Prerequisite to Measure Information Security
A State of the Art Literature Review

Rainer Diesch[1,2], Matthias Pfaff[1,2] and Helmut Krcmar[2]
[1]*fortiss GmbH, An-Institut der Technischen Universität München, Guerickestr. 25, 80805 München, Germany*
[2]*Chair of Information Systems, Technischen Universität München, Boltzmannstr. 3, München, Germany*

Keywords: Security Measurement, Security Metrics, Cyber Security, Information Security, Literature Review.

Abstract: The field of information security is growing in research and practice over the past years. Recent studies highlight a gap in measuring and monitoring information security. In this context various definitions and synonymous expressions exist to describe information security. The aim of the work is to compare and delimit the various terms in this field of research and give a thematic overview of current articles in place. In particular, five dimensions of information security are developed and outlined. Additionally, an overview of possible research directions in the field of measuring and monitoring information security is provided.

1 INTRODUCTION

The interest in aspects of information security has increased significantly in recent years. There are technical, behavioral, managerial, philosophical and organizational aspects which address the protection of assets and mitigation of threats (Crossler et al., 2013). These aspects are not to be ignored for organizations since these can lead to great harm in case of disregard. (Frizell, 2015) reported a damage of $15m within one-quarter for Sony Pictures because of a security breach. This cost only included the direct costs of cleaning up the systems. The damage caused by the loss of reputation and other factors were not included. In 2016, the ransomware 'wannacry' infected thousands of computers in more than 150 countries. The damage was not only economically as people like patients were affected as their appointments were canceled based on system errors (Bentkower, 2017). Organizations are not just affected because of potential economic damage but also of legal requirements like the security-law in Germany (Bundesanzeiger, 2015).

Recent literature reviews on information security pointed out the need for intensified research in measuring and monitoring information security related data (D'Arcy and Herath, 2011; Crossler et al., 2013; Fenz et al., 2014; Sommestad et al., 2014). This is an obligatory aspect of information security management for making good decisions (Bayuk, 2013). Also, accurate models of the security problem are not in place (D'Arcy and Herath, 2011). A problem which causes a lack of measurement of information security aspects is that the identification of security related data is not well-known (Fenz et al., 2014). But a requirement to collect and measure security related data is to understand the success factors of information security (Sommestad et al., 2014).

The aim of this work is to gain an overview of current research in the field of measuring information security. A state-of-the-art literature analysis is carried out to obtain a comprehensive overview of the area. The goal is not just to show the literature but also to define the different terms in place. Since the understanding is a requirement for measurement, a definition becomes indispensable. Thematic classes of the research area are needed to observe and assign future research.

The paper is organized as follows: Section 2 outlines the used method with the scope and the search process to collect relevant literature. Section 3 consists of a descriptive analysis, the extracted definitions and thematic classification of the investigated literature. Part 4 shows current research challenges for each of the classes. Finally, this work concludes with a conclusion and limitation section.

2 METHOD

To provide a comprehensible literature review, the method of (Webster and Watson, 2002) and the tool-

Diesch, R., Pfaff, M. and Krcmar, H.
Prerequisite to Measure Information Security - A State of the Art Literature Review.
DOI: 10.5220/0006545602070215
In *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018)*, pages 207-215
ISBN: 978-989-758-282-0

Table 1: Search process matrix.

Group	Resource	Hits[KW]	Hits[TA]	Relevant
Information Security	Information Management and Computer Security	99	7	7
	IEEE Transactions on Dependable and Secure Computing	8	1	1
	IEEE Transactions on Information Forensics and Security	7	0	0
	Computers & Security	84	12	9
Databases	Google Scholar	100	11	9
	ScienceDirect	41	6	4
	OpacPlus	110	17	11
Backward			10	10
Forward			24	19
Total		449	88	70

set of (vom Brocke et al., 2009) was used. The specific goals of this review are as follows:

1. Identify, define and delimit different terms in the field of information security.
2. Assign the relevant literature to the definitions and compare it with the used terms of the literature itself.
3. Thematic classification of the literature and show current research gaps.

Search Process: Initially, a keyword search is performed within peer-reviewed journals to select high quality articles. Journals from the security field were selected within the Scimago Journal & Country Rank (SJR) with the condition that they are part of the categories security, safety, risk or reliability. Two journals are added because they were used often in the basis literature reviews of (D'Arcy and Herath, 2011; Crossler et al., 2013; Fenz et al., 2014; Sommestad et al., 2014). These are 'Computers & Security' and 'Information Management & Computer Security'. To provide most of the relevant literature the databases ScienceDirect, OpacPlus and Google Scholar were added to the search. As the most relevant literature can be found within the first 100 result of Google Scholar the search was limited to these result set (Silic and Back, 2014). To limit the results the following keyword-string were used.

```
(it OR information OR cyber)
AND (resilience OR security)
AND (factors OR kpi OR measures OR metrics
OR measurement OR indicator OR management)
```

The first iteration of the search process resulted in a number of hits (Hits[KW]) which are shown in Table 1. After that, technical articles and those which are not related to the search topic were excluded based on their title and abstract (Hits[TA]). Finally, articles which described metrics or success factors of information security were marked as relevant. After that, a forward and backward search was carried out to get results which are relevant and were not yet found. The backward search contained all articles which were referenced in the previous iteration and which are of relevance for the information security measurement topic. Google Scholar (scholar.google.de) was used with its function 'Cited by' in order to identify all articles which reference the selected one.

3 FINDINGS

First, a descriptive statistic was done to get a background of the research area. The last row of table 1 shows the total amount of articles found in the literature. Only 15.59% of the original articles out of the first search round could be marked as relevant. This leads to the assumption that there are many different phenomena described in the research area. The high amount of articles also assumes the importance and presence in research. Many articles were identified in the forward and backward search (29) within conferences. This can be seen as an indication that the topic is still at the beginning of research. Technically oriented journals just show up with one relevant article. The quantification of information security is therefore mainly part of the security management or related area and not technical-driven.

Since there are many definitions and terms of information security in the literature, the next subsection compares and delimits them. Finally, a classification of the relevant literature in thematic classes are developed to better track and monitor future research.

3.1 The Terms in Information Security

A lot of different terms which describe 'information security' are in place during the review. These are 'Information Systems Security', 'IT Security', 'Information Security', 'Cyber Security' and 'Cyber Resilience'.

The basis of the delimitation in this article is the work of (von Solms and van Niekerk, 2013). They

defined three terms in the security area. 'Information Security' (IS), 'Information and Communication Technology Security' (ICT) and 'Cyber Security' (CS). The delimitation of the terms is based on the assets which are protected. In this case, ICT is the protection of information which is stored or transmitted via a technical system. 'IT Security' or 'Systems Security' are defined as synonyms to ICT. IS differs from this because it is the protection of information which can be stored or transmitted without using technical systems. ICT is a part of IS because IS includes the protection of the underlying technology. CS now describes the protection of assets without any information but with a relationship to them. A bugging operation is an example of this. A technical system (phone) was attacked which has 'access' to information which is in human heads. CS is protecting technical systems which have or have no information stored and therefore also includes ICT. 'Cyber Resilience' (CR) firstly appears 2013 in form of resilience management (Crossler et al., 2013). The only attempt to define CR was done by (Björck et al., 2015). They showed 5 dimensions to differ CR from CS. One of these is assets. CR is not just about the protection of assets but also to ensure business delivery despite adverse cyber events. The correlation between the terms is shown in Figure 1.

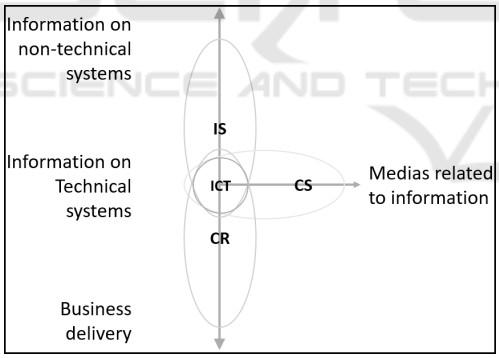

Figure 1: Delimitation of terms.

According to the definition of ICT, IS, CS and CR, the literature was assigned respectively one or more of these in two iterations. First, the article was assigned the term, which the author had intended for this. The basis of the assignment was the terms of the title, abstracts and the keywords. Second, the articles were assigned the terms according to the definition above. This is done based on the context.

The result of the assignment shows that 23 out of 70 articles (32.86%) have the same assignment to the terms for both iterations. It is noticeable that the terms are often used as synonyms. Mainly IS is used as a synonym for ICT. Articles that use the term IS (60) often have just content of ICT included in the text (37) and not IS as defined. All authors used CS and CR as synonyms for ICT. The articles which describe CS or CR used the term IS instead of them. In the present literature, there are clear definitions of the terms, but the terms are not used based on them.

3.2 Thematic Classification

The relevant literature of this review is about measurement and metrics of ICT, IS, CS and CR. To observe papers in future and better understand the context, there are several classes produced in this literature review which are based on the keywords of the underlying articles. Each paper is assigned to one of the classes which are shown in Table 2.

3.2.1 Security Management

'Information security management' is used to describe activities for the protection of valuable information assets and mitigate various risks to information coming from all aspects of the organizations environment by applying the security technology and management process (Ernest Chang and Ho, 2006). In other words, it is about processes to control, classify and manage information as well as different guidelines and policies therefrom.

Organization and Governance: These articles deal with organizational processes, policies and their effectiveness. A subset of articles also provides information and simulations of security investments and the security economy within organizations. There are also frameworks on how to set up a secure environment with a culture and guides to good policies included.

Awareness: The role of human in information security is a substantial stream in research (Kraemer et al., 2009). Therefore organizations have to consider dealing with security awareness.

Evaluation: These articles deal with the question of which success factors lead to good management or which factors influence the success of implementing a security management system. Another aspect is the validation and verification of policies and factors which causes better ones.

3.2.2 Security Measurement

Security metrics refer to the interpretation of measurements of the security performance, level and indicators (Savola and Heinonen, 2011). Therefore

Table 2: Thematic classification of the literature.

Security management	Organization and Governance	(Geer et al., 2003; Hong et al., 2003; Trèek, 2003; von Solms and von Solms, 2004; Gupta and Hammond, 2005; Anderson and Moore, 2006; Ernest Chang and Ho, 2006; Johnson and Goetz, 2007; Veiga and Eloff, 2007; Atoum et al., 2014; Narain Singh et al., 2014; Yaokumah, 2014; Fenz et al., 2014; AlHogail, 2015; Horne et al., 2017)
	Awareness	(Straub and Welke, 1998; Velki et al., 2014; Tran et al., 2016)
	Evaluation	(von Solms et al., 1994; Kraemer et al., 2009; Abu-Musa, 2010; Hall et al., 2011; Norman and Yasin, 2012; Tu and Yuan, 2014; Alqahtani, 2015; Muthukrishnan and Palaniappan, 2016; Azuwa et al., 2017)
Security measurement	Development	(Wang and Wulf, 1997; Sharman et al., 2004; Herrera, 2005; Tanna et al., 2005; Tashi and Ghernaouti-Hélie, 2008; Sowa and Gabriel, 2009; Leon and Saxena, 2010; LeMay et al., 2011; Idika and Bhargava, 2012; Jones and Horowitz, 2012; Tariq, 2012; Bayuk and Mostashari, 2013; Zalewski et al., 2014; Mazur et al., 2015; Collier et al., 2016; Young et al., 2016)
	Taxonomy	(Vaughn et al., 2003; Savola, 2007; Savola, 2009; Verendel, 2009; Purboyo et al., 2011; Pendleton et al., 2017)
	Security Metrics	(Boyer and McQueen, 2007; Premaratne et al., 2008; Dogaheh, 2010; Jafari et al., 2010; Mermigas et al., 2013; Holm and Afridi, 2015)
	Effectiveness	(Coronado et al., 2009; Bayuk, 2013; Savola, 2013)
	Visualization	(Savola and Heinonen, 2011)
Human Behavior		(Gonzalez and Sawicka, 2002; Ifinedo, 2012; Crossler et al., 2013; Vance et al., 2014; Montesdioca and Maçada, 2015; Alavi et al., 2016)
Practical Frameworks		(IT Governance Institute, 2007; NIST, S. P., 2008; ISO/IEC, 2009; Hayden, 2010; CCIB, 2017)

measurement is the process of estimating attributes of an object while metrics refer to assign a value to an object (Pendleton et al., 2017).

Development: There are methods to develop metrics for information security aspects. Examples of them are metrics which are developed based on different approaches like Goal-Question-Metric (Savola, 2007; Bayuk, 2013) or attack-graphs (Premaratne et al., 2008; LeMay et al., 2011; Idika and Bhargava, 2012). There are also frameworks with descriptions of good metrics and how to implement them.

Taxonomy: The taxonomies in this class describe and characterize different measurement approaches and several classes of metrics which are based on the objective and the measurement goal.

Security Metrics: A security metric is a quantitative indicator for various targets in operational security (Verendel, 2009). The articles focus on specific metrics and evaluate or simulate them.

Effectiveness: The effectiveness of metrics to measure information security is discussed here. The articles compare different frameworks to generate measurements and discuss different metrics in detail.

Visualization: The management has the requirement to easily understand and therefore react very fast to changed metrics (Jafari et al., 2010; Savola and Heinonen, 2011). Therefore these articles deal with an optimal visualization of complex metrics.

3.2.3 Human Behavior

Human behavior or human factors affecting information security are not to be confused with the awareness described above. These articles deal with different behavior theories like 'protection motivation' or 'planned behavior'. The perspective of attackers is included in form of social engineering attacks and factors which can prevent them.

3.2.4 Practical Frameworks

Frameworks from practice which also called best-practices are included. They are developed for practitioners to deal with information security management systems or security effectiveness.

4 DISCUSSION

The quantitative analysis of the relevant literature revealed that under the subject of the measurement of information security many phenomena can be interpreted. An exact delimitation of the topic area from others, such as management processes, would be helpful for tracking this issue. In the case of the definitions, it can be argued that there is less research in CS and CR available than in ICT and IS. Context is the measurement of information security. Future research should pay attention to the correct and uniform use of the concepts and develop them further. The thematic classification shows potential research areas in each of the different classes. The

following part describes these research areas within the different classes based on the given literature:

Security Management: To fundamentally make decisions in the area of systems security it is necessary to know the current information security status within an organization and know the weaknesses and where they are. This is currently still a gap in research (von Solms et al., 1994; Johnson and Goetz, 2007; Tu and Yuan, 2014; Horne et al., 2017). (Mermigas et al., 2013) goes one step further and says that organizations need to know how secure they are at any given point in time. A requirement to do this is the understanding of the success factors of information security within organizations and how they are related (Kraemer et al., 2009; Norman and Yasin, 2012; Horne et al., 2017). If the security status can be operationalized it is also possible to measure if the security program as well as their countermeasures or policies of the organization are effective or not. This is also an undeveloped research task (Gupta and Hammond, 2005; Fenz et al., 2014; Atoum et al., 2014). The present literature review excludes those articles which did not contain any security success factors. Further work could show and categorize the existing direct and indirect success factors which are already in place. This could be the basis for an empirical evaluation and a better understanding of security in organizations.

Security Measurement: The measurement of security as a property and the development of security metrics itself are in a very early research stage and quite underdeveloped (Savola, 2009; Savola and Heinonen, 2011; Zalewski et al., 2014). Knowing how to measure the security as well as the defense level of organizations and generally of systems is a gap in research (Vaughn et al., 2003; Purboyo et al., 2011; Alavi et al., 2016). The area of measurement goes also a step back and asks for practices to measure the coverage of visibility. This is about effective and adequate assessments of risks and assets and how it can be monitored (Abu-Musa, 2010). Specifically, there is a gap in explored metrics for the measurement of information security, which are associated with existing models and thus provide the basis for cross-sectoral and organizational independent security comparison (Sowa and Gabriel, 2009; Bayuk and Mostashari, 2013). It is often the case that just the security management program is measured and not the security itself (Tashi and Ghernaouti-Hélie, 2008; Jafari et al., 2010). There is not just a gap in developing and creating concrete metrics but also in tools to gather information security related data and monitor the security status (Wang and Wulf, 1997; Boyer and McQueen, 2007; Crossler et al., 2013). Based on this work, current metrics in place could be shown and linked to the frameworks, success factors and development models.

Human Behavior: Human behavior is little represented in this review. In case of measurement there is an open question on how to capture actual behavior (Crossler et al., 2013).

Practical Frameworks: Practical frameworks are designed to help organizations to implement and use security related information in management. The only framework who describes metrics to monitor the security status says that these metrics are not covering the minimum security requirements (NIST, S. P., 2008). Also, the automatic way to collect and measure the data is a requirement for good and repeatable metrics (NIST, S. P., 2008). Other frameworks like (IT Governance Institute, 2007; ISO/IEC, 2009) addresses just the effectiveness of security management processes and not the security status of the assets and environment itself. An empirical evaluation or test of the described issues is not present literature.

5 CONCLUSION

There is a gap in measuring and monitoring information security in current research (D'Arcy and Herath, 2011; Crossler et al., 2013; Fenz et al., 2014; Sommestad et al., 2014). To develop a measurement and collect information security related data, it is necessary to understand information security and the success factors influencing it (Sommestad et al., 2014).

This literature review after (Webster and Watson, 2002; vom Brocke et al., 2009) included journals of the information security area as well as databases. The search process results in the identification of 70 articles which are interesting for measuring information security. The chronological analysis shows that the topic has become more and more important in the past years. Also, there are a lot of terms in place which are used in different contexts. This becomes clear as soon as the keywords, the title and the contents of the articles are compared with respect to the term. The delimitation of the terms is based on the work of (von Solms and van Niekerk, 2013) and is extended in this review based on the definitions of (Björck et al., 2015) to get an overview of the current terms and their usage. Past literature uses the terms as synonyms which should be avoided in the future.

The thematic classification of the literature can

help to capture future research and better assign them a context. It is shown that the measurement of information security is often a management topic. This is useful because the measurement allows an objective control and a well-based decision-making in connection to information security.

The relevant articles show that information security is necessary for organizations and decision-makers. To manage, make good decisions and capture the current state of information security, a measurement is needed (Bayuk, 2013). Current research does not adequately cover this topic. Future research should investigate in the definition of success factors for information security to fulfill the requirement of understanding security success factors (Kraemer et al., 2009; Norman and Yasin, 2012; Horne et al., 2017) and define a current state of security (von Solms et al., 1994; Johnson and Goetz, 2007; Mermigas et al., 2013; Tu and Yuan, 2014; Horne et al., 2017). Therefore concrete metrics and tools to monitor these need to be developed (Wang and Wulf, 1997; Vaughn et al., 2003; Boyer and McQueen, 2007; Sowa and Gabriel, 2009; Purboyo et al., 2011; Crossler et al., 2013; Bayuk and Mostashari, 2013; Alavi et al., 2016). Future research could then evaluate the effectiveness of security programs and actions based on the security quantification (Gupta and Hammond, 2005; Fenz et al., 2014; Atoum et al., 2014).

6 LIMITATIONS

The limitations are based on the search process. The initial search was performed based on highly ranked journals. Therefore it is possible that articles within conferences or not included journals could influence the results of this literature review. The same could apply for articles which are excluded based on their title and abstract. It cannot be ruled out that relevant articles have been removed which does not outline to the search topic but has relevant content. In order to limit these shortcomings, the database search, as well as the forward and backward search, was performed. Moreover, this literature review does not cover management or interdisciplinary journals which could also be interesting for measuring security.

REFERENCES

Abu-Musa, A. (2010). Information security governance in saudi organizations: An empirical study. *Information Management & Computer Security*, 18(4):226–276.

Alavi, R., Islam, S., and Mouratidis, H. (2016). An information security risk-driven investment model for analysing human factors. *Information and Computer Security*, 24(2):205–227.

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, 49:567–575.

Alqahtani, A. (2015). Towards a framework for the potential cyber-terrorist threat to critical national infrastructure. *Information and Computer Security*, 23(5):532–569.

Anderson, R. and Moore, T. (2006). The economics of information security. *Science (New York, N.Y.)*, 314:610–613.

Atoum, I., Otoom, A., and Abu Ali, A. (2014). A holistic cyber security implementation framework. *Information Management & Computer Security*, 22(3):251–264.

Azuwa, M. P., Sahib, S., and Shamsuddin, S. (2017). Technical security metrics model in compliance with iso/iec 27001 standard. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 1(4):280–288.

Bayuk, J. and Mostashari, A. (2013). Measuring systems security. *Systems Engineering*, 16(1):1–14.

Bayuk, J. L. (2013). Security as a theoretical attribute construct. *Computers & Security*, 37:155–175.

Bentkower, M. (2017). Assessing the real damage of the 'wannacry' malware attack.

Björck, F., Henkel, M., Stirna, J., and Zdravkovic, J. (2015). Cyber resilience – fundamentals for a definition. In *New Contributions in Information Systems and Technologies*, Advances in Intelligent Systems and Computing, pages 311–316. Springer International Publishing, Cham.

Boyer, W. and McQueen, M. (2007). Ideal based cyber security technical metrics for control systems. In *Critical information infrastructures security*, pages 246–260.

Bundesanzeiger (2015). Gesetz zur erhoehung der sicherheit informationstechnischer systeme (it-sicherheitsgesetz). *Bundesgesetzblatt*, 1(31):1324–1331.

CCIB (2017). *Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components, Version 3.1, Revision 5*. Common Criteria.

Collier, Z. A., Panwar, M., Ganin, A. A., Kott, A., and Linkov, I. (2016). Security metrics in industrial control systems. In Colbert, E. J. M. and Kott, A., editors, *Cyber-security of SCADA and other industrial control systems*, Advances in Information Security, pages 167–185. Springer, Switzerland.

Coronado, A. S., Mahmood, M. A., Pahnila, S., and Luciano, E. M. (2009). Measuring effectiveness of information systems security: An empirical research. In *15th Americas Conference on Information Systems*.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. (2013). Future di-

rections for behavioral information security research. *Computers & Security*, 32:90–101.

D'Arcy, J. and Herath, T. (2011). A review and analysis of deterrence theory in the is security literature: Making sense of the disparate findings. *European Journal of Information Systems*, 20(6):643–658.

Dogaheh, M. A. (2010). Introducing a framework for security measurements. In *IEEE International Conference on Information Theory and Information Security*, pages 638–641.

Ernest Chang, S. and Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, 106(3):345–361.

Fenz, S., Heurix, J., Neubauer, T., and Pechstein, F. (2014). Current challenges in information security risk management. *Information Management & Computer Security*, 22(5):410–430.

Frizell, S. (2015). Sony the interview hack: Studio spending $15 million to deal with it.

Geer, D., Hoo, K. S., and Jaquith, A. (2003). Information security: Why the future belongs to the quants. *IEEE Security & Privacy Magazine*, 1(4):24–32.

Gonzalez, J. J. and Sawicka, A. (2002). A framework for human factors in information security. In *2002 WSEAS International Conference on Information Security, Hardware/Software Codesign, E-Commerce and Computer Networks*, pages 1871–1877.

Gupta, A. and Hammond, R. (2005). Information systems security issues and decisions for small businesses. *Information Management & Computer Security*, 13(4):297–310.

Hall, J. H., Sarkani, S., and Mazzuchi, T. A. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security*, 19(3):155–176.

Hayden, L. (2010). *IT security metrics: A practical framework for measuring security & protecting data*. McGraw Hill, New York.

Herrera, S. (2005). Information security management metrics development. In *Proceedings / 39th Annual 2005 International Carnahan Conference on Security Technology*, pages 51–56.

Holm, H. and Afridi, K. K. (2015). An expert-based investigation of the common vulnerability scoring system. *Computers & Security*, 53:18–30.

Hong, K.-S., Chi, Y.-P., Chao, L. R., and Tang, J.-H. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, 11(5):243–248.

Horne, C. A., Maynard, S. B., and Ahmad, A. (2017). Information security strategy in organisations: Review, discussion and future research. *Australasian Journal of Information Systems*, 21.

Idika, N. and Bhargava, B. (2012). Extending attack graph-based security metrics and aggregating their application. *IEEE Transactions on Dependable and Secure Computing*, 9(1):75–85.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1):83–95.

ISO/IEC (2009). *ISO/IEC 27004:2009(E) - Information technology - Security techniques - Information security management - Measurement*. ISO/IEC.

IT Governance Institute (2007). *COBIT 4.1: Framework, control objectives, management guidelines, maturity models*. IT Governance Institute, Rolling Meadows.

Jafari, S., Mtenzi, F., Fitzpatrick, R., and O'Shea, B. (2010). Security metrics for e-healthcare information systems: A domain specific metrics approach. *International Journal of Digital Society (IJDS)*, 1(4):238–245.

Johnson, M. E. and Goetz, E. (2007). Embedding information security into the organization. *IEEE Security & Privacy Magazine*, 5(3):16–24.

Jones, R. A. and Horowitz, B. (2012). A system-aware cyber security architecture. *Systems Engineering*, 15(2):225–240.

Kraemer, S., Carayon, P., and Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, 28(7):509–520.

LeMay, E., Ford, M. D., Keefe, K., Sanders, W. H., and Muehrcke, C. (2011). Model-based security metrics using adversary view security evaluation (advise). In *Eighth International Conference on Quantitative Evaluation of SysTems*, pages 191–200.

Leon, P. G. and Saxena, A. (2010). An approach to quantitatively measure information security. In *3rd India Software Engineering Conference*.

Mazur, K., Ksiezopolski, B., and Kotulski, Z. (2015). The robust measurement method for security metrics generation. *The Computer Journal*, 58(10):2280–2296.

Mermigas, D., Patsakis, C., and Pirounias, S. (2013). Quantification of information systems security with stochastic calculus. In *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, pages 1–9.

Montesdioca, G. P. Z. and Maçada, A. C. G. (2015). Measuring user satisfaction with information security practices. *Computers & Security*, 48:267–280.

Muthukrishnan, S. M. and Palaniappan, S. (2016). Security metrics maturity model for operational security. In *IEEE Symposium on Computer Applications and Industrial Electronics*, pages 101–106.

Narain Singh, A., Gupta, M. P., and Ojha, A. (2014). Identifying factors of "organizational information security management". *Journal of Enterprise Information Management*, 27(5):644–667.

NIST, S. P. (2008). *800-55r1: Performance measurement guide for information security*. National Institute of Standards and Technology, Gaithersburg, MD.

Norman, A. A. and Yasin, N. M. (2012). Information systems security management (issm) success factor: Retrospection from the scholars. In *Proceedings of the 11th European Conference on Information warfare and security*.

Pendleton, M., Garcia-Lebron, R., Cho, J.-H., and Xu, S. (2017). A survey on systems security metrics. *ACM Computing Surveys*, 49(4):1–35.

Premaratne, U., Samarabandu, J., Sidhu, T., Beresh, B., and Tan, J.-C. (2008). Application of security metrics in auditing computer network security: A case study. In *4th International Conference on Information and Automation for Sustainability*, pages 200–205.

Purboyo, T. W., Rahardjo, B., and Kuspriyanto (2011). Security metrics: A brief survey. In *2011 2nd International Conference on Instrumentation, Communications, Information Technology and Biomedical Engineering*, pages 79–82.

Savola, R. (2007). Towards a security metrics taxonomy for the information and communication technology industry. In *International Conference on Software Engineering Advances (ICSEA)*, pages 60–66.

Savola, R. M. (2009). A security metrics taxonomization model for software-intensive systems. *Journal of Information Processing Systems*, 5(4):197–206.

Savola, R. M. (2013). Quality of security metrics and measurements. *Computers & Security*, 37:78–90.

Savola, R. M. and Heinonen, P. (2011). A visualization and modeling tool for security metrics and measurements management. In *2011 Information Security for South Africa*, pages 1–8.

Sharman, R., Rao, R., and Upadhyaya, S. (2004). Metrics for information security: A literature review. In *10th Americas Conference on Information Systems*.

Silic, M. and Back, A. (2014). Information security: Critical review and future directions for research. *Information Management & Computer Security*, 22(3):279–308.

Sommestad, T., Hallberg, J., Lundholm, K., and Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security*, 22(1):42–75.

Sowa, S. and Gabriel, R. (2009). Multidimensional management of information security: A metrics based approach merging business and information security topics. In *International Conference on Availability, Reliability and Security*, pages 750–755. IEEE.

Straub, D. W. and Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, 22(4):441.

Tanna, G. B., Gupta, M., Rao, H. R., and Upadhyaya, S. (2005). Information assurance metric development framework for electronic bill presentment and payment systems using transaction and workflow analysis. *Decision Support Systems*, 41(1):242–261.

Tariq, M. I. (2012). Towards information security metrics framework for cloud computing. *International Journal of Cloud Computing and Services Science (IJ-CLOSER)*, 1(4).

Tashi, I. and Ghernaouti-Hélie, S. (2008). Efficient security measurements and metrics for risk assessment. In *The Third International Conference on Internet Monitoring and Protection*, pages 131–138.

Tran, H., Campos-Nanez, E., Fomin, P., and Wasek, J. (2016). Cyber resilience recovery model to combat zero-day malware attacks. *Computers & Security*, 61:19–31.

Trèek, D. (2003). An integral framework for information systems security management. *Computers & Security*, 22(4):337–360.

Tu, Z. and Yuan, Y. (2014). Critical success factors analysis on effective information security management: A literature review. In *20th Americas Conference on Information Systems*.

Vance, A., Eargle, D., Anderson, B. B., and Kirwan, C. B. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (eeg). *Journal of the Association for Information Systems*, 15:679–722.

Vaughn, R. B., Henning, R., and Siraj, A. (2003). Information assurance measures and metrics - state of practice and proposed taxonomy. In *Proceedings of the 36th Annual Hawaii International Conference on System Sciences*.

Veiga, A. D. and Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management*, 24(4):361–372.

Velki, T., Solic, K., and Ocevcic, H. (2014). Development of users' information security awareness questionnaire (uisaq) — ongoing work. In *37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pages 1417–1421.

Verendel, V. (2009). Quantified security is a weak hypothesis: A critical survey of results and assumptions. In *Proceedings of the 2009 workshop on New security paradigms workshop*.

vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., and Cleven, A. (2009). Reconstructing the giant: On the importance of rigour in documenting the literature search process. *17th European Conference on Information Systems (ECIS)*.

von Solms, B. and von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, 23(5):371–376.

von Solms, R., van der Haar, H., von Solms, S. H., and Caelli, W. J. (1994). A framework for information security evaluation. *Information & Management*, 26(3):143–153.

von Solms, R. and van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38:97–102.

Wang, C. and Wulf, W. A. (1997). Towards a framework for security measurement. In *20th National Information Systems Security Conference*, pages 522–533.

Webster, J. and Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, 26(2):xiii–xxiii.

Yaokumah, W. (2014). Information security governance implementation within ghanaian industry sectors. *Information Management & Computer Security*, 22(3):235–250.

Young, D., Lopez, J., Rice, M., Ramsey, B., and McTasney, R. (2016). A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection*, 14:43–57.

Zalewski, J., Drager, S., McKeever, W., and Kornecki, A. J. (2014). Measuring security: A challenge for the generation. In *2014 Federated Conference on Computer Science and Information Systems*, Annals of Computer Science and Information Systems, pages 131–140.