
		IQT79639852	IQT46195899	IQT46196077	IQT79636605	IQT46224986	IQT46224976	IQT46205397	IQT46205357
		IQT62119234	IQT113995175	IQT46898760	IQT79639422	IQT46195560	IQT46195580	IQT51023261	IQT51023262

Table K.1 continued from previous page

Event	Date (Adj.)	S&P CIQ CDS contracts							
		IQT46197653	IQT46197623	IQT79639344	IQT79639334	IQT46225026	IQT46225006	IQT46197792	IQT51023314
		IQT46200144	IQT99877909	IQT46199344	IQT263205692	IQT46531429	IQT46198882	IQT46225103	IQT46225083
		IQT46198242	IQT46198272	IQT46225888	IQT46225908	IQT46224760	IQT46224740	IQT46198666	IQT46200364
		IQT46200394	IQT46200474	IQT46200504	IQT79639213	IQT81952228	IQT50061992	IQT46200725	IQT51023323
		IQT79634296	IQT79634307	IQT46201289	IQT46201319	IQT51023343	IQT46201716	IQT46202628	IQT51023359
		IQT79634644	IQT60516149	IQT46202896	IQT46211987	IQT111873228	IQT79634397	IQT79634077	IQT79634087
		IQT46225394	IQT46225374	IQT46206772	IQT46206790	IQT49750965	IQT61533550	IQT46206992	IQT106833134
		IQT106833144	IQT46207440	IQT46207410	IQT62270069	IQT79640104	IQT46205219	IQT46216976	IQT79636635
		IQT46207892	IQT46207872	IQT46208393	IQT46198904	IQT46302646	IQT46302656	IQT51023405	IQT51023395
		IQT46208242	IQT49751006	IQT106833163	IQT46209464	IQT46209484	IQT46211551	IQT60388494	IQT46210205
		IQT46210109	IQT46195620	IQT46195600	IQT106833271	IQT106833261	IQT79634901	IQT79634891	IQT46225735
		IQT46225715	IQT46211858	IQT46211878	IQT60388534	IQT217327837	IQT46224699	IQT46224719	IQT46531419
		IQT46875219	IQT46875229	IQT46196336	IQT46196296	IQT46213563	IQT46213533	IQT46207195	IQT46302636
		IQT79633891	IQT60389288	IQT46215397	IQT46217059	IQT46217039	IQT79640014	IQT313313741	IQT46217158
		IQT46193103	IQT46193083	IQT46217375	IQT49751126	IQT79635832	IQT263207246	IQT51649278	IQT46262257
		IQT46262247	IQT46226132	IQT46226152	IQT46226224	IQT46226204	IQT254955233	IQT46217425	IQT46219703
		IQT46219673	IQT46219740	IQT79636257	IQT49751156	IQT49751166	IQT49751186	IQT49751176	IQT46199472
		IQT46212072	IQT108848440	IQT49896508	IQT46217092	IQT106490915	IQT46206453	IQT46206423	IQT51532171
		IQT51611338	IQT79634506	IQT51649277	IQT46222579	IQT46223228	IQT46223646	IQT46223666	IQT46223350
		IQT79635962	IQT46224202	IQT51532178	IQT51532188				
42	08/07/2011	IQT46193310	IQT79636176	IQT47049262	IQT313307154	IQT46198389	IQT46199324	IQT46199662	IQT47086788
		IQT79636365	IQT46206853	IQT59069886	IQT46208821	IQT46210064	IQT46210338	IQT46218727	IQT46210574
		IQT46215826	IQT46221691	IQT46202880	IQT46205997	IQT46262306	IQT46216560	IQT126850872	IQT46221764
		IQT46223545	IQT46224308	IQT46224595					
44	23/09/2011	IQT61227153	IQT46202081	IQT263207526	IQT46224423	IQT46200654	IQT46209914	IQT46219771	IQT46216386
		IQT46217188	IQT46219514	IQT79635209					
46	10/02/2012	IQT46222436	IQT46194326	IQT46194401	IQT46199905	IQT79634555	IQT46213371	IQT46203843	IQT79636355
		IQT46206556	IQT60389110	IQT46219344	IQT46221892				
47	22/02/2012	IQT313309643	IQT46210384	IQT46225203	IQT46197673	IQT46218844	IQT46198111	IQT46199968	IQT46206014
		IQT46208192	IQT46208212	IQT46209157	IQT51880919	IQT46211658	IQT46210614	IQT46213329	IQT46212467
		IQT46213253	IQT46210181	IQT46214631	IQT46217028	IQT46720472	IQT46218070	IQT46218602	IQT46221836
		IQT46196166	IQT46221137	IQT46223728					
50	04/05/2012	IQT383116910	IQT46216064	IQT46196675	IQT46200323	IQT46225228	IQT127280715	IQT46205898	IQT46206517
		IQT182349386	IQT60388226	IQT46210225	IQT46213024	IQT46214415	IQT46214901	IQT51023384	IQT46219791
		IQT51023594	IQT46221332	IQT46223258	IQT46899474				
51	18/05/2012	IQT46217355	IQT46199947	IQT81859700	IQT46200286	IQT46204180	IQT46222762	IQT79634872	IQT46196520
		IQT46196274	IQT46200009	IQT79639153	IQT46199619	IQT79636848	IQT46200019	IQT46201472	IQT46200923
		IQT79640084	IQT46204005	IQT46220647	IQT46205259	IQT46206260	IQT46198430	IQT46470865	IQT79634367
		IQT46210288	IQT79639234	IQT46213799	IQT46215275	IQT46215190	IQT46215375	IQT46215155	IQT46217917
		IQT46531439	IQT46217385	IQT81859720	IQT46197353	IQT313312430	IQT46220562	IQT46219118	IQT46207217
		IQT46211253	IQT46213465	IQT79636247	IQT46222529	IQT140598277	IQT46206812	IQT46222839	IQT46198346
		IQT46207989	IQT46224107						
60	11/01/2013	IQT46194401	IQT46199905	IQT79634555	IQT46207083	IQT46213371	IQT46203843	IQT79636355	IQT46206556
		IQT60389110	IQT46219344	IQT46221892					

Table K.1 continued from previous page

Event	Date (Adj.)	S&P CIQ CDS contracts							
61	30/01/2013	IQT237925204	IQT90110031	IQT51023574	IQT79634872	IQT46196520	IQT46196274	IQT46200009	IQT79639153
		IQT79635517	IQT46302605	IQT46199619	IQT79636848	IQT46200019	IQT46201472	IQT46200923	IQT79640084
		IQT46204005	IQT46220647	IQT46205259	IQT46198430	IQT46470865	IQT79634367	IQT46210288	IQT79639234
		IQT46213799	IQT46215275	IQT46215190	IQT46215375	IQT46215155	IQT46217917	IQT46531439	IQT81859720
		IQT46217385	IQT46197353	IQT46204180	IQT313312430	IQT46220562	IQT46219118	IQT46207217	IQT46211253
		IQT79636247	IQT46222529	IQT140598277	IQT46206812	IQT46222839	IQT46198346	IQT46207989	IQT46224107
64	22/02/2013	IQT644701487	IQT263815084	IQT46197734	IQT46217745	IQT46207150	IQT46213903		
66	28/03/2013	IQT323680451	IQT46193381	IQT46204639	IQT46199354	IQT46198161	IQT52439017	IQT46202967	IQT46203463
		IQT46204238	IQT46205682	IQT46206554	IQT46200602	IQT46218475	IQT226853103	IQT46219023	IQT46215170
		IQT79636455	IQT79635149						
67	28/03/2013	IQT46193556	IQT323680451	IQT579299842	IQT46207150	IQT60388494	IQT46214601	IQT313313245	IQT46195905
		IQT46193455	IQT46261982	IQT46193940	IQT217703448	IQT46262002	IQT46261992	IQT51649261	IQT51649271
		IQT46193135	IQT46194523	IQT46194543	IQT46211367	IQT46211397	IQT46208924	IQT46208954	IQT51023496
		IQT51023497	IQT46195940	IQT46195910	IQT51023287	IQT137102612	IQT46196922	IQT60387202	IQT79639264
		IQT225526445	IQT46302585	IQT79639473	IQT52023880	IQT52023890	IQT79634417	IQT79634427	IQT51023522
		IQT51023512	IQT46226010	IQT46226030	IQT46636340	IQT46195491	IQT79639852	IQT46195899	IQT46196077
		IQT79636605	IQT46224986	IQT46224976	IQT46205357	IQT46205397	IQT217327818	IQT217327808	IQT62119234
		IQT113995175	IQT46898760	IQT79639422	IQT46195560	IQT46195580	IQT51023261	IQT46197653	IQT46197623
		IQT79639344	IQT79639334	IQT46225026	IQT46225006	IQT46197792	IQT51023314	IQT46200144	IQT99877909
		IQT46199344	IQT263205692	IQT46531429	IQT46198882	IQT46197694	IQT46197714	IQT46225103	IQT46225083
		IQT46198242	IQT46198272	IQT46225888	IQT46225908	IQT46224760	IQT46224740	IQT46198666	IQT46200394
		IQT46200364	IQT46200474	IQT46200504	IQT79639213	IQT81952228	IQT50061992	IQT46200725	IQT51023323
		IQT79634307	IQT79634296	IQT51023343	IQT46201716	IQT46202628	IQT51023359	IQT60516149	IQT79634644
		IQT46202896	IQT111873228	IQT46211987	IQT79634397	IQT79634077	IQT79634087	IQT46225394	IQT46225374
		IQT46206772	IQT46206790	IQT49750965	IQT61533550	IQT46206992	IQT106833134	IQT106833144	IQT46207440
		IQT46207410	IQT62270069	IQT79640104	IQT46205219	IQT46216976	IQT79636635	IQT46208393	IQT46198904
		IQT46302646	IQT46302656	IQT51023395	IQT51023405	IQT46208242	IQT49751006	IQT106833163	IQT46209464
		IQT46209484	IQT46211551	IQT46210205	IQT46210109	IQT46195620	IQT46195600	IQT106833271	IQT106833261
		IQT79634901	IQT79634891	IQT46225735	IQT46225715	IQT46211858	IQT46211878	IQT60388534	IQT46224719
		IQT46224699	IQT46531419	IQT46875219	IQT46875229	IQT46196296	IQT46196336	IQT46213563	IQT46213533
		IQT46302636	IQT46207195	IQT60389288	IQT46215397	IQT217387953	IQT139428738	IQT139428745	IQT46217059
		IQT46217039	IQT79640014	IQT313313741	IQT46217158	IQT46193103	IQT46193083	IQT46217375	IQT49751126
		IQT79635832	IQT263207246	IQT51649278	IQT46262257	IQT46262247	IQT46226132	IQT46226152	IQT46226204
		IQT46226224	IQT254955233	IQT46217425	IQT46219703	IQT46219673	IQT46219740	IQT79636257	IQT49751166
		IQT49751156	IQT49751176	IQT49751186	IQT46199472	IQT46212072	IQT49896508	IQT217327865	IQT46217092
		IQT106490915	IQT46206423	IQT46206453	IQT51532171	IQT51611338	IQT79634506	IQT51649277	IQT46222579
		IQT46223228	IQT46223646	IQT46223666	IQT79635962	IQT46224202	IQT51532178	IQT51532188	IQT217387932
69	22/07/2013	IQT46193310	IQT263815084	IQT46195910	IQT46196015	IQT46196872	IQT217703455	IQT46201372	IQT46200923
		IQT46225517	IQT540717389	IQT46210288	IQT559971761	IQT46220562	IQT61227153	IQT46200654	IQT46206055
		IQT46209914	IQT46219771	IQT46216386	IQT46217188	IQT46219514	IQT79635209	IQT46224423	
72	09/08/2013	IQT600184961	IQT46201656	IQT46193028	IQT46195733	IQT46196785	IQT46204207	IQT46204814	IQT79636325
		IQT46203342	IQT46209597	IQT46214216	IQT46216944	IQT46222809	IQT46216688	IQT46221943	IQT46205935
		IQT46195429							
77	25/11/2013	IQT46194483	IQT46194851	IQT46195070	IQT46197502	IQT46196176	IQT46197168	IQT79634851	IQT46213361

Table K.1 continued from previous page

Event	Date (Adj.)	S&P CIQ CDS contracts							
		IQT46199685	IQT46201240	IQT46206126	IQT46202606	IQT46203740	IQT46203055	IQT46203682	IQT46204311
		IQT46205882	IQT46206085	IQT46205488	IQT46205718	IQT46206198	IQT46207323	IQT79636156	IQT46217959
		IQT46208339	IQT46209291	IQT46208841	IQT46199029	IQT46212416	IQT46205810	IQT46214758	IQT46202612
		IQT79636554	IQT46218486	IQT46206065	IQT46218864	IQT46200552	IQT99877923	IQT46222229	IQT46222343
		IQT81859776	IQT46224179	IQT46205468	IQT46224255				
78	05/12/2013	IQT46193556	IQT323680451	IQT579299842	IQT46207150	IQT60388494	IQT46214601	IQT313313245	IQT46195905
		IQT250056879	IQT250056869	IQT46193455	IQT46193940	IQT46261982	IQT217703448	IQT46262002	IQT46261992
		IQT51649271	IQT51649261	IQT46193135	IQT46194523	IQT46194543	IQT46211367	IQT46211397	IQT46208924
		IQT46208954	IQT51023497	IQT51023496	IQT46195940	IQT46195910	IQT51023287	IQT137102612	IQT79639264
		IQT46196922	IQT60387202	IQT225526445	IQT46302585	IQT79639473	IQT52023890	IQT52023880	IQT79634417
		IQT79634427	IQT225478176	IQT51023522	IQT51023512	IQT46226010	IQT46226030	IQT46636340	IQT46195491
		IQT79639852	IQT46195899	IQT46196077	IQT79636605	IQT46224976	IQT46224986	IQT46205397	IQT46205357
		IQT217327808	IQT217327818	IQT62119234	IQT113995175	IQT46898760	IQT79639422	IQT46195560	IQT46195580
		IQT51023261	IQT46197653	IQT46197623	IQT79639344	IQT79639334	IQT46225026	IQT46225006	IQT46197792
		IQT51023314	IQT46200144	IQT99877909	IQT250610560	IQT46199344	IQT263205692	IQT133066284	IQT46531429
		IQT46198882	IQT46197694	IQT46197714	IQT46225103	IQT46225083	IQT46198242	IQT46198272	IQT46225888
		IQT46225908	IQT46224740	IQT46224760	IQT46198666	IQT46200394	IQT46200364	IQT46200504	IQT46200474
		IQT79639213	IQT81952228	IQT50061992	IQT51023323	IQT46200725	IQT79634296	IQT79634307	IQT51023343
		IQT46201716	IQT46202628	IQT51023359	IQT79634644	IQT60516149	IQT46202896	IQT46211987	IQT111873228
		IQT79634397	IQT79634077	IQT79634087	IQT46225374	IQT46225394	IQT46206772	IQT46206790	IQT49750965
		IQT61533550	IQT46206992	IQT106833134	IQT106833144	IQT46207440	IQT46207410	IQT62270069	IQT79640104
		IQT46205219	IQT46216976	IQT79636635	IQT46208393	IQT46198904	IQT46302646	IQT46302656	IQT51023395
		IQT51023405	IQT46208242	IQT49751006	IQT106833163	IQT46209484	IQT46209464	IQT46211551	IQT46210205
		IQT46210109	IQT46195600	IQT46195620	IQT106833261	IQT106833271	IQT79634901	IQT79634891	IQT46225715
		IQT46225735	IQT46211878	IQT46211858	IQT60388534	IQT46224719	IQT46224699	IQT46531419	IQT46875229
		IQT46875219	IQT46196336	IQT46196296	IQT46213563	IQT46213533	IQT46207195	IQT46302636	IQT60389288
		IQT46215397	IQT217387953	IQT139428745	IQT139428738	IQT46217059	IQT46217039	IQT79640014	IQT313313741
		IQT46217158	IQT46193103	IQT46193083	IQT46217375	IQT49751126	IQT79635832	IQT263207246	IQT51649278
		IQT46262257	IQT46262247	IQT46226152	IQT46226132	IQT46226224	IQT46226204	IQT256193521	IQT254955233
		IQT46217425	IQT46219703	IQT46219673	IQT46219740	IQT79636257	IQT46219321	IQT49751156	IQT49751166
		IQT49751176	IQT49751186	IQT244437080	IQT46199472	IQT46212072	IQT49896508	IQT217327865	IQT46217092
		IQT106490915	IQT46206453	IQT46206423	IQT51532171	IQT51611338	IQT79634506	IQT51649277	IQT46222579
		IQT79639432	IQT46223228	IQT46223646	IQT46223666	IQT79635962	IQT46224202	IQT51532178	IQT51532188
		IQT217387932							
80	13/12/2013	IQT79636815	IQT46193890	IQT49751066	IQT46208706	IQT46200572	IQT46207342	IQT46207777	IQT46208750
		IQT79639842	IQT46203137	IQT79634157	IQT46720471	IQT46213382	IQT46207938	IQT46218397	IQT46220173
		IQT46223556							
81	27/12/2013	IQT323680451	IQT46193381	IQT46204639	IQT46199354	IQT46198161	IQT52439017	IQT46202967	IQT46203463
		IQT46204238	IQT46205682	IQT46206554	IQT46200602	IQT46218475	IQT226853103	IQT46219023	IQT46215170
		IQT79636455	IQT79635149						
82	07/02/2014	IQT46197343	IQT46197768	IQT46209261	IQT46210415	IQT79635189	IQT46200788	IQT46193236	IQT46196745
		IQT46195846	IQT46196206	IQT143266031	IQT46199609	IQT46200858	IQT46225838		
86	26/02/2014	IQT46193310	IQT263815084	IQT46195910	IQT46196015	IQT46196872	IQT217703455	IQT46201372	IQT46200923
		IQT46225517	IQT540717389	IQT46210288	IQT559971761	IQT46220562	IQT61227153	IQT46200654	IQT46206055
		IQT46209914	IQT46219771	IQT46216386	IQT46217188	IQT46219514	IQT79635209	IQT46224423	

Table K.1 continued from previous page

Event	Date (Adj.)	S&P CIQ CDS contracts							
88	04/03/2014	IQT323680451	IQT313313245	IQT46193381	IQT46204639	IQT46195298	IQT46198161	IQT52439017	IQT46202967
		IQT46203463	IQT46204238	IQT46205682	IQT46206554	IQT46200602	IQT46218475	IQT79635248	IQT226853103
		IQT46219023	IQT46215170	IQT79636455	IQT79635149				
94	11/07/2014	IQT46201656	IQT46193028	IQT46195184	IQT60388803	IQT46195429	IQT313309436	IQT600184961	IQT46195733
		IQT46196785	IQT263213154	IQT46204207	IQT46204814	IQT79636325	IQT46203342	IQT46209597	IQT46212734
		IQT46214216	IQT46216944	IQT46222809	IQT46216688	IQT46221943	IQT46205935		
95	11/07/2014	IQT46201656	IQT313310897	IQT46205935	IQT600184961	IQT313305470	IQT46193028	IQT46195733	IQT46196785
		IQT263213154	IQT46204207	IQT46204814	IQT79636325	IQT46203342	IQT46212734	IQT46214216	IQT46216944
		IQT46222809	IQT46216688	IQT46221943	IQT46195429				
96	21/07/2014	IQT313307823	IQT46220227	IQT46213231	IQT46199259	IQT46198595	IQT46199155	IQT79636795	IQT46201797
		IQT46201442	IQT217387925	IQT46202459	IQT46204123	IQT79635417	IQT46208739	IQT46212364	IQT46216996
		IQT46217519	IQT46219033	IQT46202365	IQT46220399	IQT46223052	IQT46223534		
97	15/08/2014	IQT46208706	IQT46207922	IQT46193195	IQT46194964	IQT46197746	IQT46199384	IQT46199418	IQT46199578
		IQT46200632	IQT263213267	IQT49937990	IQT46217447	IQT46193890	IQT46193206	IQT46215699	IQT46215628
		IQT46220056	IQT46211613	IQT46220092	IQT46221681	IQT46224012	IQT46224060		
98	18/08/2014	IQT542600614	IQT46222242	IQT313309795	IQT46193699	IQT46193123	IQT46223889	IQT46193870	IQT46197768
		IQT46198775	IQT46200059	IQT46200090	IQT46201533	IQT79636625	IQT46205770	IQT46225248	IQT79635660
		IQT46205914	IQT46206320	IQT46209261	IQT46205508	IQT46210360	IQT46210687	IQT46213573	IQT79635782
		IQT46200788	IQT46220857	IQT247023954	IQT46222425				
100	28/08/2014	IQT46193556	IQT323680451	IQT579299842	IQT46207150	IQT60388494	IQT46214601	IQT313313245	IQT46195905
		IQT250056879	IQT250056869	IQT46193455	IQT46193940	IQT46261982	IQT217703448	IQT46262002	IQT46261992
		IQT51649261	IQT51649271	IQT46193135	IQT46194523	IQT46194543	IQT46211367	IQT46211397	IQT46208924
		IQT46208954	IQT51023497	IQT51023496	IQT46195940	IQT46195910	IQT51023287	IQT137102612	IQT60387202
		IQT46196922	IQT79639264	IQT225526445	IQT79639473	IQT46302585	IQT52023890	IQT52023880	IQT79634417
		IQT79634427	IQT225478176	IQT51023512	IQT51023522	IQT46226010	IQT46226030	IQT46636340	IQT46195491
		IQT79639852	IQT46195899	IQT46196077	IQT79636605	IQT46224976	IQT46224986	IQT46205357	IQT46205397
		IQT217327808	IQT217327818	IQT62119234	IQT113995175	IQT79639422	IQT46898760	IQT46195560	IQT46195580
		IQT51023261	IQT46197653	IQT46197623	IQT231906871	IQT79639344	IQT79639334	IQT46225026	IQT46225006
		IQT46197792	IQT99877909	IQT46200144	IQT250610560	IQT263205692	IQT46199344	IQT133066284	IQT46531429
		IQT46198882	IQT263212912	IQT46197714	IQT46197694	IQT46225103	IQT46225083	IQT46198242	IQT46198272
		IQT46225908	IQT46225888	IQT263213197	IQT46224760	IQT46224740	IQT46198666	IQT46200364	IQT46200394
		IQT46200474	IQT46200504	IQT79639213	IQT81952228	IQT50061992	IQT46200725	IQT51023323	IQT79634307
		IQT79634296	IQT51023343	IQT46201716	IQT46202628	IQT51023359	IQT79634644	IQT60516149	IQT46202896
		IQT111873228	IQT46211987	IQT79634397	IQT79634087	IQT79634077	IQT46225374	IQT46225394	IQT46206772
		IQT46206790	IQT49750965	IQT61533550	IQT46206992	IQT106833134	IQT106833144	IQT46225517	IQT46207410
		IQT46207440	IQT62270069	IQT79640104	IQT46205219	IQT46216976	IQT79636635	IQT46208393	IQT46198904
		IQT46302646	IQT46302656	IQT51023405	IQT51023395	IQT46208242	IQT263213101	IQT49751006	IQT106833163
		IQT46209484	IQT46209464	IQT46211551	IQT46210205	IQT46210109	IQT46195600	IQT46195620	IQT106833261
		IQT106833271	IQT79634901	IQT79634891	IQT46225735	IQT46225715	IQT46211878	IQT46211858	IQT60388534
		IQT46224699	IQT46224719	IQT46531419	IQT143266041	IQT46875229	IQT46875219	IQT46196336	IQT46196296
		IQT46213563	IQT46213533	IQT46207195	IQT46302636	IQT60389288	IQT46215397	IQT217387953	IQT139428738
		IQT139428745	IQT46217039	IQT46217059	IQT313313741	IQT79640014	IQT46217158	IQT46193103	IQT46193083
		IQT46217375	IQT49751126	IQT79635832	IQT263207246	IQT51649278	IQT46262257	IQT46262247	IQT46226152
		IQT46226132	IQT46226204	IQT46226224	IQT256193521	IQT254955233	IQT46217425	IQT46219673	IQT46219703
		IQT79636257	IQT46219740	IQT46219321	IQT49751166	IQT49751156	IQT49751176	IQT49751186	IQT244437080

Table K.1 continued from previous page

Event	Date (Adj.)	S&P CIQ CDS contracts							
		IQT46199472	IQT46212072	IQT49896508	IQT217327865	IQT263213132	IQT263213143	IQT46217092	IQT46220329
		IQT106490915	IQT46206453	IQT46206423	IQT49750875	IQT51532171	IQT51611338	IQT79634506	IQT51649277
		IQT46222579	IQT79639432	IQT46223228	IQT46223646	IQT46223666	IQT79635962	IQT46224202	IQT51532178
		IQT51532188	IQT217387932						
101	02/09/2014	IQT46193310	IQT263815084	IQT46195910	IQT46196015	IQT46196872	IQT217703455	IQT46201372	IQT46200923
		IQT46225517	IQT540717389	IQT46210288	IQT559971761	IQT46220562	IQT61227153	IQT46200654	IQT46206055
		IQT46209914	IQT46219771	IQT46216386	IQT46217188	IQT46219514	IQT79635209	IQT46224423	
102	02/09/2014	IQT46193836	IQT46194500	IQT46195359	IQT46195869	IQT46195950	IQT46210519	IQT265079462	IQT46201339
		IQT79636815	IQT46208360	IQT46209775	IQT46209672	IQT247023968	IQT49751066	IQT46216933	IQT46218917
		IQT46204804	IQT46220901	IQT46221292					
103	06/10/2014	IQT46194493	IQT323679950	IQT46220237	IQT46226245	IQT644701487	IQT263207493	IQT46197228	IQT46200009
		IQT217703455	IQT46200019	IQT46200923	IQT79636815	IQT46210288	IQT263815084	IQT46196015	IQT46196575
		IQT127288394	IQT46200124	IQT46199947	IQT214738016	IQT46201372	IQT46898887	IQT46875103	IQT46200286
		IQT46213991	IQT46207093	IQT46208685	IQT46208665	IQT46209833	IQT46213157	IQT46213841	IQT109027089
		IQT79634236	IQT46203750	IQT46214136	IQT60387242	IQT46215566	IQT46215546	IQT79635812	IQT46218241
		IQT79639812	IQT46226266	IQT79635882	IQT49751096	IQT46220521	IQT46226296	IQT46220769	IQT46220923
		IQT46220614	IQT46220634	IQT46220961	IQT46220541	IQT46220309	IQT266978831	IQT79639406	IQT46223278
		IQT79636665	IQT79636675	IQT79640270	IQT79636685	IQT46223743	IQT46223793	IQT113995168	
104	10/10/2014	IQT79636815	IQT46209672	IQT46200572	IQT46207342	IQT46207777	IQT46208750	IQT79639842	IQT46203137
		IQT79634157	IQT46720471	IQT46213382	IQT46207938	IQT46218397	IQT46220173	IQT46220782	IQT46223556
105	20/10/2014	IQT49751066	IQT46193836	IQT46194500	IQT46195359	IQT46195869	IQT46195950	IQT46210519	IQT265079462
		IQT46201339	IQT79636815	IQT272307325	IQT46208360	IQT46209775	IQT46209672	IQT247023968	IQT46216933
		IQT46204804	IQT46205518	IQT46220901	IQT46221292				
109	26/12/2014	IQT644701487	IQT263815084	IQT79636815	IQT46210064	IQT46197734	IQT46217745	IQT46207150	IQT46213903
110	02/01/2015	IQT46194413	IQT46194502	IQT46195460	IQT46200333	IQT46209797	IQT84135655	IQT263204406	IQT46207725
		IQT46225868	IQT46217309	IQT46194002	IQT46209809				
111	05/01/2015	IQT579299842	IQT60388494	IQT46217561	IQT46262077	IQT46875079	IQT106833201	IQT46195642	IQT79636565
		IQT46199861	IQT46199841	IQT46200317	IQT46200432	IQT46200412	IQT263204979	IQT46875109	IQT46205104
		IQT217387939	IQT102286632	IQT84609938	IQT46202230	IQT46202260	IQT46210462	IQT46262097	IQT46262087
		IQT46225948	IQT46225968	IQT46212786	IQT62270106	IQT46223596	IQT46223626	IQT46210657	IQT46220667
		IQT263578030	IQT46197292	IQT46204957	IQT46204987	IQT46222168	IQT46222188	IQT46223289	IQT46223159
113	05/02/2015	IQT46193699	IQT46193123	IQT46193870	IQT46197768	IQT46198775	IQT46200195	IQT46200059	IQT46200090
		IQT46201533	IQT79636625	IQT46205770	IQT46225248	IQT79635660	IQT46205914	IQT46206320	IQT46209261
		IQT46205508	IQT46210360	IQT46210687	IQT46213573	IQT79635782	IQT46200788	IQT46220857	IQT247023954
		IQT46222425	IQT46222242						
115	02/04/2015	IQT644701487	IQT263815084	IQT79636815	IQT46210064	IQT46197734	IQT46217745	IQT46207150	IQT46213903
116	08/04/2015	IQT46194493	IQT323679950	IQT46220237	IQT46226245	IQT644701487	IQT263207493	IQT46197228	IQT46200009
		IQT217703455	IQT46200019	IQT46200923	IQT79636815	IQT46210288	IQT263815084	IQT46196015	IQT46196575
		IQT127288394	IQT46200124	IQT46199947	IQT214738016	IQT46201372	IQT46898887	IQT46875103	IQT46200286
		IQT46213991	IQT46207093	IQT46208685	IQT46208665	IQT46209833	IQT46213157	IQT46213841	IQT109027089

Table K.1 continued from previous page

Event	Date (Adj.)	S&P CIQ CDS contracts							
		IQT79634236	IQT46203750	IQT46214136	IQT60387242	IQT46215566	IQT46215546	IQT79635812	IQT46218241
		IQT79639812	IQT46226266	IQT79635882	IQT49751096	IQT46220521	IQT46226296	IQT46220769	IQT46220923
		IQT46220614	IQT46220634	IQT46220961	IQT46220541	IQT46220309	IQT266978831	IQT79639406	IQT46223278
		IQT79636665	IQT79636675	IQT79640270	IQT79636685	IQT46223743	IQT46223793	IQT113995168	IQT288776504
119	29/07/2015	IQT284865129	IQT46194413	IQT46194502	IQT46195460	IQT46200333	IQT46209797	IQT84135655	IQT263204406
		IQT46207725	IQT46225868	IQT46217309	IQT46194002	IQT46209809			
125	09/11/2015	IQT46217355	IQT46199947	IQT81859700	IQT46200286	IQT46204180	IQT46222762	IQT263811768	IQT79634872
		IQT46196520	IQT46196274	IQT46200009	IQT79639153	IQT46199619	IQT79636848	IQT46200019	IQT46200996
		IQT46201472	IQT46200923	IQT79640084	IQT46204005	IQT46220647	IQT46205259	IQT46198430	IQT46470865
		IQT79634367	IQT46210288	IQT79639234	IQT46213799	IQT46215275	IQT46215190	IQT46215375	IQT46215155
		IQT46217917	IQT46531439	IQT46217385	IQT81859720	IQT46197353	IQT46220562	IQT46219118	IQT46207217
		IQT46211253	IQT46213465	IQT79636247	IQT46222529	IQT285746028	IQT140598277	IQT46206812	IQT46222839
		IQT46198346	IQT46207989	IQT46224107					
126	20/11/2015	IQT323680561	IQT79635351	IQT46193310	IQT79636176	IQT263205962	IQT46198389	IQT46198409	IQT46199662
		IQT47086788	IQT46201254	IQT273869904	IQT272304501	IQT79636365	IQT244437052	IQT46206853	IQT311701972
		IQT59069886	IQT46208821	IQT263213011	IQT46210064	IQT46210338	IQT46218727	IQT46210574	IQT272307369
		IQT46215826	IQT46221691	IQT46202880	IQT46262306	IQT46216560	IQT126850872	IQT46221764	IQT46223545
		IQT79634856	IQT46224308	IQT46224595					
127	21/12/2015	IQT46194211	IQT46199892	IQT46211478	IQT46212776	IQT46194201	IQT46209576		
135	03/05/2016	IQT313305671	IQT46470877	IQT46217561	IQT60388107	IQT46262077	IQT46875079	IQT106833201	IQT46195642
		IQT79636565	IQT46199861	IQT46199841	IQT46200317	IQT46200412	IQT46200432	IQT263204979	IQT328439949
		IQT46875109	IQT46205104	IQT217387939	IQT102286632	IQT84609938	IQT46202260	IQT46202230	IQT46210462
		IQT46262097	IQT46262087	IQT46225948	IQT46225968	IQT46212786	IQT62270106	IQT46223596	IQT46223626
		IQT46210657	IQT46220667	IQT263578030	IQT46197292	IQT46204987	IQT46204957	IQT46222168	IQT46222188
		IQT46223289	IQT46223159						
136	05/05/2016	IQT213789472	IQT313309519	IQT46197985	IQT46199459	IQT46193411	IQT46199872	IQT46203147	IQT46203954
		IQT46206637	IQT46212162	IQT46224244	IQT46221361	IQT46222272			
146	12/12/2016	IQT46193699	IQT46193123	IQT46223889	IQT46193870	IQT46197768	IQT46198775	IQT46200195	IQT46200059
		IQT46200090	IQT46201533	IQT46205770	IQT263205017	IQT46225248	IQT79635660	IQT46205914	IQT46206320
		IQT46209261	IQT46205508	IQT46210360	IQT46210687	IQT79635782	IQT46220857	IQT247023954	IQT46222425
		IQT46222242							
150	06/02/2017	IQT323680451	IQT313313245	IQT46193381	IQT46204639	IQT46195298	IQT263212887	IQT79636835	IQT263205078
		IQT46198161	IQT52439017	IQT46202967	IQT46203463	IQT46205682	IQT46206554	IQT46200602	IQT46218475
		IQT79635248	IQT226853103	IQT46219023	IQT46215170	IQT79636455	IQT79635149		
156	17/05/2017	IQT46200090	IQT46224012	IQT46198775	IQT323680331	IQT46207922	IQT46193195	IQT46194964	IQT46197746
		IQT46199384	IQT46199418	IQT46199578	IQT46200632	IQT263213267	IQT316209945	IQT49937990	IQT46217447
		IQT46193890	IQT46193206	IQT46215699	IQT46220056	IQT46211613	IQT46219881	IQT46220092	IQT46221681
		IQT46208706	IQT226470443	IQT279643601	IQT46224060				
160	31/07/2017	IQT46193699	IQT46193123	IQT46193870	IQT46197768	IQT46198775	IQT46200195	IQT46200059	IQT46200090
		IQT46201533	IQT46205770	IQT263205017	IQT46225248	IQT79635660	IQT46205914	IQT46206320	IQT46209261
		IQT46205508	IQT46210360	IQT46210687	IQT79635782	IQT46200788	IQT46220857	IQT247023954	IQT46222425

Table K.1 continued from previous page

Event	Date (Adj.)	S&P CIQ CDS contracts							
		IQT46222242							
166	22/01/2018	IQT46206228	IQT46194291	IQT81952238	IQT46205549	IQT323680521	IQT79639712	IQT46875135	IQT79633967
		IQT46197448	IQT46194777	IQT46203547	IQT46198038	IQT46219530	IQT46200888	IQT46203042	IQT46208382
		IQT46220217	IQT46214332	IQT46216406	IQT46217278	IQT46214083			
167	16/02/2018	IQT644701487	IQT59069893	IQT323680561	IQT46218727	IQT53957994	IQT79635351	IQT46193310	IQT79636176
		IQT46198389	IQT46198409	IQT46199662	IQT47086788	IQT46201254	IQT272304501	IQT273869904	IQT79636365
		IQT244437052	IQT46206853	IQT311701972	IQT59069886	IQT46208821	IQT263213011	IQT46210338	IQT341877193
		IQT46210574	IQT272307369	IQT46215826	IQT46221691	IQT46202880	IQT46205997	IQT46262306	IQT46216560
		IQT126850872	IQT46221764	IQT46223545	IQT79634856	IQT46224308	IQT46224595		
169	06/04/2018	IQT46194502	IQT46207659	IQT284865129	IQT46194413	IQT46195460	IQT46209797	IQT84135655	IQT263204406
		IQT46207725	IQT46225868	IQT46217309	IQT46194002	IQT46209809	IQT46222125	IQT133277400	IQT46197882
171	20/04/2018	IQT46225354	IQT313313245	IQT250056879	IQT250056869	IQT46193455	IQT310462941	IQT46193940	IQT46261982
		IQT217703448	IQT46262002	IQT46261992	IQT51649271	IQT51649261	IQT46193135	IQT46194543	IQT46194523
		IQT46211397	IQT46211367	IQT46208954	IQT46208924	IQT46195910	IQT46195940	IQT51023287	IQT137102612
		IQT46196922	IQT46197025	IQT225526445	IQT46302585	IQT79639473	IQT52023890	IQT52023880	IQT79634417
		IQT79634427	IQT225478176	IQT51023522	IQT51023512	IQT46226010	IQT46226030	IQT46636340	IQT46195491
		IQT79639852	IQT46195899	IQT46196077	IQT79636605	IQT46224976	IQT46224986	IQT46205397	IQT46205357
		IQT217327818	IQT217327808	IQT62119234	IQT113995175	IQT79639422	IQT46898760	IQT46195560	IQT46195580
		IQT286096131	IQT286096135	IQT51023261	IQT46197653	IQT46197623	IQT231906871	IQT79639344	IQT79639334
		IQT46225026	IQT46225006	IQT305938504	IQT46197792	IQT99877909	IQT46200144	IQT250610560	IQT313309489
		IQT46199344	IQT133066284	IQT313313591	IQT46531429	IQT46198882	IQT263212912	IQT46197694	IQT46197714
		IQT46225103	IQT46225083	IQT46198242	IQT46198272	IQT46225908	IQT46225888	IQT263213197	IQT46224760
		IQT46224740	IQT381016479	IQT381016469	IQT46198666	IQT46200364	IQT46200394	IQT46200504	IQT46200474
		IQT79639213	IQT81952228	IQT50061992	IQT46200725	IQT51023323	IQT79634296	IQT79634307	IQT319851547
		IQT319851537	IQT51023343	IQT46201716	IQT46202628	IQT51023359	IQT79634644	IQT60516149	IQT46202896
		IQT111873228	IQT46211987	IQT79634397	IQT79634077	IQT79634087	IQT46225374	IQT46225394	IQT46206772
		IQT46206790	IQT49750965	IQT61533550	IQT46206992	IQT106833144	IQT106833134	IQT313313488	IQT46225517
		IQT46207440	IQT46207410	IQT62270069	IQT79640104	IQT46205219	IQT46216976	IQT79636635	IQT46207872
		IQT46207892	IQT313311056	IQT46208393	IQT46198904	IQT273728799	IQT273728789	IQT46302646	IQT46302656
		IQT51023405	IQT51023395	IQT46208242	IQT263213101	IQT49751006	IQT106833163	IQT46209464	IQT46209484
		IQT528809131	IQT540717389	IQT46211551	IQT60388494	IQT46210205	IQT46210109	IQT46195620	IQT46195600
		IQT106833261	IQT106833271	IQT79634891	IQT79634901	IQT46225715	IQT46225735	IQT46211878	IQT46211858
		IQT60388534	IQT46224699	IQT46224719	IQT46531419	IQT143266041	IQT46875219	IQT46875229	IQT46196336
		IQT46196296	IQT46213563	IQT46213533	IQT46207195	IQT46302636	IQT60389288	IQT46215397	IQT217387953
		IQT139428738	IQT139428745	IQT46217039	IQT46217059	IQT79640014	IQT313317344	IQT46217158	IQT279643592
		IQT46193083	IQT46193103	IQT46217375	IQT49751126	IQT79635832	IQT51649278	IQT46262247	IQT46262257
		IQT46226152	IQT46226132	IQT46226204	IQT46226224	IQT254955233	IQT256193521	IQT46217425	IQT46219703
		IQT46219673	IQT46219740	IQT79636257	IQT49751166	IQT49751156	IQT49751176	IQT49751186	IQT244437080
		IQT313312671	IQT313310854	IQT289841277	IQT46199472	IQT46212072	IQT49896508	IQT217327865	IQT263213132
		IQT263213143	IQT46217092	IQT46220329	IQT313306476	IQT313307410	IQT424221615	IQT106490915	IQT46206453
		IQT46206423	IQT49750875	IQT51532171	IQT51611338	IQT79634506	IQT51649277	IQT46222579	IQT79639432
		IQT46223228	IQT46223666	IQT46223646	IQT79635962	IQT46224202	IQT51532188	IQT51532178	IQT217387932
180	05/11/2018	IQT46212680	IQT46200572	IQT46207342	IQT46207777	IQT46208750	IQT79639842	IQT46203137	IQT79634157
		IQT46720471	IQT46213382	IQT46218397	IQT266699714	IQT46220173	IQT46220782	IQT46223556	
183	11/09/2017	IQT46216677	IQT46209732	IQT111277363	IQT46202772	IQT46202311	IQT46210967	IQT46217541	

Table K.1 continued from previous page

Event	Date (Adj.)	S&P CIQ CDS contracts							
186	28/06/2018	IQT46209384	IQT46215204	IQT46209171	IQT46209311	IQT46211285	IQT46212619	IQT46207837	IQT268882239
		IQT46223029							
188	04/09/2009	IQT46199132	IQT313310897	IQT46203791	IQT313308907	IQT46201116	IQT313311411	IQT79634535	IQT46198796
		IQT79640340	IQT79636105	IQT46204660	IQT46206935	IQT79634931	IQT46210076	IQT46211047	IQT46212723
		IQT79639396	IQT46215743	IQT62270107	IQT79635059	IQT46222649	IQT79635942		
189	27/12/2010	IQT313310897	IQT383116910	IQT46216064	IQT46196675	IQT46200323	IQT46225228	IQT46202947	IQT46206517
		IQT60388226	IQT46210225	IQT46213024	IQT46214415	IQT46214901	IQT51023384	IQT46219791	IQT51023594
		IQT46221332	IQT46223258	IQT46899474					
191	02/03/2012	IQT61227153	IQT46899474	IQT46200654	IQT46202081	IQT46206055	IQT46209914	IQT46219771	IQT46216386
		IQT46217188	IQT46219514	IQT46224423					
193	03/06/2009	IQT46193556	IQT648548478	IQT46193586	IQT79639193	IQT79639183	IQT46194263	IQT46194233	IQT46193185
		IQT46193175	IQT46193721	IQT46193990	IQT46194573	IQT46224866	IQT46224846	IQT46194032	IQT46193815
		IQT46203802	IQT106833211	IQT46195246	IQT46195266	IQT46195318	IQT46198177	IQT46198222	IQT46193330
		IQT46199166	IQT46215898	IQT46203234	IQT46203254	IQT46302616	IQT46204682	IQT46225299	IQT46225319
		IQT79639832	IQT46209211	IQT46209241	IQT88648731	IQT88648721	IQT46209617	IQT46209786	IQT46211181
		IQT46210265	IQT46210275	IQT46210495	IQT46302708	IQT46225775	IQT46225755	IQT79639314	IQT79639304
		IQT46213913	IQT46213738	IQT46213768	IQT46875110	IQT46215244	IQT46215264	IQT46215520	IQT46216580
		IQT46216873	IQT46216893	IQT46217123	IQT46226090	IQT46226070	IQT46217623	IQT49751106	IQT46302727
		IQT46219208	IQT46219188	IQT83051483	IQT46194102	IQT46205674	IQT46214580	IQT46219178	IQT46210831
		IQT51023605	IQT51023600	IQT46222488	IQT46224381	IQT46224622	IQT46224642		
194	26/09/2013	IQT46224054	IQT46193509	IQT51023574					
198	16/04/2013	IQT46219033	IQT46222913	IQT46223052	IQT46209629	IQT46193628	IQT79640350	IQT46201686	IQT46720464
		IQT46198818	IQT46201205	IQT46201523	IQT46202123	IQT46201810	IQT46202344	IQT46202143	IQT46202385
		IQT46202802	IQT46898927	IQT46213188	IQT46202849	IQT46203210	IQT46203791	IQT60387947	IQT46208675
		IQT46262117	IQT79634167	IQT46203652	IQT46212973	IQT46210855	IQT46262043	IQT46214156	IQT46214891
		IQT46214559	IQT46215912	IQT79634516	IQT222934195	IQT79636116	IQT106833301	IQT46219097	IQT46220708
		IQT222889485	IQT46207460	IQT46208041	IQT46218659	IQT223291528	IQT46221076	IQT60389388	IQT46224339

Appendix L
CDS Regression Sample: Country Indices, Risk-Neutral Rates, Volatility Indices

Country of Incorporation	Stock Market Index	Risk-Neutral Rate
Australia	S&P/ASX 200 Index	Bank Bill Swap Rate - AUD - 3 Month
Austria	MSCI Austria Index	ICE LIBOR - EUR - 3 Month
Bahrain	MSCI Bahrain Index	World Bank Discount Rates - 3 Month
Belgium	Brussels BEL 20 Index	ICE LIBOR - EUR - 3 Month
Bermuda	S&P 500 Index	ICE LIBOR - USD - 3 Month
Brazil	MSCI Brazil Index	Brazil CDI - BRL - Overnight
Canada	S&P/TSX Composite Index	Canada T-Bills - CAD - 3 Months[1]
Cayman Islands	FTSE 100 Index	ICE LIBOR - GBP - 3 Month
China	Shanghai Composite Index	SHIBOR - CNY - 3 Month[2]
Denmark	OMX Copenhagen 20 Index	ICE LIBOR - EUR - 3 Month
Finland	OMX Helsinki 25 Index	ICE LIBOR - EUR - 3 Month
France	Paris CAC 40 Index	ICE LIBOR - EUR - 3 Month
Germany	Germany DAX Index	ICE LIBOR - EUR - 3 Month
Greece	ATHEX Composite Index	ICE LIBOR - EUR - 3 Month
Hong Kong	Hang Seng Inde	HIBOR - HKD - 3 Month
Iceland	OMX Iceland All Share Index	ICE LIBOR - EUR - 3 Month
India	Nifty 50 Index	LIBOR - INR - 3 Month[3]
Ireland	Ireland ISEQ Overall Index	ICE LIBOR - EUR - 3 Month
Italy	FTSE MIB Index	ICE LIBOR - EUR - 3 Month
Japan	Nikkei 225 Index	ICE LIBOR - JPY - 3 Month
Jersey	FTSE 100 Index	ICE LIBOR - GBP - 3 Month
Luxembourg	LuxX Index	ICE LIBOR - EUR - 3 Month
Malaysia	Kuala Lumpur Composite Index	KLIBOR - MYR - 1 Month[4]
Mexico	S&P/BMV IPC Index	World Bank Discount Rates - 3 Month

Table L.1 continued from previous page

Country of Incorporation	Stock Market Index	Risk-Neutral Rate
Netherlands	Amsterdam AEX Index	ICE LIBOR - EUR - 3 Month
New Zealand	S&P/NZX 50 Index	LIBOR - NZD - 3 Month[5]
Norway	Oslo OBX Index	NIBOR - NOK - 3 Month[6]
Panama	S&P 500 Index	ICE LIBOR - USD - 3 Month
Portugal	PSI-20 Index	ICE LIBOR - EUR - 3 Month
Qatar	QE Index	World Bank Discount Rates - 3 Month
Russia	MSCI Russia Index	World Bank Discount Rates - 3 Month
Saudi Arabia	Tadawul All Share Index	SAUDI IBOR - SAR - 3 Month[7]
Singapore	FTSE Straits Times Index	Singapore Government Debt - SGD - 2 Year
South Korea	SK Kospi Composite Index	South Korea Government Debt - KRW - 2 Year
Spain	Madrid Ibex 35 Index	ICE LIBOR - EUR - 3 Month
Sweden	OMX Stockholm 30 Index	STIBOR - SEK - 3 Month[8]
Switzerland	MSCI Switzerland Index	ICE LIBOR - CHF - 3 Month
Taiwan	Taiwan TAIEX Index	SHIBOR - CNY - 3 Month[9]
Turkey	Istanbul National 100 Index	LIBOR - TRY - 3 Month
United Arab Emirates	MSCI UAE Index	EIBOR - AED - 3 Month[10]
United Kingdom	FTSE 100 Index	ICE LIBOR - GBP - 3 Month
United States of America	S&P 500 Index	ICE LIBOR - USD - 3 Month

[1]For events 30, 33, and 35, ICE LIBOR - USD - 3 Month was used; [2]For events 22 and 23, World Bank Discount Rates - 3 Month was used; [3]For events 22 and 23, World Bank Discount Rates - 3 Month was used; [4]For events 22, 23, 174, and 178, World Bank Discount Rates - 3 Month was used; [5]For events 110 and 123, Australian Bank Bill Swap Rate - AUD - 3 Month was used; [6]For events 22, 23, and 178, ICE LIBOR - EUR - 3 Month was used; [7]For events 23 and 178, World Bank Discount Rates - 3 Month was used; [8]For events 22, 23, and 195, ICE LIBOR - EUR - 3 Month was used; [9]For events 22, 23, 189, World Bank Discount Rates - 3 Month was used; [10]For events 22 and 23, World Bank Discount Rates - 3 Month was used

Country of Incorporation	Volatility Index
Australia	S&P/ASX 200 VIX Index[1]
Austria	EURO STOXX 50 Volatility Index
Bahrain	CBOE Volatility S&P 500 Index (VIX)
Belgium	EURO STOXX 50 Volatility Index
Bermuda	CBOE Volatility S&P 500 Index (VIX)
Brazil	CBOE Brazil ETF Volatility Index[2]
Canada	CBOE Volatility S&P 500 Index (VIX)
Cayman Islands	EURO STOXX 50 Volatility Index
China	CBOE China ETF Volatility Index[3]
Denmark	EURO STOXX 50 Volatility Index
Finland	EURO STOXX 50 Volatility Index
France	EURO STOXX 50 Volatility Index
Germany	EURO STOXX 50 Volatility Index
Greece	EURO STOXX 50 Volatility Index
Hong Kong	HSI Volatility Index[4]
Iceland	EURO STOXX 50 Volatility Index
India	CBOE Volatility S&P 500 Index (VIX)
Ireland	EURO STOXX 50 Volatility Index
Italy	EURO STOXX 50 Volatility Index
Japan	CBOE Volatility S&P 500 Index (VIX)
Jersey	EURO STOXX 50 Volatility Index
Luxembourg	EURO STOXX 50 Volatility Index
Malaysia	CBOE Volatility S&P 500 Index (VIX)
Mexico	CBOE Brazil ETF Volatility Index[5]
Netherlands	EURO STOXX 50 Volatility Index
New Zealand	CBOE Volatility S&P 500 Index (VIX)
Norway	EURO STOXX 50 Volatility Index
Panama	CBOE Volatility S&P 500 Index (VIX)
Portugal	EURO STOXX 50 Volatility Index
Qatar	CBOE Volatility S&P 500 Index (VIX)
Russia	Moscow Exchange Volatility Index[6]
Saudi Arabia	CBOE Volatility S&P 500 Index (VIX)
Singapore	CBOE Volatility S&P 500 Index (VIX)
South Korea	CBOE Volatility S&P 500 Index (VIX)
Spain	EURO STOXX 50 Volatility Index

Table L.2 continued from previous page

Country of Incorporation	**Volatility Index**
Sweden	EURO STOXX 50 Volatility Index
Switzerland	EURO STOXX 50 Volatility Index
Taiwan	CBOE China ETF Volatility Index[7]
Turkey	EURO STOXX 50 Volatility Index
United Arab Emirates	CBOE Volatility S&P 500 Index (VIX)
United Kingdom	EURO STOXX 50 Volatility Index
United States of America	CBOE Volatility S&P 500 Index (VIX)

[1]For events 5, 17, 22, 23, 31, 33, 35, 42, 44, 46, 47, 73, 84, 86, 103, 106, 110, 111, and 189, VIX was used; [2]For events 45, 195, and 196, VIX was used; [3]For events 22, 23, 44, 46, 73, 84, and 106, VIX was used; [4]For events 35, 44, 46, and 73, VIX was used; [5]For events 30 and 35, VIX was used; [6]For events 22, 23, 44, 46, 73, 84, 106, and 195, VIX was used; [7]For events 22, 23, 42, 44, 46, 51, 73, 84, 106, and 189, VIX was used