A Success Model for Cyber Threat Intelligence Management Platforms

Adam Zibak[1a], Clemens Sauerwein[b], Andrew Simpson[a]

[a]*Department of Computer Science, University of Oxford*
Wolfson Building, Parks Road, Oxford OX1 3DQ, UK
firstname.lastname@cs.ox.ac.uk
[b]*Department of Computer Science, University of Innsbruck*
ICT Building, Technikerstraße 21a, A-6020 Innsbruck, Austria
firstname.lastname@uibk.ac.at

Abstract

The increasingly persistent and sophisticated threat actors, along with the sheer speed at which cyber attacks unfold, have made timely decision making imperative for ensuring the continued security of most organisations. Consequently, threat intelligence management platforms have been widely adopted to assist organisations in creating and participating in inter-organisational sharing efforts to protect against cyber attacks. Measuring the effectiveness and success of these platforms is critical to understanding how such products and services should be designed, implemented and used. Nevertheless, it is a fact that research and practice lack a common understanding of factors influencing the success of threat intelligence management platforms. To investigate these issues, we adopted the DeLone and McLean information system success model to threat intelligence sharing and employed a survey-based approach to collect data from 152 security professionals for its empirical assessment. Subsequently, we identified several factors that are decisive for the organisational success of a threat intelligence management platform.

Keywords: Cyber Threat Intelligence, Platform, User Satisfaction, Survey Research, Success Model

[1]Corresponding author

1. Introduction

The increasing complexity and diversity of organisational information systems, combined with the growing number and sophistication of cyber attacks, pose serious threats to organisational security. Recent high-profile security incidents have shown that organisations are facing a wide spectrum of possible attacks and the time frame to put appropriate countermeasures in place is limited [1]. In order to ensure the confidentiality, integrity and availability of organisational services and information, timely decision making is imperative [2].

Consequently, the collection, processing and exchange of cyber threat intelligence — which can be defined as any security-related information that supports or steers organisational decisions [3] — has become a major trend [4]. However, not every organisation has the resources or knowledge to develop an independent threat intelligence programme [5, 6]. As a result, several threat intelligence management platforms (TIMPs) have been adopted to assist organisations in building and engaging in cyber security information sharing efforts [7]. Such platforms facilitate information sharing, assist with automation, and facilitate the generation, processing and validation of data [2].

Despite the fact that threat intelligence management platforms are used in security operations centres and large companies, research and practice lack a common understanding of the factors influencing the success of threat intelligence platforms. Measuring the effectiveness and success of these platforms is critical to understanding how such products and services should be designed, built, implemented and used. The effectiveness of a threat intelligence management platform at an organisation could also be indicative of the success of the organisation's overall threat intelligence sharing practice.

Previous research has identified different maturity levels of threat management platforms [8], investigated its integration into information security management processes [9], developed evaluation criteria to assess them [10, 11], and evaluated its impact on the productivity and performance of cyber security analysts [12]. However, there have been no attempts to model the success of threat intelligence management platforms.

Accordingly, we developed and validated a comprehensive multidimensional success model for determining the success of a threat intelligence management platforms. To this end, we drew inspiration from DeLone and McLean (D&M) whose interdependent and multi-construct view of information systems success is widely accepted and has been applied to a variety of

contexts including information security practices [13, 14, 15].

Two main considerations guided the design and operationalisation of our model. First, to maximise its usefulness, the model has to be complete and parsimonious — which is to say that it should consolidate previous work in the field, while remaining simple enough to preserve its explanatory value regardless of the complexity of its real-world applications [14]. Secondly, the model has to capture and integrate the characteristics of threat intelligence managements platforms while retaining as much as possible of the richness of the D&M model. Accordingly, we expanded the D&M information system success model by adding additional constructs (e.g. perceived trust) in order for it to be applicable to threat intelligence management platforms. To accomplish this, we developed and tested 13 hypotheses based on the relationships of the model's constructs.

The remainder of this paper is structured as follows. Section 2 discusses background information and related work on information systems success models and threat intelligence management platforms. Section 3 introduces the research model and briefly describes its constructs and the associated hypotheses. Section 4 outlines the applied research methodology. Section 5 analyses and discusses the results of the research model's empirical validation. Section 6 examines those results and their implications for research and practice. Section 7 presents the study's limitations and gives consideration to potential areas of future work. Finally, Section 8 provides a summary of the findings of this paper.

2. Background and related work

In order to capture the complex, interdependent and multi-dimensional nature of information system success, DeLone and McLean (D&M) proposed a model for information system success [13]. The initial model was subsequently subjected to close scrutiny including a number of modifications [16, 17]. In subsequent work, DeLone and McLean examined these suggestions and revised their original model accordingly [14]. The updated version, as shown in Figure 1, extended the concept of quality to include *service quality* in addition to information and system quality as antecedents of use and user satisfaction. The use construct was also further clarified in the new model by adding the *intention to use* construct to measure the user's attitude. A third and final refinement to the model stemmed from the argument that the impact of an information system can stretch beyond the individual and

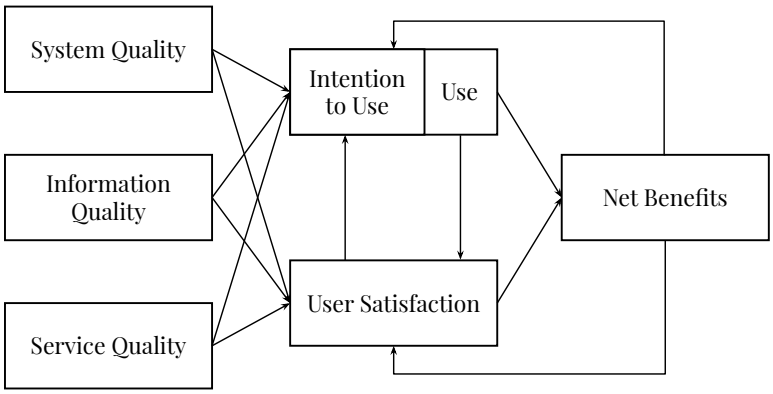

Figure 1: DeLone and McLean's updated information systems success model [14].

organisational levels [18]. The revised model therefore substituted individual impact and organisational impact with *net benefits* to account for benefits occurring on multiple levels of analysis [19]. The revised model consisted of six main constructs [14]. We summarise these constructs below.

- *Information quality* captures the desirable characteristics of the system's output or content.
- *System quality* refers to the desirable characteristics of the information system itself.
- *Service quality* refers to the quality of the support users receive from the provider's support personnel.
- *Use* denotes the extent to which the system's capabilities has been adopted by the staff or customers.
- *User satisfaction* refers to the users' level of satisfaction throughout their interaction with the system.
- *Net benefits* refers to the degree to which the system is contributing to the overall success of its users, departments, organisations, industries or societies, depending on the context and level of analysis.

As shown in Figure 1, the model suggests that information, system and service quality influence use and user satisfaction, while the latter two constructs influence each other and the net benefits of system. The net benefits construct, in turn, influences user satisfaction and the use of the system [14].

The revised model has since been utilised as a framework to guide and organise measuring success factors in information systems [19]. However, determining success constructs and the associated metrics depends on the specific nature and objectives of the system being assessed [20]. The DeLone and McLean model is widely accepted and has been applied to a variety of contexts including information security practices [13, 14, 15], knowledge management systems [21, 22], e-commerce systems [23], e-government systems [24], and employee portals [25].

Existing research in the field of threat intelligence management platforms has tended to focus on *opportunities, requirements and challenges* [26, 27, 4, 28, 29, 8], *legal and regulatory aspects* [30, 31], *standardisation efforts* [32, 33, 34, 35, 36, 37, 38, 39], *implementation details* [40, 41, 5, 2, 4, 42, 43], and *aspects of organisational integration and processes*. The last of these includes papers that examine aspects regarding the integration of threat intelligence sharing and its platforms into organisational processes, policies and decisions [8, 7, 44, 9, 45]. There has been some recent research giving consideration to criteria and methodologies to evaluate threat intelligence sharing platforms from an organisational perspective [10, 11].

Examining the threat intelligence sharing literature reveals that there is no common understanding of the success of threat management platforms. Therefore, this contribution extends the state-of-the-art by providing a comprehensive analysis of different success factors of threat intelligence management platforms, as well as the relationships between them.

3. Research model

In this section we outline and discuss our threat intelligence management platform (TIMP) success model that builds on and adapts the refined D&M model of [14]. The model is shown in Figure 2 and consists of the six main success constructs of the D&M model — content quality, system quality, service quality, use, user satisfaction, and net benefits — as well as the newly added construct: perceived trust. Our model uses content quality instead of information quality in order to capture the richness and diversity of the TIMP's content. The arrows between the constructs represent temporal and causal relationships, with each corresponding to a hypothesis. We decided not to include the feedback loop found in the D&M model for the sake of simplicity and in order to minimise the time needed to participate in the resulting

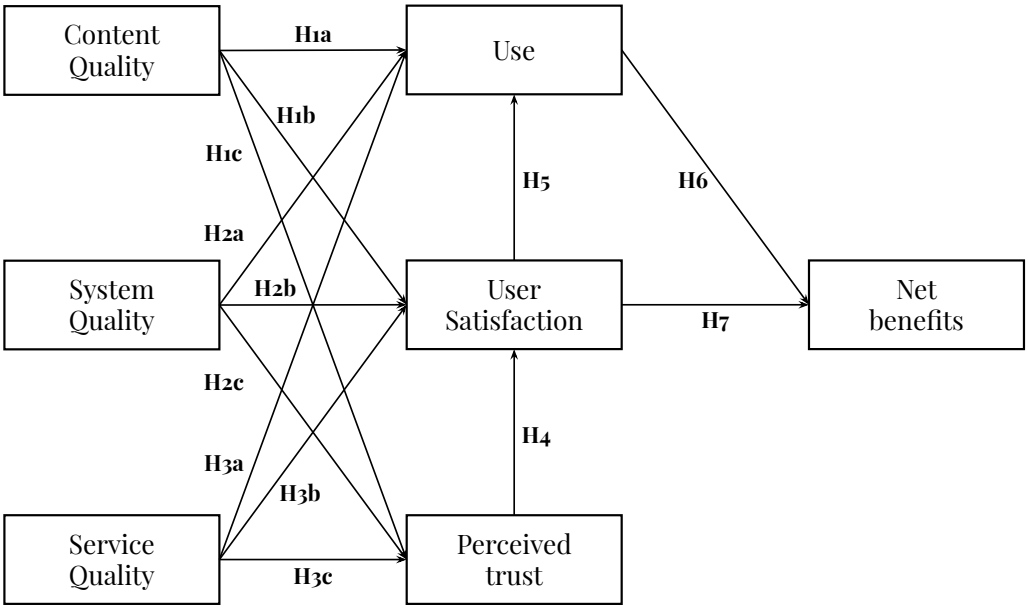

Figure 2: Our research model.

survey. Section 3.1 examines the constructs and their operationalisation and Section 3.2 presents the associated hypotheses and the rationale behind them.

3.1. Constructs

In developing our model's constructs, we examined the definition of each of the success factors in the D&M model, contrasted them with the specific features and objectives of threat intelligence management platforms, and incorporated the relevant concepts that appear in the literature. This process resulted in a theoretical model that comprises the following seven constructs. (Table 1 provides an overview of these constructs.)

3.1.1. Content quality

Guided by DeLone and McLean's characterisation of information quality as a content issue, our model attempts to capture the quality of threat intelligence in a construct labelled *content quality*. This is the quality of the information available through the platform, which includes indicators of compromise, incident reports, country and threat actor profiles, lessons learnt and so forth, in structured and unstructured formats. Despite its similarity to the information quality construct in D&M's model, the content

quality construct in our model is adapted to be a broader construct aimed at capturing the richness and diversity of the TIMP's content.

We measure the content quality construct using the findings of our previous work. In [46], we reported that a Delphi panel of 30 threat intelligence practitioners agreed on seven dimensions to measure the quality of threat data and intelligence. Six of these dimensions are content-related, namely: accuracy, actionability, provenance, relevance, reliability and timeliness.

3.1.2. System quality

The *system quality* construct captures the performance and functionality of the system itself by measuring the extent to which it is technically sound and has the desirable characteristics [19]. When the users are the vendor's customers, as opposed to its employees — as is the case with most threat intelligence management solutions — their use of the system is usually volitional [14]. This means that unsatisfactory usability, functionality or responsiveness could discourage customer usage of that system.

Although system quality has been commonly determined using the simplified ease of use measure, some studies have found that perceived ease of use does not fully represent the system quality construct [19]. Instead, an increasing number of researchers have developed and tested their own instruments using dimensions adapted from the original D&M model [13] or through an independent review of relevant system quality literature [19].

Based on our review of the literature concerning the function and characteristics of threat intelligence management platforms, our system quality scale includes the interoperability, functionality, reliability and usability of the system based on the findings of [25] and [46].

3.1.3. Service quality

Service quality is generally described as how well a delivered service matches customer expectations [50]. In our context, service quality is a subjective assessment of the quality of the user-vendor interaction including the extent to which specific service needs have been met [15]. Measures of information system effectiveness usually focus on the products instead of the services of the information system function [16]. Therefore, adding service quality to the assessment model has the potential to result in a more accurate and balanced measure of the system's effectiveness.

The multi-dimensional nature of the service quality construct is often captured using the SERVQUAL instrument [51]. This is adapted from marketing

Construct	Operational definition	Dimensions
Content quality (CONQ)	The extent to which data and intelligence retrieved from the TIMP meets the requirements and expectations of the user.	Accuracy[a] Actionability[a] Provenance[a] Relevance[a] Reliability[a] Timeliness[a]
System quality (SYSQ)	The extent to which the TIMP itself possesses desired characteristics and is technically sound.	Interoperability[a] Functionality [25] Reliability [25] Usability [25]
Service quality (SERQ)	The extent to which the services provided by the TIMP vendor meet the user's needs or expectations.	Assurance [14, 19] Empathy [14, 19] Reliability [14, 19] Responsiveness [14, 19]
Perceived trust (PT)	The extent to which the user believes that the TIMP is safe and secure.	Compliance [47] Security [47] Overall Trust [47]
Use (USE)	The extent to which the users actually use TIMP in performing their tasks.	Analysis [2] Collection [2] Dissemination [2]
User satisfaction (USAT)	The extent to which the user is satisfied with their interaction with the TIMP.	Adequacy [48] Effectiveness [48] Efficiency [48] Overall satisfaction [48]
Net benefits (NETB)	The extent to which the use of the TIMP benefits the organisation as a whole.	Improved breach detection[b] Enhanced resilience[b] Improved intelligence validation[b] Improved incident response[b] Improved situational awareness[b]

Table 1: The definition and operationalisation of the proposed model's constructs.

[a] adopted from [46].
[b] adopted from [49].

research and is designed to measure consumers' expectations and perceptions of a service. SERVQUAL has been found to be a valid and satisfactory measure of information systems service quality [52]. Therefore, our model adopts the SERVQUAL approach by measuring the service quality construct along SERVQUAL's dimensions: reliability, responsiveness, assurance, and empathy [14, 19].

3.1.4. Perceived trust

In addition to the quality of the content, system and service, users' disposition towards security and compliance issues such as privacy and data protection could influence their overall satisfaction with the TIMP. The extent to which a vendor is able to ensure that TIMP installation and utilisation can be carried out securely without any intrusion or disruption is an important consideration that might affect the customers' satisfaction. This observation is in line with Molla and Licker's argument in [47] that user trust usually refers to two main issues: security and privacy.

The literature on trust in threat intelligence focuses on the establishment of trust between members of a sharing group [6, 53]. In the context of our research, the *perceived trust* construct refers to the confidence TIMP users have that the system and the party behind the system have adequate security and are consistent with relevant data protection regulations such as the EU's General Data Protection Regulation (GDPR). Moreover, due to the complex nature of the concept of *trust* (e.g. trust in content, trust between sharing groups, trust in platform provider) in the context of TIMPs and keeping the model at the same level of abstraction, we decided to make an abstraction of the dimension of trust based on the assessment of the overall trust. Therefore, in our study we adopted a scale that consisted of three dimensions: security, compliance and overall trust in the platform.

3.1.5. Use

The *use* of an information system has been widely accepted as an important success measure in IS research [14]. However, the actual use, as an indicator of success, only makes sense when the use of the system is voluntary. The use of threat intelligence platforms is largely voluntary and therefore we decided to adopt the construct in our model in its original form.

Due to the complex nature of the use construct, empirical studies have employed a range of subjective and objective measures including frequency of use, intention to use, self-reported use and actual use [14, 19]. However,

as Doll and Torkzadeh note in [54], a multi-dimensional measure of system use that is based on the nature or purpose of the system provides a better understanding of how a system is utilised.

We follow Doll and Torkzadeh's [54] recommendation in operationalising the use construct in our model. The dimensions were extracted from Dandurand and Serrano's [2] summary of a threat intelligence management platform objectives. According to their characterisation, a TIMP facilitates information sharing, enables automation, and facilitates the generation, refinement and vetting of data through burden sharing collaboration or outsourcing [2].

3.1.6. User satisfaction

User satisfaction generally refers to the extent to which the users believe that a particular system they use meets their information requirements [55]. Given that determining the effectiveness of information systems is in most cases difficult to measure, user satisfaction with the system has been widely accepted as a potentially measurable substitute for evaluating the utility and effectiveness of the system in decision making [55]. The majority of usability studies have also included user satisfaction measures [56].

Several approaches have been used to measure the user satisfaction construct. The first approach uses single-item rating to measure overall satisfaction with an information system [57]. This approach has been found to provide limited information about what the user finds dissatisfying or satisfying and has therefore been deemed unreliable. Conversely, the second approach employs multiple-item semantic differential scale and has become increasingly common [55]. In our study we adopt the latter approach by employing a scale proposed by Seddon and Yip in [48], which consists of four dimensions: adequacy, efficiency, effectiveness, and overall satisfaction with the platform.

3.1.7. Net benefits

The *net benefits* construct is the final dependent variable in our model and aims to capture the overall beneficial outcomes of the use of an information system [20]. DeLone and McLean [2] introduced the construct in their revised success model based on their belief that the impacts of information systems are no longer limited to the immediate user, but they include other entities such as the industry and society.

In developing the net benefits measuring instrument, we rely on the findings of [49], in which the benefits of threat-centric information sharing were captured. This was achieved by selecting the questionnaire statements that focused on the benefits of threat-centric sharing and achieved more than 50% agreement by the participants after excluding neutral responses. Seven statements met the criteria. However, it is important to make sure that the person assessing the benefits is in a position and has the required knowledge to answer the questions [19]. Therefore, we decided to exclude two of the seven statements since only managers or highly experienced professionals would be able to evaluate them accurately. The process resulted in the adoption of the following set of statements concerning the benefits of threat intelligence sharing: it supports incident response efforts; it contributes to breach detection and recovery; it enhances defensive agility and resilience; validates and complements other sources of intelligence; and it improves overall security posture and situational awareness.

3.2. Hypotheses

Using the findings of DeLone and McLean [14] and related studies [19, 47, 48, 51], as well as the additional success dimensions, we present a theoretical model which assumes that content, system and service quality, as well as perceived trust, are associated with the TIMP's user satisfaction and usage. We also propose that the latter two, in turn, have an impact on the platform's net benefits to the organisation.

Our model's hypothesised relationships are mostly based on the D&M success model. We also expect the newly added success dimension *perceived trust* to have an impact on some of the model's other constructs.

We expect that each of content, system and service quality has a role to play in establishing and maintaining users' trust in the platform. The three quality constructs will also influence the use of the platform. We therefore hypothesise that the higher the platform's content, system and service quality are, the more trust users have in the platform and the more likely they are to use it. We also hypothesise that the more trust users have in the platform, the more satisfied they are with it. We expect that the user's satisfaction with and use of the platform will influence the overall benefits of employing the system. This results in a set of hypotheses to be tested, as shown in Table 2.

Recalling Figure 2, we find that each of the the arrows represents one of the hypotheses to be tested. We transformed the theoretical model into a

H1.a	Content quality has a positive influence on the use of a TIMP.
H1.b	Content quality has a positive influence on user satisfaction with a TIMP.
H1.c	Content quality has a positive influence on user trust in a TIMP.
H2.a	System quality has a positive influence on the use of a TIMP.
H2.b	System quality has a positive influence on user satisfaction with a TIMP.
H2.c	System quality has a positive influence on the perceived trust.
H3.a	Service quality has a positive influence on the use of a TIMP.
H3.b	Service quality has a positive influence on user satisfaction with a TIMP.
H3.c	Service quality has a positive influence on the perceived trust.
H4	Perceived trust has a positive influence on user satisfaction with a TIMP.
H5	User satisfaction has a positive influence on the use of a TIMP.
H6	TIMP use has a positive influence on the net benefits of the platform.
H7	User satisfaction has a positive influence on the net benefits of the TIMP.

Table 2: Research hypotheses.

structural equation model (SEM), which we tested empirically.

4. Research methodology

In line with the established practices of information system success studies [25], we developed and employed a survey-based approach to collect the data required for the empirical assessment of our theoretical success model. Quantitative methods are generally preferred to qualitative research when it comes to hypotheses testing [58].

4.1. Research instrument

Our primary measurement tool was a self-administered questionnaire based on previous empirical research as shown in Table 1. The resulting questionnaire can be found in Appendix A. To ensure content validity, we thoroughly examined relevant empirical and theoretical literature covering studies in the fields of both information systems and threat intelligence. This was used in identifying the appropriate operational definitions and measures for each of the constructs. The questionnaire was then tested for readability, clarity and ease of comprehension.

We first discussed the draft within our research team and modified it accordingly. Next, 15 threat intelligence specialists were invited to examine and comment on the wording and layout of the questionnaire to ensure face validity. Subsequently, we finalised the questionnaire's presentation and instructions including the rewording of eight items and the removal of one.

In addition to questions regarding the respondent's background, all seven constructs in our model were measured using a seven-point Likert-type scale with 1 corresponding to 'strongly disagree', 7 corresponding to 'strongly agree', and 4 corresponding to 'neither agree nor disagree'.

4.2. Data collection

The data collection period was between September 2020 and November 2020. The target group consisted of users of threat intelligence management platforms in all sectors. Invitations were sent to users primarily located in the United Kingdom and Europe.

An invitation to participate in the self-administered online questionnaire was posted on several online threat intelligence interest groups and forums. It was also sent by email to a number of connections and security-focused mailing lists. The invitation included a description of the purpose of the study and instructions to access the online questionnaire. We encouraged participants to share the questionnaire with all or a subset of their platform's users as they saw appropriate.

We emphasised in the invitations, as well as in the questionnaire's preamble, that we would use all reasonable endeavours to keep the responses confidential and that the respondent's identity could not be inferred. This was done in order to ensure best possible response rate. A total of 152 completed questionnaires were collected.

5. Analysis and results

We used the empirical data collected through the survey in testing the research hypotheses. To do so, we followed the partial least squares (PLS) approach [59] to analyse the data and assess the measurement properties of the model. The PLS, or variance-based SEM, is well-suited to complex models with large number of indicators and relatively small data samples [60]. It is also useful for models where the measures are not well established [61].

The analysis is presented in three parts. Section 5.1 describes the survey respondents and their organisations, and provides descriptive statistics of the

Variable		Frequency (n=152)	Percentage
Sector	Information or communication	77	50.6%
	Finance or insurance	37	24.3%
	Manufacturing	13	9.2%
	Utilities	9	6.0%
	Public Sector or Defence	7	4.6%
	Retail or wholesale	3	2.0%
	Education	4	2.6%
	Health or social care	1	0.7%
Number of employees	>1,000	60	39.5%
	250–1,000	31	20.4%
	50–249	43	28.3%
	<50	18	11.8%
Experience in threat intelligence	<2 years	53	34.9%
	2–5 years	55	36.2%
	>5 years	44	28.9%
Current position	Security analyst	72	47.4%
	CISO	32	21.1%
	Security researcher	27	17.8%
	Security administrator	10	6.6%
	Security engineer	11	7.2%

Table 3: Description of the survey respondents and their organisations.

responses. Section 5.2 evaluates the latent variable constructs to ascertain whether measurements used are valid and adequately describe the latent variables in this research. There are seven latent variables in this study: content quality (CONQ), system quality (SYSQ), service quality (SERQ), perceived trust (PT), use (USE), user satisfaction (USAT), and net benefits (NETB). Section 5.3 examines the structural model to assess the relationships between the latent variables in this study. We used the software package SmartPLS [62] for statistical calculations.

5.1. Demographics and descriptive statistics

By the end of the survey period, data had been collected from 152 cyber security professionals representing organisations from a range of sectors. As shown in Table 3, half of the respondents (50.6%) were working at organisations in the information or communication sectors; a quarter (24.3%)

were working at finance or insurance organisations; and the remaining quarter (25.1%) were spread across six other sectors.

The respondents' organisations also varied in size, including companies with over 1,000 employees (39.5%), between 250 and 1,000 employees (20.4%), between 50 and 249 employees (28.3%), and fewer than 50 employees (11.8%).

Less than a third of the respondents (28.9%) had over five years of experience in threat intelligence, whereas the rest were split almost equally between those with two to five years of experience (36.2%) and those with less than two years of experience (34.9%). Table 3 provides a full description of the respondents' profiles.

The mean and standard deviation were used to summarise the distribution of the indicators and latent variables. None of the included indicators had missing values. Skewness and kurtosis of the seven latent variables were also tested. The two measures illustrate the deviation of the observational data from the normal distribution. The skewness measures the asymmetry of the distribution, whereas the kurtosis estimates how sharp the distribution's peak is relative to its width. Skewness and kurtosis values between -1 and +1 are considered excellent. Values that fall outside this range but do not exceed -2 to +2 are considered acceptable [63]. As demonstrated in Table 4, we observed a fairly normal distribution for our indicators of latent factors. The skewness value for 28 out of 29 indicators fell between -1 and +1, which is considered excellent. Kurtosis values were also excellent for 25 indicators and did not exceed the -2 to 2 range for the remaining four, which is acceptable.

5.2. Measurement model evaluation

An evaluation of the constructed theoretical model was conducted to determine whether the manifest variables measured the latent variables reliably and adequately. In line with the validation guidelines proposed in [64] and [65], we carried out several tests to assess the measurement model's *unidimensionality*, *multicollinearity*, *internal consistency*, *indicator reliability*, and *convergent and discriminant validity*. The results indicate good reliability of the study's constructs and confirms the validity of their indicators. The results also confirm our theory that each set of items is related to the same corresponding construct, which confirms that the chosen sets of indicators measure the respective emergent constructs.

Item	Mean	Median	Min	Max	Standard Deviation	Excess Kurtosis	Skewness
CONQ1	3.520	4	0	6	1.347	-0.345	-0.556
CONQ2	3.454	4	0	6	1.601	-0.463	-0.479
CONQ3	3.796	4	0	6	1.553	-0.774	-0.453
CONQ4	3.625	4	0	6	1.337	-0.335	-0.455
CONQ5	3.724	4	0	6	1.553	-0.837	-0.350
CONQ6	3.355	4	0	6	1.462	-0.574	-0.381
SYSQ1	4.342	5	1	6	1.107	0.194	-0.770
SYSQ2	4.191	5	0	6	1.213	0.954	-1.133
SYSQ3	4.184	5	0	6	1.305	0.138	-0.831
SYSQ4	4.171	4	0	6	1.224	0.170	-0.746
SERQ1	4.184	4	1	6	1.172	-0.252	-0.315
SERQ2	4.039	4	1	6	1.175	-0.342	-0.348
SERQ3	4.053	4	0	6	1.191	-0.028	-0.457
SERQ4	4.211	4	1	6	1.168	-0.314	-0.318
PT1	4.059	4	1	6	1.182	-0.834	-0.188
PT2	3.954	4	1	6	1.388	-0.738	-0.260
PT3	3.961	4	0	6	1.499	-0.667	-0.441
USE1	3.947	4	1	6	1.385	-0.891	-0.160
USE2	3.717	4	0	6	1.575	-0.329	-0.371
USE3	3.704	4	0	6	1.534	-0.475	-0.275
USAT1	3.618	4	0	6	1.701	-1.197	-0.319
USAT2	3.447	4	0	6	1.780	-1.266	-0.125
USAT3	3.289	4	0	6	1.809	-1.222	-0.123
USAT4	3.546	4	0	6	1.802	-1.272	-0.287
NETB1	3.849	4	0	6	1.463	-0.538	-0.459
NETB2	3.776	4	0	6	1.518	-0.453	-0.515
NETB3	3.730	4	0	6	1.509	-0.470	-0.530
NETB4	3.842	4	0	6	1.496	-0.364	-0.560
NETB5	4.204	5	1	6	1.475	-0.694	-0.519

Table 4: Descriptive statistics of the survey items.

5.2.1. Unidimensionality test

A set of measurement items is described as unidimensional if it measures exactly one latent variable [66]. We conducted an exploratory factor analysis (EFA) to determine whether the indicators converge in the assigned constructs, each indicator has a high loading on one factor only, and this factor is the same for the indicators that are expected to measure it. Seven factors had an Eigenvalue greater than 1.0, which, according to Kaiser criterion, meant that we can select seven factors for the EFA [67].

Using R version 3.6.0 [68], we conducted an EFA with principal component analysis and varimax rotation. The results, as shown in Table 5, demonstrate a high level of unidimensionality. All items loaded highly (coefficient ≥ 0.6) on one factor only [69]. This indicates that our interpretation of each of the constructs in the model is feasible.

5.2.2. Multicollinearity test

Multicollinearity points to a strong correlation between latent variables. High multicollinearity can affect the results of the model. We used the Variance Inflation Factor (VIF) method to test multicollinearity between the model's latent variables. The VIF value of an independent variable indicates how well the variable is explained by other constructs' indicators [70]. Values $\geqslant 5$ indicate collinearity between the independent variables [71].

Table 6 shows the VIF value of our model's variables. All of the VIF values are less than 5, which confirms that there is no multicollinearity between independent variables.

5.2.3. Internal consistency

Internal consistency is usually determined according to Cronbach's alpha (CA) criterion. A high CA value indicates that all the items of one constructs have the same range and meaning [72]. However, composite reliability (CR) is used as an alternative measure to latent variables' reliability since it overcomes some of CA's shortcoming and provides more reliable results [71]. CA and CR scales range from 0 to 1, with a higher value indicating higher reliability level. Values greater than 0.7 for both scales denote acceptable construct reliability [73]. Internal consistency test results are summarised in Table 7. CA and CR values of all latent variables in our model were greater than the recommended minimum of 0.7, indicating good reliability of the study's constructs.

Item	Component						
	1	**2**	**3**	**4**	**5**	**6**	**7**
CONQ1	**0.774**	0.230	0.166	0.197	0.174	0.119	0.163
CONQ2	**0.703**	0.207	0.196	0.208	0.252	0.199	0.177
CONQ3	**0.757**	0.217	0.166	0.204	0.187	0.159	0.136
CONQ4	**0.764**	0.232	0.147	0.215	0.251	0.123	0.187
CONQ5	**0.776**	0.269	0.172	0.213	0.197	0.125	0.127
CONQ6	**0.732**	0.269	0.232	0.229	-	0.177	0.135
SYSQ1	-	0.148	0.248	0.101	**0.673**	0.152	0.143
SYSQ2	0.237	0.226	0.177	0.159	**0.759**	-	0.101
SYSQ3	0.277	0.281	0.192	0.170	**0.742**	0.182	0.135
SYSQ4	0.273	0.169	0.137	0.219	**0.740**	-	0.128
SERQ1	0.165	0.224	**0.843**	0.180	0.124	0.107	0.102
SERQ2	0.148	0.189	**0.707**	-	0.240	0.197	0.141
SERQ3	0.282	0.172	**0.719**	0.179	0.180	0.112	0.177
SERQ4	0.227	0.168	**0.774**	0.230	0.236	0.167	0.131
PT1	0.180	0.202	0.172	0.150	0.168	**0.801**	0.216
PT2	0.160	0.107	0.185	0.174	0.181	**0.764**	0.220
PT3	0.299	0.249	0.191	0.232	0.135	**0.784**	0.224
USE1	0.184	0.126	0.196	0.166	0.190	0.161	**0.708**
USE2	0.218	0.228	0.213	0.151	0.119	0.249	**0.738**
USE3	0.224	0.236	-	0.187	0.156	0.254	**0.764**
USAT1	0.300	0.137	0.182	**0.800**	0.181	0.139	0.138
USAT2	0.281	0.326	0.162	**0.678**	0.126	0.195	0.155
USAT3	0.276	0.190	0.168	**0.787**	0.196	0.170	0.124
USAT4	0.252	0.309	0.138	**0.730**	0.241	0.171	0.244
NETB1	0.265	**0.717**	0.209	0.193	0.227	0.133	0.195
NETB2	0.290	**0.801**	0.220	0.185	0.179	0.164	0.134
NETB3	0.297	**0.708**	0.210	0.216	0.184	0.194	-
NETB4	0.216	**0.758**	-	0.176	0.228	-	0.211
NETB5	0.278	**0.805**	0.243	0.190	0.189	0.145	0.161

Table 5: Assessment of unidimensionality of measured constructs using EFA.

	CONQ	SYSQ	SERQ	PT	USE	USAT	NETB
CONQ	-	-	-	1.702	2.072	1.863	-
SYSQ	-	-	-	1.668	1.751	1.717	-
SERQ	-	-	-	1.612	1.658	1.694	-
PT	-	-	-	-	-	1.59	-
USE	-	-	-	-	-	-	1.393
USAT	-	-	-	-	1.909	-	1.393
NETB	-	-	-	-	-	-	-

Table 6: Multicollinearity test using VIF.

5.2.4. Indicator reliability

Indicator reliability represents the proportion of indicator variance that is explained by the latent variable. It denotes the extent to which the set of variables is consistent in terms of what it intends to measure.

We used a confirmatory factor analysis (CFA) within PLS to evaluate indicator reliability. The number of factors was specified a priori. Each construct's reliability is calculated on its own independent of the others. Indicators with a loading below 0.7 are considered unreliable [59].

Table 8 shows that, in our model, all loadings are above the 0.7 threshold, which indicates that more than 50% of each item's variance is caused by the respective construct. The results confirm the validity of the study's indicators.

5.2.5. Convergent validity

Convergent validity measures the degree to which a set of items reflecting a construct converge, compared to items measuring different constructs. To assess convergent validity, each latent variable's Average Variance Extracted (AVE) is calculated as suggested by Fornell and Larcker in [74]. A value of 0.5 or greater is considered acceptable [73].

Table 7 shows that the AVE value for each of the latent variables in our model is above 0.5, confirming that the constructs' variance is larger than the variance caused by the associated measurement errors. This result confirms our theory that each set of items is related to the same corresponding construct.

5.2.6. Discriminant validity

Discriminant (or divergent) validity refers to the extent to which the constructs differ from one another empirically. It ensures that a construct has

Construct	CA	CR	AVE
Content quality (CONQ)	0.954	0.954	0.776
System quality (SYSQ)	0.906	0.908	0.714
Service quality (SERQ)	0.924	0.925	0.755
Perceived trust (PT)	0.937	0.939	0.839
Use (USE)	0.900	0.901	0.752
User satisfaction (USAT)	0.944	0.944	0.807
Net benefit (NETB)	0.955	0.955	0.809

Table 7: Internal consistency and convergent validity.

CA: Cronbach's alpha
CR: Composite Reliability
AVE: Average Variance Extracted

the strongest relationships with its own indicators [75]. Discriminant validity is evaluated by comparing an indicator's loading with its cross-loadings on other constructs in the model. If the indicator's outer loading on its assigned construct is greater than any of its cross-loadings on other construct, good discriminant validity is achieved [71].

The second test of discriminant validity is the Fornell–Lacker criterion, which compares the correlations between latent variables to the square root of the average variance extracted (AVE). Therefore, the square root of each construct's AVE should have a greater value than the correlations with other latent constructs [7] since it should better explain the variance of its own indicator rather than the variance of other latent constructs.

Table 8 shows that each indicator's loading is higher for its assigned construct than any of its cross-loadings on all other constructs in the research model. Table 9 shows that the square root of AVE for each of the latent variables was greater than its corresponding correlation with any of the other latent variables. The results from both tables indicate that all of our model's constructs are sufficiently dissimilar indicating good discriminant validity.

5.3. Structural model evaluation

Our assessment of the measurement model confirmed that it meets the criteria of convergent validity, discriminant validity, and construct reliability. We therefore moved to evaluating the structural model (inner model). Evaluating the structural model was done to examine the relationship between latent constructs by looking at the estimated results of the path parameter

	Factor						
	CONQ	**SYSQ**	**SERQ**	**PT**	**USAT**	**USE**	**NETB**
CONQ1	**0.903**	0.506	0.477	0.462	0.485	0.567	0.574
CONQ2	**0.889**	0.567	0.522	0.530	0.515	0.588	0.578
CONQ3	**0.899**	0.513	0.482	0.482	0.461	0.570	0.559
CONQ4	**0.917**	0.567	0.487	0.489	0.519	0.594	0.605
CONQ5	**0.920**	0.530	0.500	0.479	0.473	0.591	0.615
CONQ6	**0.882**	0.415	0.520	0.501	0.473	0.579	0.597
SYSQ1	0.353	**0.814**	0.467	0.382	0.376	0.376	0.410
SYSQ2	0.519	**0.902**	0.476	0.402	0.401	0.482	0.517
SYSQ3	0.587	**0.922**	0.524	0.496	0.469	0.531	0.606
SYSQ4	0.542	**0.893**	0.442	0.408	0.413	0.518	0.496
SERQ1	0.467	0.437	**0.923**	0.420	0.404	0.464	0.516
SERQ2	0.420	0.486	**0.861**	0.445	0.404	0.333	0.459
SERQ3	0.552	0.481	**0.904**	0.438	0.464	0.488	0.499
SERQ4	0.542	0.541	**0.922**	0.492	0.461	0.535	0.516
PT1	0.477	0.445	0.452	**0.946**	0.543	0.478	0.489
PT2	0.441	0.432	0.436	**0.924**	0.528	0.465	0.413
PT3	0.605	0.478	0.512	**0.958**	0.593	0.587	0.574
USE1	0.452	0.428	0.429	0.480	**0.889**	0.451	0.429
USE2	0.512	0.423	0.487	0.567	**0.923**	0.490	0.519
USE3	0.516	0.441	0.404	0.566	**0.926**	0.511	0.521
USAT1	0.592	0.482	0.473	0.469	0.457	**0.929**	0.490
USAT2	0.598	0.464	0.460	0.519	0.484	**0.903**	0.612
USAT3	0.587	0.497	0.472	0.496	0.451	**0.928**	0.537
USAT4	0.608	0.564	0.482	0.532	0.564	**0.940**	0.624
NETB1	0.599	0.548	0.523	0.482	0.518	0.565	**0.915**
NETB2	0.626	0.532	0.539	0.506	0.492	0.577	**0.941**
NETB3	0.610	0.518	0.508	0.510	0.449	0.575	**0.897**
NETB4	0.538	0.520	0.408	0.429	0.501	0.523	**0.900**
NETB5	0.627	0.548	0.557	0.500	0.514	0.585	**0.947**

Table 8: Outer and cross-loadings of each indicator in the model.

	CONQ	SYSQ	SERQ	PT	USE	USAT	NETB
CONQ	**0.902**						
SYSQ	0.574	**0.884**					
SERQ	0.553	0.540	**0.903**				
PT	0.545	0.481	0.498	**0.943**			
USE	0.540	0.472	0.482	0.591	**0.913**		
USAT	0.645	0.544	0.510	0.546	0.531	**0.925**	
NETB	0.653	0.580	0.552	0.528	0.538	0.614	**0.920**

Table 9: Inter-construct correlations.

Note: numbers on the diagonal represent the square root of the average variance extracted

coefficients and their significance level. We also reviewed the extent to which the model can explain the relationship between the exogenous variables and the endogenous variables. We used bootstrapping with 1,000 resamples to test regression coefficients for statistical significance and to determine the significance of the paths within the structural model. The results are depicted in Figure 3.

5.3.1. Model fit

The coefficient of determination (R^2) measures the overall effect size, or the variance explained in the structural model's endogenous construct. The value of R^2 is therefore considered a measure of the model's predictive accuracy. A model can be evaluated based on the R^2 values [76, 77]. R^2 takes values between 0 and 1 with higher values indicating higher predictive accuracy.

The use of the adjusted determination coefficient is suggested by [78] to avoid bias in the number of predictors included in the model. Four dependent variables were included in the research model. The adjusted R^2 for *perceived trust* was 0.361, which means that *content quality*, *service quality*, and *system quality* explained 36% of the variability in *perceived trust*. The adjusted R^2 for *use*, *user satisfaction*, and *net benefits* were 0.369, 0.489, and 0.433 respectively. According to [79], values greater than 0.25 (25%) indicate moderate predictive power.

We also used the Standardised Root Mean Square Residual (SRMR) to test the model fit. SRMR is defined as the difference between the model's implied correlation matrix and the observed correlation, which allow us to assess the average magnitude of the discrepancies between observed and

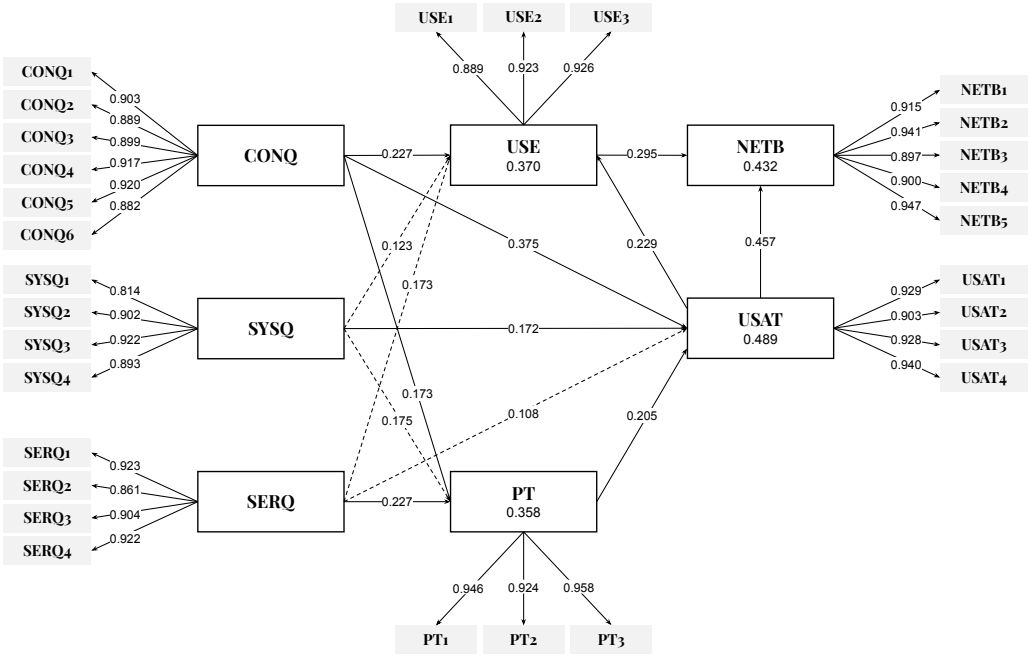

Figure 3: Path Coefficients of Partial Least Square (PLS) Analysis.

expected correlations as a measure of model. The test results showed that the model was a good fit for the data as shown by the SRMR value of 0.086, which was below the suggested threshold of 0.1 and indicated acceptable fit [80].

5.3.2. Hypothesis testing

Path coefficients (regression coefficients) obtained from Partial Least Square (PLS) were used to test the research hypotheses. The path coefficient denotes the extent to which an independent variable affects its dependent variable. Regression coefficients were tested for statistical significance using 1,000 bootstrapped resamples. The bootstrapped samples were used to calculate standard errors and the corresponding 95% confidence intervals. The consistent PLS (PLSc) algorithm was used to evaluate the research model. PLSc corrects the constructs' correlations to ensure the results are consistent with a factor-model [81].

In line with similar studies in the field and based on our sample size, we considered a hypothesis to be supported by the data if the corresponding path coefficient was significant at the $p < 0.05$ threshold [25]. Table 10 summarises

Hypothesis		β	$\bar{x}$	s	t	f^2	p	Support
H1a	CONQ → USE	0.227	0.228	0.095	2.398	0.041	0.017	Yes
H1b	CONQ → USAT	0.375	0.377	0.081	4.652	0.152	<0.001	Yes
H1c	CONQ → PT	0.319	0.317	0.081	3.545	0.095	<0.001	Yes
H2a	SYSQ → USE	0.123	0.126	0.090	1.289	0.014	0.198	No
H2b	SYSQ → USAT	0.172	0.170	0.082	2.092	0.035	0.037	Yes
H2c	SYSQ → PT	0.175	0.174	0.092	1.909	0.029	0.057	No
H3a	SERQ → USE	0.173	0.170	0.090	1.907	0.029	0.057	No
H3b	SERQ → USAT	0.107	0.108	0.077	1.394	0.014	0.164	No
H3c	SERQ → PT	0.227	0.229	0.088	2.580	0.051	0.010	Yes
H4	PT → USAT	0.206	0.201	0.087	2.381	0.054	0.017	Yes
H5	USAT → USE	0.230	0.226	0.109	2.114	0.045	0.035	Yes
H6	USE → NETB	0.295	0.294	0.088	3.357	0.111	0.001	Yes
H7	USAT → NETB	0.458	0.460	0.086	5.310	0.269	<0.001	Yes

Table 10: Hypothesis testing results.

β: path coefficient
$\bar{x}$: sample mean
s: standard deviation
f^2: effect size
t: t statistics = β/s

hypotheses testing results. The majority of the hypotheses were supported. Only four — $H2a, H2c, H3a$ and $H3b$ — were not supported by our data. We discuss these results further in Section 6.

5.3.3. Effect size

Effect size (ES) of independent variables on the corresponding dependent variables were calculated using f^2. Cohen's f^2 can be used to calculate the ES for multiple regression models when the independent variable of interest and the dependent variable are both continuous. Cohen's f^2 is presented in a form appropriate for global effect size: $f^2 = R^2/(1 - R^2)$. $f^2 \geq 0.02$, $f^2 \geq 0.15$, and $f^2 \geq 0.35$ represent small, medium, and large effect sizes, respectively. ES values are presented in Table 10.

6. Discussion

As Table 10 shows, most of the model's hypotheses are supported by our study. The paths from *content quality* to *use* and *user satisfaction*, from *use* to *user satisfaction*, and from *use* and *user satisfaction* to *net benefits*, appear to be consistent with the hypotheses made in the original D&M information

systems success model [14]. Conversely, the paths from *system* and *service quality* to *use*, and from *service quality* to *user satisfaction* are not statistically significant.

Our results, however, provide evidence for most of the hypotheses involving the newly added success construct. The paths from *content* and *service quality* to *perceived trust*, as well as from *perceived trust* to *user satisfaction*, are supported. Only the path between *system quality* and *perceived trust* is not significant.

The results indicate that *content quality* is the only construct that significantly influences *perceived trust*, *user satisfaction* and *use* at the same time. In other words, the quality of the platform's content seems to be one of the most important success factors. High-quality content would increase the users' trust in the platform and their overall satisfaction. It would also drive them to utilise the platform in performing their tasks. Therefore, ensuring the provision of good content in a TIMP may directly strengthen trust, use and user satisfaction, and, eventually, the net benefits gained from deploying the platform.

As depicted in Figure 3, *service quality* does not significantly influence *user satisfaction* or *use*. This may be explained by assuming that, for the platform's users, vendor's support personnel play a limited role in their everyday interaction with the platform. Instead, service quality significantly influence the user's perceived trust in the platform highlighting the role of the vendor's personnel in building and maintaining trust with the users. The relationship between service quality and user satisfaction has been investigated in several studies [82, 83]. However, these studies suggest mixed support for this relationship. Petter and colleagues suggest that the inconsistency in the findings is partly due to the utilisation of different methods in measuring service quality [19].

As for *system quality*, it also does not significantly influence *use*. One explanation could be that, for the users we surveyed, the actual use of a TIMP depends primarily on the content it provides and less so on the quality or features of the system. This explanation is consistent with earlier discussions with practitioners who stated that despite what is often promoted by vendors, the platform's technical features and capabilities are, in most cases, of limited use. Support for this relationship in the literature is mixed. The extent to which the technical aspect of an information system determines the use or discontinuance of use varies depending on the purpose of the system and the definition of system quality [19].

Nevertheless, *system quality* significantly influence *user satisfaction*, which is consistent with the findings of other studies in the information systems literature [19]. This observation in particular is not surprising as there is strong support for the relationship between *system quality* and *user satisfaction* in the literature [84, 19].

It is important to note that, although the utilisation of a TIMP is voluntary in most cases, for threat intelligence analysts, certain data or information can only be received or shared through the platform. The quasi-mandatory nature of using an information system as Urbach and colleagues suggest in [25] offers another possible explanation as to why *system quality* and *service quality* do not significantly influence the actual use of the platform. In line with the corresponding hypotheses in the D&M model, our results suggest that *user satisfaction* influences *use*, and that both *use* and *user satisfaction* influence the *net benefits* gained by utilising a TIMP. The highly significant impact of *user satisfaction* on *net benefits* indicates that *user satisfaction* may serve as a reasonable proxy for *net benefits* as suggested in previous studies [55, 84, 25]. However, the moderate R^2 of *net benefits* indicates that several other factors influence the final dependant construct in the model.

We also calculated the total effect of each of the model's exogenous variables, that is, *content*, *system* and *service quality*, on *net benefits* in order to further investigate the success factors that have the highest impact on the model's effectiveness level [25]. The total effect of a latent variable on another is calculated by adding the latent variable's direct effect to all its indirect effects on the other [76]. The total effects of *content*, *system* and *service quality* on *net benefits* are 0.298, 0.146 and 0.131 respectively — indicating that *content quality* is the factor that influences the model's effectiveness level the most, followed by *system* and *service quality*.

In conclusion, our findings indicate that the success constructs of the D&M model fall short of fully capturing the characteristics of a threat intelligence management platform as a particular case of an information system. Although it provides a useful starting point for modelling the success of TIMPs, the applicability of the D&M success model is limited.

On a practical level, the results provide practitioners with empirical evidence that could help in determining their organisation's priorities while trying to improve their TIMP and its use. Accordingly, practitioners should focus on the following three areas: *content quality*, *system quality* and *trust*.

First, improving content quality should be the primary consideration since it potentially has the biggest impact on users' day-to-day activities. Content

quality can be improved by the intelligence producers and appropriate quality assurance functions should be implemented within a TIMP. However, this requires a clear definition of content quality (e.g. accuracy, reliability, timeliness) dimensions by platform users and providers. Sillaber et al. highlighted the need for more empirical research on the content quality of TI [8].

Second, providers should focus on improving the *system quality*. In this context, we need to distinguish between two types of TIMPs, namely data aggregators and data processors. Data aggregators primarily, focus on the collection and sharing of data and provide limited functions for data analysis. This might be traced back to the fact that data aggregators provide their TI as input for a third-party data processor platforms. Data processors offer a variety of analysis functions designed to generate actionable threat intelligence from threat data in addition to the collection functions. Accordingly, to improve *system quality* in these platforms the implementation of the intelligence cycle (i.e. [85] should be considered by platform providers [8]. Practitioners could use the intelligence cycle while implementing a TI function and selecting an appropriate platform to ensure *system quality* [10].

Third, platform providers and organisations should focus on the *perceived trust* of the TIMP. Therefore, it should be ensured that a platform is compliant with an organisation's data protection and privacy regulations. Furthermore, the security of the platform's services and processed information play an important role in increasing and maintaining trust. Therefore, providers and operators should take all possible organisational and technical measures to ensure the security of the platform.

7. Limitations and future work

The research described in this paper faced a number of issues. However, our decisions during the planning and execution of the investigation attempted to minimise their impact.

As is the case with other empirical investigations involving voluntary participation, there is an inevitable selection bias. In order to limit this, we posted a link to our self-administered online questionnaire on a range of online threat intelligence groups and forums. We also asked the participants to share the questionnaire with their networks in an attempt to reach participants from outside our direct reach.

Some of the hypothesised relationships are not supported. Although we provided possible explanations for these results, the available data does not

allow for testing these explanations any further. The influence of system and service quality on user satisfaction and use of threat intelligence platforms seems especially worth investigating further.

Unfortunately, due to the large number of dimensions and the uniform abstraction level of the model, some dimensions could not be considered in detail or only superficially. Therefore, future research should take a closer look at some dimensions (e.g. User satisfaction, perceived trust), in order to identify further success factors and potential relationships between model constructs. For example, the efficiency of translating observed threats into actions could be another success factor in terms of user satisfaction.

With regards to other potential areas of future work, it would, of course, be beneficial to use a more random and larger sample drawn from a pool of organisations, with a view both to provide a more accurate insight into the effects among the model's constructs and to increase the generalisability of the findings. It would also be beneficial to apply such a research instrument to a single organisation in order to assess in greater detail how the variables relate in the context of that organisation.

We should also note that we captured and investigated the user perceptions of threat intelligence management platform based on different commercial platforms, each of which had been customised to the organisation's requirements. Future research could replicate the study across a group of organisations using the same platform.

8. Conclusion

In this paper we introduced and tested a multi-dimensional success model for threat intelligence management platforms (TIMPs). To the best of our knowledge, this paper represents the first attempt to empirically validate a comprehensive success model for threat intelligence platforms.

The model was based on DeLone and McLean's information systems success model [14] and incorporated findings from the literature and our previous research. We developed a number of hypotheses that reflected the associations between the model's success factors and tested them via a survey in which 152 cyber security professionals participated.

The measurement and structural evaluation of the model revealed that the quality of the content and the perceived trust in the platform are among the most important success factors and have to be considered as priorities for operating a successful TIMP.

These findings should allow practitioners to better understand the factors that influence the improvement and success of their TIMP and how these factors interact with each other. The empirical validation of this comprehensive success model for TIMPs advances the theoretical and practical understanding in the area of threat intelligence sharing. Furthermore, we have laid the groundwork for further research that might investigate certain constructs in detail and revise the model accordingly. For example, we figured out that content quality is one of the most important constructs for user satisfaction. Therefore, our future work might include further empirical research on content quality which might affect the model.

Acknowledgments

The authors thank the anonymous reviewers for their helpful and constructive comments. Adam Zibak's research is funded by EPSRC via the Centre for Doctoral Training in Cyber Security at the University of Oxford.

Declaration of Interest Statements

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] J. Jang-Jaccard, S. Nepal, A survey of emerging threats in cybersecurity, Journal of Computer and System Sciences 80 (2014) 973–993.

[2] L. Dandurand, O. Serrano, Towards improved cyber security information sharing , in: Proceedings of the 5th International Conference on Cyber Conflict, CyCon 2013, IEEE, 2013, pp. 1–16. URL: http://ieeexplore.ieee.org/xpls/abs{_}all.jsp?arnumber=6568369. doi:10.1109/HICSS.2014.252.

[3] D. Chismon, M. Ruks, Threat Intelligence: Collecting, Analysing, Evaluating, https://www.mwrinfosecurity.com/assets/Whitepapers/Threat-Intelligence-Whitepaper.pdf, 2015.

[4] S. Brown, J. Gommers, O. Serrano, From Cyber Security Information Sharing to Threat Management, in: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, WISCS '15, ACM, 2015, pp. 43–49. URL: http://doi.acm.org/10.1145/2808128.2808133. doi:10.1145/2808128.2808133.

[5] C. Sauerwein, C. Sillaber, A. Mussmann, R. Breu, Threat Intelligence Sharing Platforms : An Exploratory Study of Software Vendors and Research Perspectives, in: Proceedings of 13th International Conference on Wirtschaftsinformatik, WI 2017, 2017, pp. 837–851. URL: https://www.wi2017.ch/images/wi2017-0188.pdf.

[6] D. F. Vazquez, O. P. Acosta, C. Spirito, S. Brown, E. Reid, Conceptual framework for cyber defense information sharing within trust relationships, in: Proceedings of the 4th International Conference on Cyber Conflict, CYCON 2012, IEEE, 2012, pp. 1–17. URL: https://ieeexplore.ieee.org/document/6243990.

[7] C. Sauerwein, C. Sillaber, R. Breu, Shadow Cyber Threat Intelligence and Its Use in Information Security and Risk Management Processes, in: Proceedings of Multikonferenz Wirtschaftsinformatik 2018, MKWI '18, 2018, pp. 1333–1344.

[8] C. Sillaber, C. Sauerwein, A. Mussmann, R. Breu, Data quality challenges and future research directions in threat intelligence sharing practice, in: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, WISCS '16, ACM, 2016, pp. 65–70. URL: http://doi.acm.org/10.1145/2994539.2994546. doi:10.1145/2994539.2994546.

[9] M. Gschwandtner, L. Demetz, M. Gander, R. Maier, Integrating threat intelligence to enhance an organization's information security management, in: Proceedings of the 13th International Conference on Availability, Reliability and Security, 2018, pp. 1–8.

[10] S. Bauer, D. Fischer, C. Sauerwein, S. Latzel, D. Stelzer, R. Breu, Towards an evaluation framework for threat intelligence sharing platforms, in: Proceedings of the 53rd Hawaii International Conference on System Sciences, 2020.

[11] A. de Melo e Silva, J. J. Costa Gondim, R. de Oliveira Albuquerque, L. J. García Villalba, A methodology to evaluate standards and platforms within cyber threat intelligence, Future Internet 12 (2020) 108.

[12] A. Zibak, A. Simpson, Can We Evaluate the Effectiveness of Cyber Security Information Sharing Efforts?, in: Proceedings of the 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2018, IEEE, 2018. doi:10.1109/CyberSA.2018.8551462.

[13] W. H. DeLone, E. R. McLean, Information systems success: The quest for the dependent variable, Information Systems Research 3 (1992) 60—95. URL: https://doi.org/10.1287/isre.3.1.60. doi:10.1287/isre.3.1.60.

[14] W. H. DeLone, E. R. McLean, The DeLone and McLean model of information systems success: A ten-year update, Journal of Management Information Systems 19 (2003) 9–30. doi:10.1080/07421222.2003.11045748.

[15] G. P. Z. Montesdioca, A. C. G. Maçada, Quality dimensions of the delone-mclean model to measure user satisfaction: An empirical test on the information security context, in: Proceedings of the 2015 48th Hawaii International Conference on System Sciences, IEEE, 2015, pp. 5010–5019. doi:10.1109/HICSS.2015.593.

[16] L. F. Pitt, R. T. Watson, C. B. Kavan, Service quality: A measure of information systems effectiveness, MIS Quarterly 19 (1995) 173–187. URL: http://www.jstor.org/stable/249687.

[17] P. B. Seddon, A respecification and extension of the delone and mclean model of is success, Information Systems Research 8 (1997) 240–253. URL: https://doi.org/10.1287/isre.8.3.240. doi:10.1287/isre.8.3.240.

[18] P. B. Seddon, S. Staples, R. Patnayakuni, M. Bowtell, Dimensions of information systems success, Communications of the Association for Information Systems 2 (1999). URL: https://aisel.aisnet.org/cais/vol2/iss1/20. doi:10.17705/1CAIS.00220.

[19] S. Petter, W. H. DeLone, E. R. McLean, Measuring information systems success: Models, dimensions, measures, and interrelationships, European Journal of Information Systems 17 (2008) 236–263. doi:10.1057/ejis.2008.15.

[20] S. Chatterjee, S. Chakraborty, S. Sarker, S. Sarker, F. Y. Lau, Examining the success factors for mobile work in healthcare: A deductive study, Decision Support Systems 46 (2009) 620–633. URL: http://dx.doi.org/10.1016/j.dss.2008.11.003. doi:10.1016/j.dss.2008.11.003.

[21] J. Wu, Y. Wang, Measuring kms success: A respecification of the delone and mclean's model, Information and Management 43 (2006) 728–739. URL: http://www.sciencedirect.com/science/article/pii/S0378720606000498. doi:https://doi.org/10.1016/j.im.2006.05.002.

[22] U. Kulkarni, S. Ravindran, R. Freeze, A knowledge management success model: Theoretical development and empirical validation, Journal of Management Information Systems 23 (2007) 309–347. doi:10.2753/NUS0742-1222230311.

[23] W. H. DeLone, E. R. McLean, Measuring e-commerce success: Applying the delone and mclean information systems success model, International Journal of Electronic Commerce 9 (2004) 31–47. doi:10.1080/10864415.2004.11044317.

[24] Y. Wang, Y. Liao, Assessing egovernment systems success: A validation of the delone and mclean model of information systems success, Government Information Quarterly 25 (2008) 717–733. URL: http://www.sciencedirect.com/science/article/pii/S0740624X07000615. doi:https://doi.org/10.1016/j.giq.2007.06.002.

[25] N. Urbach, S. Smolnik, G. Riempp, An empirical investigation of employee portal success, Journal of Strategic Information Systems 19 (2010) 184–206. URL: http://dx.doi.org/10.1016/j.jsis.2010.06.002. doi:10.1016/j.jsis.2010.06.002.

[26] W. Tounsi, H. Rais, A survey on technical threat intelligence in the age of sophisticated cyber attacks, Computers and Security 72 (2018) 212–233. URL: https://doi.org/10.1016/j.cose.2017.09.001. doi:10.1016/j.cose.2017.09.001.

[27] M. S. Abu, S. R. Selamat, A. Ariffin, R. Yusof, Cyber threat intelligence–issue and challenges, Indonesian Journal of Electrical Engineering and Computer Science 10 (2018) 371–379.

[28] W. Zhao, G. White, A collaborative information sharing framework for community cyber security, in: Homeland Security (HST), 2012 IEEE Conference on Technologies for, IEEE, 2012, pp. 457–462.

[29] O. Serrano, L. Dandurand, S. Brown, On the Design of a Cyber Security Data Sharing System, in: Proceedings of the 2014 ACM Workshop on Information Sharing and Collaborative Security, WISCS '14, ACM, 2014, pp.

61–69. URL: http://dl.acm.org/citation.cfm?doid=2663876.2663882. doi:10.1145/2663876.2663882.

[30] A. Schwartz, S. C. Shah, M. H. MacKenzie, S. Thomas, T. S. Potashnik, B. Law, Automatic threat sharing: How companies can best ensure liability protection when sharing cyber threat information with other companies or organizations, U. Mich. JL Reform 50 (2016) 887.

[31] A. Nolan, Cybersecurity and information sharing: Legal challenges and solutions, Congressional Research Service, 2015.

[32] C. S. Johnson, M. L. Badger, D. A. Waltermire, J. Snyder, C. Skorupka, Guide to Cyber Threat Information Sharing, Technical Report 800-150, National Institute of Standards and Technology, 2016. URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf. doi:10.6028/NIST.SP.800-150.

[33] S. Barnum, Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX), https://www.mitre.org/publications/technical-papers/standardizing-cyber-threat-intelligence-information-with-thee, 2014.

[34] OASIS Committee Specification, TAXII^{TM} Version 2.0, http://docs.oasis-open.org/cti/taxii/v2.0/cs01/taxii-v2.0-cs01.html, 2017.

[35] F. Skopik, G. Settanni, R. Fiedler, A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing, Computers & Security 60 (2016) 154–176. URL: http://dx.doi.org/10.1016/j.cose.2016.04.003http://linkinghub.elsevier.com/retrieve/pii/S0167404816300347. doi:10.1016/j.cose.2016.04.03.

[36] J. Steinberger, A. Sperotto, M. Golling, H. Baier, How to exchange security events? Overview and evaluation of formats and protocols, in: Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), IEEE, 2015, pp. 261–269. doi:10.1109/INM.2015.7140300.

[37] P. Kampanakis, Security automation and threat information-sharing options, IEEE Security Privacy 12 (2014) 42–51. doi:10.1109/MSP.2014.99.

[38] E. Asgarli, E. Burger, Semantic ontologies for cyber threat sharing standards, in: 2016 IEEE Symposium on Technologies for Homeland Security (HST), IEEE, 2016, pp. 1–6.

[39] F. Menges, G. Pernul, A comparative analysis of incident reporting formats, Computers & Security 73 (2018) 87–101.

[40] C. Wagner, A. Dulaunoy, G. Wagener, A. Iklody, MISP - The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform, in: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, WISCS '16, ACM, 2016, pp. 49–56. URL: http://doi.acm.org/10.1145/2994539.2994542http://dl.acm.org/citation.cfm?doid=2994539.2994542. doi:10.1145/2994539.2994542.

[41] M. Mutemwa, J. Mtsweni, N. Mkhonto, Developing a cyber threat intelligence sharing platform for south african organisations, in: 2017 Conference on Information Communication Technology and Society (ICTAS), IEEE, 2017, pp. 1–6.

[42] M. A. Alhawamdeh, Developing a conceptual national information sharing security framework to combat cybercrimes in jordan, in: 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), IEEE, 2017, pp. 344–350.

[43] S. Appala, N. Cam-Winget, D. McGrew, J. Verma, An Actionable Threat Intelligence system using a Publish-Subscribe communications model, in: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, WISCS '15, ACM, 2015, pp. 61–70. URL: http://dl.acm.org/citation.cfm?doid=2808128.2808131. doi:10.1145/2808128.2808131.

[44] C. Sillaber, C. Sauerwein, A. Mussmann, R. Breu, Towards a Maturity Model for Inter-Organizational Cyber Threat Intelligence Sharing: A Case Study of Stakeholders' Expectations and Willingness to Share, in: Proceedings of Multikonferenz Wirtschaftsinformatik 2018, MKWI '18, 2018, pp. 1409–1420.

[45] P. Amthor, D. Fischer, W. E. Kühnhauser, D. Stelzer, Automated cyber threat sensing and responding: Integrating threat intelligence into security-policy-controlled systems, in: Proceedings of the 14th International Conference on Availability, Reliability and Security, 2019, pp. 1–10.

[46] A. Zibak, C. Sauerwein, A. Simpson, Towards a Cyber Threat Intelligence Quality Model, Under consideration by Digital Threats: Research and Practice., 2020.

[47] A. Molla, P. S. Licker, E-Commerce Systems Success : an Attempt To Extend and Respecify the Delone and Maclean Model of IS Success, Journal of Electronic Commerce Research 2 (2001) 131–141.

[48] P. B. Seddon, S. K. Yip, An empirical evaluation of user information satisfaction (UIS) measures for use with general ledger accounting software, Journal of Information Systems 6 (1992) 75–92.

[49] A. Zibak, A. Simpson, Cyber threat information sharing: Perceived benefits and barriers, in: Proceedings of the 14th International Conference on Availability, Reliability and Security, ARES '19, ACM, 2019, pp. 85:1–85:9. URL: http://doi.acm.org/10.1145/3339252.3340528. doi:10.1145/3339252.3340528.

[50] A. Parasuraman, V. A. Zeithaml, L. L. Berry, Servqual: A multiple-item scale for measuring consumer perceptions of service quality, Journal of Retailing 64 (1988) 12–40.

[51] C. W. Chen, Impact of quality antecedents on taxpayer satisfaction with online tax-filing systems - An empirical study, Information and Management 47 (2010) 308–315. URL: http://dx.doi.org/10.1016/j.im.2010.06.005. doi:10.1016/j.im.2010.06.005.

[52] J. J. Jiang, G. Klein, C. L. Carr, Measuring Information System Service Quality: SERVQUAL from the Other Side, MIS Quarterly 26 (2002) 145. URL: https://www.jstor.org/stable/10.2307/4132324?origin=crossref. doi:10.2307/4132324.

[53] T. D. Wagner, E. Palomar, K. Mahbub, A. E. Abdallah, A Novel Trust Taxonomy for Shared Cyber Threat Intelligence, Security and Communication Networks 2018 (2018). URL: https://doi.org/10.1155/2018/9634507. doi:10.1155/2018/9634507.

[54] W. J. Doll, G. Torkzadeh, Developing a multidimensional measure of system-use in an organizational context, Information and Management 33 (1998) 171 – 185. URL: http://www.sciencedirect.com/science/article/pii/S0378720698000287. doi:https://doi.org/10.1016/S0378-7206(98)00028-7.

[55] B. Ives, M. H. Olson, J. J. Baroudi, The measurement of user information satisfaction, Communications of the ACM 26 (1983) 785–793. doi:10.1145/358413.358430.

[56] K. Hornbaek, Current practice in measuring usability: Challenges to usability studies and research, International Journal of Human-Computer Studies 64 (2006) 79 – 102. URL: http://www.sciencedirect.com/science/article/pii/S1071581905001138. doi:https://doi.org/10.1016/j.ijhcs.2005.06.002.

[57] A. Rai, S. S. Lang, R. B. Welker, Assessing the validity of IS success models: An empirical test and theoretical analysis, Information Systems Research 13 (2002) 50–69. doi:10.1287/isre.13.1.50.96.

[58] N. Urbach, S. Smolnik, G. Riempp, The State of Research on Information Systems Success, Business & Information Systems Engineering: The International Journal of WIRTSCHAFTSINFORMATIK 1 (2009) 315–325. URL: https://ideas.repec.org/a/spr/binfse/v1y2009i4p315-325.html. doi:10.1007/s12599-009-0059-y.

[59] W. W. Chin, The partial least squares approach for structural equation modeling., in: Modern methods for business research., Methodology for business and management., Lawrence Erlbaum Associates Publishers, 1998, pp. 295–336.

[60] J. F. Hair, M. Sarstedt, L. Hopkins, V. G. Kuppelwieser, Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research, European Business Review 26 (2014) 106–121. URL: https://doi.org/10.1108/EBR-10-2013-0128. doi:10.1108/EBR-10-2013-0128.

[61] C. Fornell, F. L. Bookstein, Two structural equation models: Lisrel and pls applied to consumer exit-voice theory, Journal of Marketing Research 19 (1982) 440–452. URL: http://www.jstor.org/stable/3151718.

[62] C. M. Ringle, S. Wende, J. Becker, Smartpls 3, http://www.smartpls.com, 2015.

[63] W. Trochim, J. P. Donnelly, The Research Methods Knowledge Base, Cengage Learning, 2006. URL: https://books.google.co.uk/books?id=097mAAAACAAJ.

[64] D. Straub, M. Boudreau, D. Gefen, Validation guidelines for is positivist research, Communications of the Association for Information Systems 3 (2004) 380–427. doi:10.17705/1CAIS.01324.

[65] B. R. Lewis, G. F. Templeton, T. A. Byrd, A methodology for construct development in mis research, European Journal of Information Systems 14 (2005) 388–400. URL: https://doi.org/10.1057/palgrave.ejis.3000552. doi:10.1057/palgrave.ejis.3000552.

[66] D. W. Gerbing, J. C. Anderson, An updated paradigm for scale development incorporating unidimensionality and its assessment, Journal of Marketing Research 25 (1988) 186–192. URL: http://www.jstor.org/stable/3172650.

[67] H. F. Kaiser, The application of electronic computers to factor analysis, Educational and Psychological Measurement 20 (1960) 141–151. URL: https://doi.org/10.1177/001316446002000116. doi:10.1177/001316446002000116.

[68] R Core Team, R: A Language and Environment for Statistical Computing, R Foundation for Statistical Computing, Vienna, Austria, 2013. URL: http://www.R-project.org/.

[69] D. Gefen, D. Straub, A practical guide to factorial validity using pls-graph: Tutorial and annotated example, Communications of the Association for Information Systems 16 (2005) 91–109. doi:10.17705/1CAIS.01605.

[70] C. M. Cassel, P. Hackl, A. H. Westlund, On measurement of intangible assets: A study of robustness of partial least squares, Total Quality Management 11 (2000) 897–907. doi:10.1080/09544120050135443.

[71] J. F. Hair, G. T. M. Hult, C. Ringle, M. Sarstedt, A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM), SAGE Publications, 2016. URL: https://books.google.co.uk/books?id=JDWmCwAAQBAJ.

[72] L. J. Cronbach, Coefficient alpha and the internal structure of tests, Psychometrika 16 (1951) 297–334.

[73] K. Wong, Partial least square structural equation modeling (pls-sem) techniques using smartpls, Marketing Bulletin 24 (2013) 1–32.

[74] C. Fornell, D. F. Larcker, Evaluating structural equation models with unobservable variables and measurement error, Journal of Marketing Research 18 (1981) 39–50. URL: http://www.jstor.org/stable/3151312.

[75] M. Lewis-Beck, A. E. Bryman, T. F. Liao, The SAGE Encyclopedia of Social Science Research Methods, SAGE Publications, 2003.

[76] J. Henseler, C. M. Ringle, R. R. Sinkovics, The use of partial least squares path modeling in international marketing, in: R. R. Sinkovics, P. N. Ghauri (Eds.), New Challenges to International Marketing, volume 20 of *Advances in International Marketing*, Emerald Group Publishing Limited, 2009, pp. 277–319. URL: https://doi.org/10.1108/S1474-7979(2009)0000020014. doi:10.1108/S1474-7979(2009)0000020014.

[77] J. F. Hair, M. Sarstedt, T. M. Pieper, C. M. Ringle, The use of partial least squares structural equation modeling in strategic management research: A review of past practices and recommendations for future applications, Long Range Planning 45 (2012) 320 – 340. URL: http://www.sciencedirect.com/science/article/pii/S0024630112000568. doi:https://doi.org/10.1016/j.lrp.2012.09.008.

[78] J. Cohen, P. Cohen, S. West, L. Aiken, Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences, Routledge, 2003. doi:https://doi.org/10.4324/9780203774441.

[79] I. Ghozali, Structural equation modeling: metode alternatif dengan partial least square (PLS), Badan Penerbit Universitas Diponegoro, 2008. URL: https://books.google.com.eg/books?id=x1ZAngAACAAJ.

[80] L. Hu, P. Bentler, Fit indices in covariance structure modeling: Sensitivity to underparameterized model misspecification, Psychological Methods 3 (1998) 424–453.

[81] T. Dijkstra, J. Henseler, Consistent partial least squares path modeling, MIS Quarterly 39 (2015) 297–316. doi:10.25300/MISQ/2015/39.2.02.

[82] J. M. Choe, The relationships among performance of accounting information systems, influence factors, and evolution level of information systems, Journal of Management Information Systems 12 (1996) 215–239. doi:10.1080/07421222.1996.11518107.

[83] L. A. Halawi, R. V. McCarthy, J. E. Aronson, An empirical investigation of knowledge management systems' success, Journal of Computer Information Systems 48 (2008) 121–135. doi:10.1080/08874417.2008.11646014.

[84] J. Iivari, An empirical test of the delone-mclean model of information system success, ACM SIGMIS Database 36 (2005) 8–27. doi:10.1145/1066149.1066152.

[85] M. Dempsey, Joint intelligence, Joint Publication (2013) 2–0.

Appendix A. Questionnaire

Q1. Which of these best describe your organisation's primary activity?

☐ Manufacturing	☐ Utilities
☐ Construction	☐ Retail/wholesale
☐ Food/hospitality	☐ Transportation/storage
☐ Finance/insurance	☐ Information/communication
☐ Real estate	☐ Professional/scientific/technical
☐ Administration	☐ Public Sector/defence
☐ Education	☐ Health/social care
☐ Entertainment	☐ Other service activities

Q2. Which of these best represents the number of employees working in your organisation?

☐ <50	☐ 50–249
☐ 250–1,000	☐ > 1,000

Q3. What is your current position at the organisation?

Q4. How many years of professional experience do you have in threat intelligence?

☐ <2 years ☐ 2–5 years ☐ > 5 years

Q5. Please assess the *content quality* of your organisation's threat intelligence management platform. 1 (strongly disagree) to 7 (strongly agree).

The platform's content is accurate
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The platform's content is actionable
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The platform's content is relevant
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The platform's content is reliable
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The platform's content is timely
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The process through which the platform's content was produced is traceable
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7

Q6. Please assess the *system quality* of your organisation's threat intelligence management platform. 1 (strongly disagree) to 7 (strongly agree).

The platform is easy to use and navigate
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The platform is reliable
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The platform offers appropriate functionality
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7

The platform is interoperable with other systems or tools
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7

Q7. Please assess the *service quality* of the vendor responsible for the support of your organisation's threat intelligence management platform. 1 (strongly disagree) to 7 (strongly agree).
The vendor is willing to help whenever I need support with the platform
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The vendor provides personal attention when I experience problems with the platform
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The vendor provides services related to the platform at the promised time
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The vendor has sufficient knowledge to answer my questions regarding the platform
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7

Q8. Please assess the your *trust* in the organisation's threat intelligence management platform. 1 (strongly disagree) to 7 (strongly agree).
The platform is compliant with applicable data protection and privacy regulations
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The platform is secure and safe to use
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
Overall, I trust the platform
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7

Q9. To what extent you agree or disagree with the following statements regarding the *use* of your organisation's threat intelligence management platform? 1 (strongly disagree) to 7 (strongly agree).
I use the platform to receive and collect threat data or intelligence
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
I use the platform to enrich and analyse the collected threat data or intelligence
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
I use the platform to disseminate threat data or intelligence to relevant tools or stakeholders
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7

Q10. Please assess your *satisfaction* with your organisation's threat intelligence management platform. 1 (strongly disagree) to 7 (strongly agree).
The platform adequately supports my area of work and responsibility
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The platform is efficient
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The platform is effective
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
I am satisfied with the platform as a whole
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7

Q11. To what extent you agree or disagree with the following statements regarding the *benefits* of your organisation's threat intelligence management

platform? 1 (strongly disagree) to 7 (strongly agree).

The platform contributes to breach detection and recovery

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7

The platform supports incident response efforts

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7

The platform enhances defensive agility and resilience

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7

The platform complements other sources of intelligence

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7

The platform improves overall security posture and situational awareness

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7