Integration of Cyber Security Frameworks, Models and Approaches for Building Design Principles for the Internet-of-Things in Industry 4.0

Petar Radanliev, Dave De Roure *, Jason R.C. Nurse♣, Razvan Nicolescu, Michael Huth♦,
Stacy Cannady, Rafael Mantilla Montalvo †, *Oxford e-Research Centre, UK, david.deroure@oerc.ox.ac.uk,
petar.radanliev@oerc.ox.ac.uk, ♣ University of Oxford, UK, jason.nurse@cs.ox.ac.uk, ♦Imperial College London, UK,
r.nicolescu@imperial.ac.uk, m.huth@imperial.ac.uk, †Cisco Systems, USA, scannady@cisco.com

Abstract:

This research article reports the results of a qualitative case study that correlates academic literature with five Industry 4.0 cyber trends, seven cyber risk frameworks and two cyber risk models. While there is a strong interest in industry and academia to standardise existing cyber risk frameworks, models and methodologies, an attempt to combine these approaches has not been done until present. We apply the grounded theory approach to derive with integration criteria for the reviewed frameworks, models and methodologies. Then, we propose a new architecture for the integration of the reviewed frameworks, models and methodologies. We therefore advance the efforts of integrating standards and governance into Industry 4.0 and offer a better understanding of a holistic economic impact assessment model for IoT cyber risk.

Keywords: Industry 4.0., Internet of Things, case study, cyber security framework

1 Introduction

The term Internet-of-Things (IoT) usually refers to network-connected cyber-physical devices that can communicate and share data in different constraining environments. Such technologies often seriously increase safety risk and raise important ethical concerns. Integrating IoT devices and cyber security technology in the communications networks of critical infrastructure implies major ethical aspects that humans should be able to sense and understand, while benefiting of maximum possible levels of trust and privacy.

This concern is represented by the need different IoT verticals have to develop reliable cyber security frameworks to prevent abuse from malicious interventions, including those originated by organised crime, terror organisations or state-sponsored aggressors. Companies that are interested in obtaining new revenue streams from such data will pursue innovative and cost-effective ways to comply with these new regulations. Analysis of the complete economic impact of data compromise would empower the communications network providers to create clear, rigorous, industry-accepted mechanisms to measure, control, analyse, distribute and manage critical data needed to develop, deploy and operate cost-effective cyber security for critical infrastructure.

The aim of this research is to provoke a debate among practitioners and academics by offering new design principles for assessing the cyber risk from IoT in the context of I4.0. The research undertakes a holistic investigation of the cyber risk of IoT in Industry 4.0 (I4.0). Our research approach combines qualitative data extracted from secondary sources. The research applies case study research to derive with new design principles for assessing the economic impact of IoT cyber risks. We will work with five I4.0 cyber trends (IIC, DCMS, IVI, Industrie 4.0., NTI,), seven cyber risk frameworks (FAIR, CMMI, CVSS, ISO, NIST, Octave and TARA) and two cyber risk models (RiskLense and Cyber VaR). This promotes the adaptation of existing models and methodologies by presenting the strengths and weaknesses of the frameworks and models.

Secondly, we conduct a comprehensive literature review, focused on the way an increase in cyber security in IoT systems can minimise safety and security concerns and increase reliability, ethical acceptability and trust in this space. The documented process represents the design principles for mapping and optimising IoT cyber security and assessing its associated economic impact.

The new design principles reported here have two objectives. The first objective is to enable a quick and up-to-date overview of existing and emerging IoT advancements in the field of Industry 4.0 (I4.0), which includes cyber-physical systems, the Internet of things, cloud computing and cognitive computing [1]–[3]. The second objective is to capture and enable the adaptation of the best cyber security practices in industry.

1.1 Research plan

In Section 2 we present the research methodology. In Section 3 we propose the design principles by considering case studies of the main Industry 4.0 trends, cyber security frameworks and two cyber security quantitative models. In Section 4 we present the design principles for assessing the cyber risk of IoT in Industry 4.0. In Section 5 we discuss the new principles. In Section 6 we present the conclusions of the research.

2 Research methodology

The methods applied in this study consist of literature review and case study research. We use practical studies of major projects in the I4.0 to showcase recent developments of IoT systems in the I4.0 context. We need practical studies to bridge the gaps and overcome some of the limitations and to construct the relationship between IoT and I4.0. The design principles support the process of building a holistic IoT cyber risk impact assessment model.

3 Development of design principles

The design initiates with integrating best practices from the case analysis. To our knowledge, this represents the first I4.0 attempt to integrate the academic literature with I4.0 practical initiatives applied globally. The integration of existing models with case study of I4.0 national initiatives leads to a new set of techniques, such as comparison of the national initiatives in I4.0 in terms of cyber risk focus. These techniques imply contrasting national policies and efforts towards standardisation, which are not discussed in the existing literature. Therefore, we discuss the I4.0 initiatives in the context of major efforts in standards and governance (e.g. National Institute of Standards and Technology (NIST) and Factor Analysis of Information Risk (FAIR).

To map the evolution of Internet of Things (IoT) and its associated cyber risks for the Industry 4.0 sector, we correlate seven cyber risk frameworks with I4.0 cyber trends. These frameworks are: FAIR, CMMI, CVSS, ISO, NIST, Octave and TARA. The stated seven frameworks are related to assessing general cyber risks. The new approach aims to identify the related aspects of IoT cyber risks. We compare existing cyber security measures and standards (e.g. FAIR and NIST cyber security frameworks) to propose a new and improved design principles for calculating the economic impact of IoT cyber risk.

3.1 Understanding IoT in Industry 4.0 initiatives

The Industrial Internet Consortium [4], [5] promotes a fully connected and automated production line that brings the customer into the production process as a decision-maker, with the ability to adjust their preferences at the time of production. In addition, IIC supports highly automated (rules engines, protective overrides) and human operated (visualisation, intervention controls) usage environments. The IIC promotes Cloud-computing platforms and disaster recovery plans. However, disaster recovery plans are only mentioned once in a diagram, with no explanation on details or how it would be executed. Simply mentioning recovery planning, does not by default address the issue of having recovery planning in place.

The most recent UK report by Department for Culture, Media and Sport [6] focuses extensively on the cloud integration in I4.0. However, while some initiatives are supported with direct examples of how the strategy can be executed (e.g. cloud data centres from Amazon, IBM, and Microsoft; or the cloud skills initiative to train public service in digital skills and assure the development of larger cloud technology skills), other initiatives are not well defined. This could in some instances be beneficial, as loosely defined standards provide flexibility in evolving as requirements change. Nevertheless, practical implementations (see Table 1) show that a concrete area of focus is required for the integration of IoT in I4.0.

In addition, the DCMS [6] refers to digital real-time interoperable records for healthcare, and developing a real-time platform for sharing information on missing persons and suspects. This report on the UK digital industry covers the aspects of autonomous cognitive decisions in great detail, listing specific projects, programs and funding sources (listed in Table 1), but does not mention real-time CPS-IoT platforms for I4.0. The main area of concern for the DCMS (2016), is that it does not provide guidance on recovery planning. The report is strongly focused on Active Cyber Defence and General Data Protection of customer data, but ignores other key risks, such as risks of unexpected failure for which recovery planning is crucial as such failures cannot be anticipated in advance.

The recent Industrial Value Chain Initiative [7], [8] does not report concrete plans for real-time embedded systems or recovery plans. The German initiative; Industrie 4.0 [9] promotes cloud computing integration with the Internet of Services, and proposes cloud-based security networks, but fails to state recovery plans. The NIT initiative [10] represents a rather long-term forecasting for IoT and I4.0 and focuses on market network creations. This initiative contributes with new insights to I4.0 by arguing that market creation for new technologies is the key to the future businesses and supply chain integration in I4.0. However, the NIT forecasting does not assess the issues of real-time cloud networks, and critically, does not provide suggestions for recovery planning mechanisms.

IoT in I4.0				
I4.0 cyber trends	IoT Cloud in I4.0	Real-time IoT in I4.0	Autonomous cognitive IoT in I4.0	Recovery plans for IoT in I4.0
IoT cyber elements for I4.0				
IIC, 2016	Cloud-computing platforms.	Adapt businesses and operational models in real time; Customised product offers and marketing in real time.	Fully connected and automated production line; Support highly automated environments.	Disaster recovery.
DCMS, 2016	Cloud technology skills; Cloud computing technologies; Cloud data centres; Cloud-based software; Cloud-based computing; Cloud guidance.	Digital real-time and interoperable records; Platform for real-time information.	UK Robotics and Autonomous Systems; Support for robotics and artificial intelligence; Encourage automation of industrial processes; Active Cyber Defence.	Not discussed
IVI, 2017	Cloud enabled monitoring; Integration framework in cloud computing.	Not discussed	Factory Automation Suppliers and IT vendors; Utilisation of Robot Program Assets by CPS.s	Not discussed
Industrie 4.0, 2013	CPS automated systems; Automated conservation of resources.	Cloud computing; Cloud-based security networks.	Automated production; Automated conservation of recourses.	Not discussed

NTI, 2015	Not discussed	Not discussed	Artificial intelligence and control systems	Not discussed

Table 1: IoT in I4.0 cyber trends

3.2 Conclusions from the case study of I4.0 initiatives

Research shows that global sharing of existing innovation testbeds (22 US testbeds from IIC; 11 UK catapults; over 500 projects in Germany), would reduce cost and enable faster product to market process. Global sharing is also needed for the IoT key markets, bringing into focus the G20 initiative policy key point for trade liberalisation [11]. The second policy of the G20 initiative (the elimination of subsidies) is somewhat confusing. While there is a compelling argument for the elimination of subsidies in the traditional industries, the concept of I4.0 requires technologies that are still in the infant stage of research and development. Economic policy dictates that infant industries need state support, hence emerging digital technologies also require state support. On the other hand, the NTI guiding principle [10] for focusing on market development is designed to reduce substantially any financial involvement of the state. The NTI policy approach would address the second G20 policy key point 'the elimination of subsidies' [11]. The most concerning finding from the case study is the lack of clarity on disaster recovery plans. Recovery planning is somewhat blurred and this is of concern as in the literature the recovery planning is strongly emphasised.

3.3 Reflecting on cyber risk standards and cyber risk models

A key part of understanding the risks and issues facing the IoT and I4.0 involves reflecting on the standards and models present today. In what follows, we reflect on seven cyber risk standards and two cyber risk models.

The Factor Analysis of Information Risk [12] promotes a standard quantitative risk model for information security and operational risk. In practice, FAIR represents a framework for understanding, measuring and analysing information risk in financial terms. The FAIR model is complementary to existing risk frameworks and applies knowledge from existing quantitative models, such as RiskLens [13], and Cyber VaR [14].

Next, the Capability Maturity Model Integrated (CMMI) [15] is examined. CMMI integrates five levels of the original Capability Maturity Model (CMM) [16]. However, this model does not provide guidance on disaster and recovery planning.

The Common Vulnerability Scoring System (CVSS) [17] provides 'Modified Base Metrics' for assigning metric values to real vulnerabilities. The 'Modified Base Metrics' represent a severity group (low, medium, high, critical), associated with a mathematical approximation of metric combinations ranked in order of severity. CVSS works on assembling standards, guidelines, and practices that are working effectively in industry.

The International Organisation for Standardisation [18] is an international standard-setting body. The ISO 27032 is a framework for collaboration that provides specific recommendations for cyber security. ISO 27001 sets requirements for organisations to establish an Information Security Management System (ISMS). Notable for this discussion, ISO 27031 provides recommendations for disaster recovery. The other frameworks (in Table 2) and the cyber risk models (Table 3) should integrate the conclusions from the ISO framework.

The National Institute of Standards and Technology's [19] Cyber Security Framework (NIST, 2014) organises cyber security activities in five categories: Identify, Protect, Detect, Respond, and Recover. The recovery category differentiates this framework from all other frameworks. The NIST framework recognises the importance of recovery planning and suggest the development, implementation and maintenance of plans for timely recovering and restoring any capabilities or services that were impaired by a cyber-attack.

Another approach is OCTAVE, which stands for Operationally Critical Threat, Asset, and Vulnerability Evaluation method [20]. This is a qualitative method for measuring cyber risk through workshops. The OCTAVE method recommends three levels of recovery (low, medium, high), but fails to provide a quantification method for calculating the required level of recovery. Hence, one way to regard OCTAVE is as a guide for researchers measuring cyber risks.

The Threat Assessment & Remediation Analysis (TARA) [21] is a qualitative analytical model that applies threat matrix and standardised template to record system threats. TARA promotes and somewhat facilitates the identification of appropriate recovery options, but fails to quantify the impact of cyber risks, which is crucial for deciding on appropriate recovery planning.

Risk Frameworks:	FAIR	CMMI	CVSS	ISO	NIST	Octave	TARA
How to measure risk:	Financial model	Combine /integrate capability maturity models	Modified Base Metrics	ISO 27032	Categorising risk	Workshops	Threat Matrix
How to standardise risk:	Complementary	Reflected in ISO 15504 - SPICE	Mathematical approximation	ISO 27001	Assembling standards, guidelines, and practices	Encouraging institutionalisation and repeatability	Using standard template to record system threats
How to compute risk:	Quantitative	Staged representation with five maturity levels	Qualitative Severity Rating Scale	Compliance based	Compliance based	Guide and training - qualitative	Qualitative analytical
Disaster and recovery planning:	Acceptable level of exposure	N/A	N/A	ISO 27031	Recovery Planning; Improvements; and Communications	Recovery impact areas	Promotes and facilitates system recovery

Table 2: Leading Cyber Risk Frameworks

3.4 Findings from the leading cyber risk frameworks

Findings for the reviewed frameworks can be summarized as follows:

- The FAIR promotes a quantitative, risk based, acceptable level of loss exposure.
- The CMMI and CVSS do not discuss disaster and recovery planning.
- The ISO promotes a standard for disaster recovery.
- NIST is the most advanced framework in terms of disaster and recovery planning and it provides recommendations on recovery planning, improvements and communications.
- The OCTAVE developed a standardised questionnaire to investigate and categorise recovery impact areas.
- TARA promotes and facilitates system recovery, but does not provide a detailed methodology for disaster and recovery planning.

Beyond these issues, research has highlighted other challenges in adopting existing cyber risk frameworks for dynamic and connected systems, where the IoT presents great complexities For example the the high degrees of connectivity in coupling of digital, cyber-physical, and social systems [22].

3.5 Comparing two Quantitative Risk Models – RiskLens and Cyber VaR

The two cyber risk assessment models promoted by the World Economic Forum (Cyber VaR) and the FAIR institute (RiskLense) are analysed to compare the similarities and differences. The two approaches are selected for comparison because both are promoted as a standardised quantitative reference models for assessing cyber risks.

Quantitative Risk Models:	RiskLens	Cyber VaR
How to measure risk:	BetaPERT distributions	VaR
How to standardise risk:	Adopt FAIR	World Economic Forum
How to compute risk:	Quantitative risk analytics with Monte Carlo and sensitivity analysis	Quantitative risk analytics with Monte Carlo
Disaster and recovery planning:	Not included	Not included

Table 3: Quantitative Cyber Risk Models

The main difference between the two models is that RiskLense uses BetaPERT distributions [13] and the Cyber VaR is based on the Value at Risk model [14], [23]–[25]. Both models use Monte Carlo simulations for assessing cyber risk with minimal data sets, and both models are focused on loss exposure, loss event frequency and vulnerability. The two models do not assess the precise cost of recovery, but for the cyber insurance purposes, the loss exposure and loss event frequency can be used to calculate the potential cost of recovery.

4 Proposed design principles

We propose a new set of design principles for assessing the cyber risk from IoT integration into I4.0. The principles derived from the qualitative case study. The case study of IoT in I4.0 (Table 1) shows that I4.0 trends have failed to implement the recovery planning in the leading national initiatives. This is in contradiction with the findings from the second reflection of the leading cyber risk frameworks (Table 2), where the recovery planning is strongly emphasised (*see:* ISO, FAIR, NIST, Octave, TARA). It seems that the leading national I4.0 initiatives have ignored the recommendations from the world leading cyber risk frameworks. A new model for IoT in I4.0 should firstly consider the findings from the I4.0 trends, secondly the recommendations from the leading cyber risk frameworks. To identify the cost of recovery planning or the cost of cyber insurance, a new quantitative model is needed that would be applicable to IoT cyber risks.

There are currently two leading quantitative cyber risk models. First is the RiskLens approach, promoted by FAIR. Second is the Cyber VaR, promoted by the World Economic Forum, Deloitte and more recently by FAIR. The unifying link between the two cyber risk models is the application of Monte Carlo simulations for predicting cyber risk uncertainty.

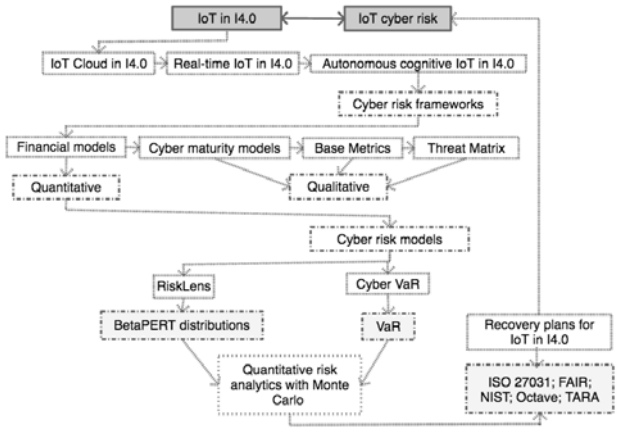

Figure 1: Design principles for assessing IoT cyber risks in I4.0

From the case study, it appears that a new impact assessment model for the cyber risks from IoT integration into I4.0, should start with the guidance from RiskLense and Cyber VaR. The application of Monte Carlo simulation would reduce the IoT cyber risk uncertainty and enable the approximation and estimation of the economic impact of cyber risk from IoT devices. Such calculation would enable companies to develop appropriate recovery planning and the insurance industry to provide a more realistic cost of cyber insurance.

The proposed design principles suggest anticipating recovery planning in the assessment of economic impact of IoT cyber

risk. Such approach would enable cyber insurance companies to value the impact of IoT cyber risks in I4.0. The rationale of the proposed design principles is that without appropriate recovery planning, the economic impact can be miscalculated, resulting in greater losses than we anticipated initially. The design principles in Figure 1 are developed to advance the existing efforts (from the World Economic Forum, Deloitte, FAIR, etc) in developing a standardised quantitative approach for assessing the impact of cyber risks.

5 Discussion

The lack of disaster and recovery planning is consistent in all the I4.0 initiatives reviewed. Adding to this, the new risks emerging from IoT connected devices and services, and the lack of economic impact assessments from IoT cyber risks, makes it imperative to emphasise the lack of recovery planning in the leading I4.0 initiatives. The volume of data generated by the IoT devices creates diverse challenges in variety of verticals (e.g. machine learning, ethics, business models). Simultaneously, to design and build cyber security architecture for complex coupled IoT systems, while understanding the economic impact, demands bold new solutions for optimisation and decision making [22]. Much of the research is application-oriented and by default interdisciplinary, requiring hybrid research in different academic areas. This enabled the design of cyber security architectures that integrate economic impact assessment in IoT verticals, that meet public acceptability, security standards, and legal scrutiny.

6 Conclusion

This paper combines existing literature in order to derive common approaches and to incorporate existing standards. This result with mapping of the existing initiatives, frameworks and methods for assessing the impact of cyber risk This results with a new set of design principles supported with a new set of design criteria, specific for cyber risk from the IoT. The proposed design principles present recommendations for cyber security recovery improvements. The design principles enable the visualisation of IoT cyber risk and inform organisations in this space of best practices.

The new design principles map interactions among different factors in the IoT devices, and derive new sets of cyber security assessment criteria. The design principles described here can be used for assessing the economic impact of IoT compromises and to make recommendations for IoT devices. The design principles are also relevant to national and international I4.0 networks, specifically for building recovery planning.

6.1 Areas for further research

In order to design the proposed new impact assessment model, research should focus on: IoT economic impact, IoT machine ethics, IoT sensor networks, IoT safety, IoT cyber security and IoT equipment combined. The nature of such interdisciplinary research would benefit the advancements of smart city design, intelligent transport design, smart grid design and individual industries and services (e.g. commercial and industrial IoT equipment), by bridging gaps between cyber risk and economic value. The research will benefit the literature by integrating economic impact and cyber risk assessment models that have not been previously considered in combination.

This work was supported by the UK EPSRC with project [grant number EP/N02334X/1 and EP/N023013/1] and by the Cisco Research Centre [grant number 2017-169701 (3696)].

7 References

[1] S. Weyer, M. Schmitt, M. Ohmer, and D. Gorecky, “Towards Industry 4.0 - Standardization as the crucial challenge for highly modular, multi-vendor production systems,” *IFAC-PapersOnLine*, vol. 48, no. 3, pp. 579–584, 2015.

[2] M. of E. I. and C. A. MEICA, “Industria Conectada 4.0: La transformación digital de la industria española Dossier de prensa,” Madrid, 2015.

[3] Y. Liao, F. Deschamps, E. de F. R. Loures, and L. F. P. Ramos, “Past, present and future of Industry 4.0 - a systematic literature review and research agenda proposal,” *Int. J. Prod. Res.*, vol. 55, no. 12, pp. 3609–3629, Jun. 2017.

[4] I. I. C. IIC, “The Industrial Internet of Things Volume G5: Connectivity Framework,” 2017.

[5] I. I. C. IIC, “The Industrial Internet of Things, Volume B01: Business Strategy and Innovation Framework,” 2016.

[6] M. and S. DCMS, Department for Culture, “UK Digital Strategy 2017 - GOV.UK,” London, 2017.

[7] I. V. C. I. IVI, “Industrial Value Chain Reference Architecture,” Hannover, Germany, 2017.

[8] IVI. Industrial Value Chain Initiative, “An Outline of Smart Manufacturing Scenarios 2016,” in *Monozukuri Nippon Conference*, 2016.

[9] W. Wahlster, J. Helbig, A. Hellinger, M. A. V. Stumpf, J. Blasco, H. Galloway, and H. Gestaltung, “Recommendations for implementing the strategic initiative INDUSTRIE 4.0,” Federal Ministry of Educationand Research, 2013.

[10] A. for strategic initiatives ASI, “National Technology initiative, Agency for Strategic Initiatives,” *Government of Russia*, 2016. [Online]. Available: https://asi.ru/eng/nti/. [Accessed: 10-May-2017].

[11] G20, “G20 New Industrial Revolution Action Plan,” 2016.

[12] FAIR, “Quantitative Information Risk Management | The FAIR Institute,” *Factor Analysis of Information Risk* , 2017. [Online]. Available: http://www.fairinstitute.org/. [Accessed: 26-Dec-2017].

[13] RiskLens, “Risk Analytics Platform | FAIR Platform Management,” 2017. [Online]. Available: https://www.risklens.com/platform. [Accessed: 26-Dec-2017].

[14] FAIR, “What is a Cyber Value-at-Risk Model?,” 2017. [Online]. Available: http://www.fairinstitute.org/blog/what-is-a-cyber-value-at-risk-model. [Accessed: 26-Dec-2017].

[15] CMMI, “What Is Capability Maturity Model Integration (CMMI)®? | CMMI Institute,” *CMMI Institute*, 2017. [Online]. Available: http://cmmiinstitute.com/capability-maturity-model-integration. [Accessed: 26-Dec-2017].

[16] U.S. Department of Energy, “Cybersecurity Capability Maturity Model (C2M2) | Department of Energy,” Washington, DC, 2014.

[17] CVSS, “Common Vulnerability Scoring System SIG,” *FIRST.org*, 2017. [Online]. Available: https://www.first.org/cvss/. [Accessed: 26-Dec-2017].

[18] ISO, “ISO - International Organization for Standardization,” 2017. [Online]. Available: https://www.iso.org/home.html. [Accessed: 26-Dec-2017].

[19] NIST, “Framework for Improving Critical Infrastructure Cybersecurity,” 2014.

[20] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, “Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process,” Hansom AFB, MA, 2007.

[21] J. Wynn, G. Whitmore, L. Upton, D. Spriggs, R. McKinnon, R. McInnes, L. Graubart, and J. Clausen, “Threat Assessment & Remediation Analysis (TARA) Methodology Description Version 1.0,” Bedford, MA, 2011.

[22] J. R. C. Nurse, S. Creese, and D. De Roure, “Security Risk Assessment in Internet of Things Systems,” *IT Prof.*, vol. 19, no. 5, pp. 20–26, 2017.

[23] J. Buith, “Cyber Value at Risk in the Netherlands,” 2016.

[24] K. Ruan, “Introducing cybernomics: A unifying economic framework for measuring cyber risk,” *Comput. Secur.*, vol. 65, pp. 77–89, 2017.

[25] V. Jacobs, J. Bulters, and M. Van Wieren, “Modeling the Impact of Cyber Risk for Major Dutch Organizations.”