Computers & Security 92 (2020) 101747

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

A comprehensive model of information security factors for decision-makers

Rainer Diesch[a,b,*], Matthias Pfaff[a,b], Helmut Krcmar[b]

[a] fortiss GmbH, Guerickestr. 25, 80805 Munich, Germany
[b] Technical University of Munich, Boltzmannstr. 3, 85748 Garching, Germany

ARTICLE INFO

Article history:
Received 9 January 2019
Revised 9 December 2019
Accepted 4 February 2020
Available online 4 February 2020

Keywords:
Key Security Indicators
Security Success
Security Model
Security Management Decision-Making
Expert Interview

ABSTRACT

Decision-making in the context of organizational information security is highly dependent on various information. For information security managers, not only relevant information has to be clarified but also their interdependencies have to be taken into account. Thus, the purpose of this research is to develop a comprehensive model of relevant management success factors (MSF) for organizational information security. First, a literature survey with an open-axial-selective analysis of 136 articles was performed to identify factors influencing information security. These factors were categorized into 12 areas: physical security, vulnerability, infrastructure, awareness, access control, risk, resources, organizational factors, CIA, continuity, security management, compliance & policy. Second, an interview series with 19 experts from the industry was used to evaluate the relevance of these factors in practice and explore interdependencies between them. Third, a comprehensive model was developed. The model shows that there are key-security-indicators, which directly impact the security-status of an organization while other indicators are only indirectly connected. Based on these results, information security managers should be aware of direct and indirect MSFs to make appropriate decisions.

1. Introduction

Today, most businesses are based or even fully dependent on information such as financial data for banks to stay at the market and be competitive (Knapp et al., 2006). According to thycotic, 62 % of all cyber-attacks are hitting small- and mid-sized businesses of which 60 % are going out of businesses six months after such an attack (Thycopic Software Ltd., 2017). 53 % of the attacks are causing $500.000 or more (Cisco Systems Inc., 2018) while the average cost of a data breach was $3.86 million (Ponemon Institute LLC, 2018). Not just financial losses are a risk but also legal and reputation repercussions (Tu and Yuan, 2014). Therefore, it is necessary for organizations to keep their information and the underlying technology secure against business-harming attacks.

In the past, information security was purely a technical concern and therefore, technical employees were responsible for information security issues within an organization (Willison and Backhouse, 2006). This perspective fails when it comes to a comprehensive and holistic view and the overall security strategy. Thus, in the past years, there was a shift from the executive technology expert to a management responsibility and a more business-focused view protecting information (Ashenden, 2008; Ransbotham and Mitra, 2009; Yeh and Chang, 2007). Nowadays, security managers are fully responsible to consider and respond to information security issues (Abu-Musa, 2010; Soomro et al., 2016). Various cases like the “Equifax breach” had shown the consequences for the top management in case of information security disregards. There, over 146 million personal information were stolen because of an unpatched system, which was a technical shortcoming. This causes, that the company gets rid of their CEO, CIO, and CSO by the “retirement” of them right after the breach (Bernard and Cowley, 2017). The technical personal was not affected. This goes further in manifesting the management responsibility within laws like the German Stock Corporation Act (§91 Section 2) which also requires an active risk management within companies.

Because of the shift from a technical to a management perspective, the research focus also changed from studies in a technical context to exploring the management role (Soomro et al., 2016). Managers must be able to take technical threats as well as other factors like human behavior into account to take the right and effective actions to mitigate threats (Coronado et al., 2009). To provide necessary funds, make good decisions and argue to the business, it is necessary for information security managers to

* Corresponding author at: Guerickestr. 25, 80805 Munich, Germany.
E-mail address: diesch@fortiss.org (R. Diesch).

https://doi.org/10.1016/j.cose.2020.101747

understand the complexity of information security (Willison and Backhouse, 2006) and have a comprehensive view on the topic (Soomro et al., 2016). This comprehensive view with specific factors and their interdependencies as well as the impact on the security status of an organization is still a gap in research (Diesch et al., 2018; Horne et al., 2017; Kraemer et al., 2009; Norman and Yasin, 2013; Soomro et al., 2016). Therefore, this study has the purpose to identify the key factors, evaluate them and explore interdependencies to finally generate a comprehensive model to understand the information security complexity and thus provide good information security management decisions.

The remaining research article is structured as follows. In Section 2, previous work on management practices and management success factors (MSF) in information security is described and the need for a comprehensive information security model with current shortcomings is shown. In Section 3, the three-step methodology which contains the literature survey, the literature analysis, and the expert interview series is presented. In Section 4, the evaluated MSFs are provided. The MSFs in conjunction with interdependencies are proposed as a comprehensive model in Section 5. In Section 6, a critical discussion of the results and areas for future research are highlighted. A conclusion is given in Section 7.

2. Background and motivation

This chapter is divided into three sections. In Section 2.1, standards and best practices in information security management for practitioners and their shortcomings are described. In Section 2.2, the term MSF and the current state of the art in research regarding this topic is introduced. In Section 2.3 the need for practitioners, as well as the gap in the literature, are highlighted to motivate this research.

2.1. Standards and best practices

Information security management is often build based on international standards or best practices (Hedström et al., 2011). The terms “standard” and “best practice” are often used as synonyms but “standards” are usually checked by an international standardization organization while “best practices” and other frameworks are published independently.

The most common standard from such an organization is the ISO/IEC 27000-series (ISO/IEC, 2018). This standard is widely accepted, play an important role and it is possible to certify the organizational information security based on it (Siponen and Willison, 2009). The ISO/IEC 27000-series defines basic requirements in order to implement an information security management system. Also, control guidance, implementation guidance, management measures, and the risk management approach is specified. Special sub-norms are also included in the series, for example, the ISO/IEC 27011 which deals especially with telecommunication organizations.

In addition to the information security management standard, there are frameworks or best practices like the NIST SP800-series (NIST, 2018b), the Standard of Good Practices from the Information Security Forum (ISF) (ISF, 2018) or the COBIT framework (ISACA, 2012). These best practices are used to implement an information security management system (ISMS), define and develop controls and address the most pressing problems regarding information security with an overview for their risk mitigation strategy (Mijnhardt et al., 2016). All in all, security standards provide a common basis for organizations to help reducing risks by developing, implementing and measuring security management (Ernest Chang and Ho, 2006).

Information security management certificates do provide a basic assurance level and show that some security measures are available. But in practice, experts are skeptical about certificates. Experts mentioned, that standards do help with compliance but not always help to reduce risk or improve security (Johnson and Goetz, 2007). Lee et al. (2016) show, that a higher security standard does not necessarily lead to a higher security level. The following shortcomings of standards were highlighted in the past literature:

(1) Well known standards are very generic in scope and tend to be very abstract (Siponen and Willison, 2009). For these standards, concrete countermeasures and combinations of them are missing, which leads to inefficient or even misleading risk mitigation strategies (Fenz et al., 2013).
(2) Standards consists of a huge amount of information. For example, the ISO 27000-series consists of 450 items with 9 focus areas. This complexity and the fact, that there are rarely fully implemented standards in small- and medium-sized businesses in place, leads to a fall back to ad-hoc implementations. An easy to understand toolkit is missing (Mijnhardt et al., 2016).
(3) The defined controls and countermeasures of the frameworks are often implemented without sufficient consideration of the daily work or their need (Hedström et al., 2011). This is because the organization usually do not consider the relationships between the security concepts (Fenz et al., 2013) and do not check whether a control is really necessary or less critical (Bayuk and Mostashari, 2013; Tu and Yuan, 2014).
(4) Rigorous empirical studies which consider different factors which may affect the decisions and validate the standards and best practices are missing in literature (Diesch et al., 2018; Siponen and Willison, 2009).
(5) There are regional differences in the use and contexts of frameworks. For example, the NIST SP800-series is “developed to address and support the security and privacy needs of U.S. Federal Government information and information systems” (NIST, 2018b) while the current standard in Australia is the ISO/IEC 27000-series (Smith et al., 2010). Therefore the NIST SP800 framework “is individually useful but (outside of the U.S.) do not provide a cohesive and explicit framework to manage information security” (Smith et al., 2010).

2.2. Information security success

Besides standards and best practices which were described before, there are theories and concepts in the literature which help decision-makers in information security. Managers need to know the current information security status of their organizational assets to make decisions. If there are not well protected, they need possible sets of controls with the consideration of the related costs to improve the information security situation (Diesch et al., 2018; Horne et al., 2017; Johnson and Goetz, 2007; Tu and Yuan, 2014; von Solms et al., 1994).

The literature deals with MSFs to describe the state of information security which is needed in practice. The term was used first in 1987 to describe factors which take into account as “catalysts to generate new and more effective systems security activities” in the security context (Wood, 1987). After that the theory of information systems success of DeLone and McLean (1992) deals with different dependent and independent variables, which are indicating a successful information systems strategy and that they can be categorized into dimensions. Recent studies used other terms in the context of information security:

1. “Information systems security management success factors” are factors to show the state of elements, which has to anticipate

preventing information security failure in the e-commerce context (Norman and Yasin, 2013).
2. "Critical success factors" describe factors, which influence the successful implementation of an information security management system (Tu and Yuan, 2014).
3. "Critical success factors are described as key areas in the firm that, if they are satisfactory, will assure successful performance for the organization" (Tu et al., 2018).

In this research, management success factors (MSF) are defined as factors to show the state of elements, which has to take into account in order to make appropriate management decisions in the information security context of an organization. If the security decisions are appropriate, it assures a successful security performance for the organization.

Current literature mostly looks on factors which influence security separately. To highlight just a view studies, they separately deal with organizational factors (Ernest Chang and Ho, 2006; Hall et al., 2011; Kankanhalli et al., 2003; Kraemer et al., 2009; Mijnhardt et al., 2016; Narain Singh et al., 2014), policy compliance issues (Boss et al., 2009; Goel and Chengalur-Smith, 2010; Höne and Eloff, 2002; Ifinedo, 2012; Johnston et al., 2016; Lowry and Moody, 2015a) or human factors (Alavi et al., 2016; AlHogail, 2015; Ashenden, 2008; Gonzalez and Sawicka, 2002; Kraemer et al., 2009). The reason for the separation is, that security is managed in a separate manner in different departments which includes information security, risk management, business continuity, operational security (Tashi and Ghernaouti-Hélie, 2008). This shows that various studies are available which do discuss different factors in great detail but do not include a integral view on them. There are just a view attempts to consolidate the body of knowledge in comprehensive MSFs. The information systems success theory explains six factors which are contributing to the systems success (DeLone and McLean, 1992). This view does not include specific security considerations including the costs and available countermeasures that a manager must consider. The authors self-criticized the proposed theory because of the missing evaluation. The only other success factor model was a model of factors, influencing the successful implementation of an information security management system (Norman and Yasin, 2013) and not the security decisions of managers itself.

2.3. Shortcomings in literature and practice

As the Sections 2.1 and 2.2 suggest, there are a view shortcomings in literature for supporting decisions on the security management level. A recent survey of McKinsey & Company with 1125 managers involved in 2017 identified three main problems, managers face in order to deal with information security issues (Boehm et al., 2017). These are *the lack of structure* within reports with dozens of indicators with inconsistent and too-high levels of details. The *lack of clarity* because of reports, which are too technical which a manager typically not understand. A *lack of consistent real-time data*.

The *lack of clarity* within reports is not just present in practice. Managers do not know all technical details and do not need them because of their teams and experts (Fenz et al., 2013; May, 1997). But they have to establish a security establishment and have to improve the security status by using a security dashboard (Dogaheh, 2010). The reports and dashboards have to be on the need for information security managers (Wilkin and Chenhall, 2010) but there are no standards for the content of such dashboards (Bayuk and Mostashari, 2013). The *lack of structure* is related to the first problem and causes in the high diversity and complexity of the information security problem which causes uncertainty and confusion among top managers (Savola, 2007; 2009; von Solms et al., 1994; Willison and Backhouse, 2006). This causes in the fact, that managers do not make decisions based on data but on their experience, judgment and their best knowledge (Chai et al., 2011). Therefore, current research asks for a comprehensive approach to information security management (Abu-Musa, 2010; Nazareth and Choi, 2015; Savola, 2007; 2009; 2013; Soomro et al., 2016; Tu and Yuan, 2014) which captures the definition of "factors that have a significant impact on the information security" (Bayuk, 2013; Leon and Saxena, 2010; Ransbotham and Mitra, 2009; Soomro et al., 2016) and the established relationships between these fundamental objectives (Dhillon and Torkzadeh, 2006; Hu et al., 2012; Soomro et al., 2016). This research addresses the described needs with the development of the first theory of interrelated MSFs, which give a basis for decision-makers to understand the complexity of information security on an abstract level and also could be the basis of multiple future needs also described in literature like the goal based security metrics development (Bayuk, 2013; Boss et al., 2009; Diesch et al., 2018; Hayden, 2010; Jafari et al., 2010; Johnson and Goetz, 2007; Pendleton et al., 2017; Savola, 2007; Zalewski et al., 2014).

3. Methodology

To develop a comprehensive model of information security factors for decision makers the methodology of this work consists of two steps. Fig. 1 illustrates the steps. The first step is to find relevant literature with the help of a literature search process described in Section 3.1. The second step is to analyze the relevant literature for factors which have an influence on information security decisions. The results are categorized and high-level impact factors which are derived from literature. This step is illustrated in Section 3.2. The third step contains a semi-structured expert interview in order to evaluate the relevance of the impact factors in practice and explore interdependencies between them. The results are evaluated and relevant MSFs in practice as well as interdependencies which results in the comprehensive model of MSFs for decision-makers. In Section 3.3 the description of the expert interview methodology is shown.

3.1. Literature search

The search process is performed based on the method of Webster and Watson (2002). The literature search consists of the search scope followed by a keyword-search which ends in a forward and backward search. To provide high-quality articles, the scope is set to highly ranked journals within the information security domain and the information systems management domain because of the relation to the management view. Journals of the management domain were selected from the Senior Scholars' Basket of Journals (AIS Members, 2011). The journals of the security domain were selected from the Scimago Journal & Country Rank (SJR) (SJR, 2018) with the condition that they need to be part of the following categories: security, safety, risk or reliability. To not limit the search only to Journals, the scope was extended to several databases. These are ScienceDirect, OpacPlus and Google Scholar. OpacPlus is a wrapper of multiple databases including Scopus, Elsevier, Wiley, and ACM Digital Library. The results of Google Scholar were limited by 100 hits because the most relevant articles can be found within the first sites (Silic and Back, 2014). After the scope definition, the following search string was used to find articles: "(it OR information OR cyber)AND (resilience OR security)AND (factors OR kpi OR measures OR metrics OR measurement OR indicator OR management)". Because the management literature is not information security specific, the search string of these journals was adjusted to the first two parts: "(it OR information OR cyber)AND (resilience OR security)". Another adjustment

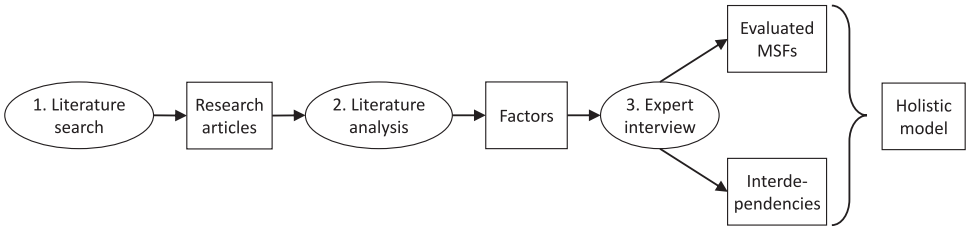

Fig. 1. Methodology of theory development.

was done by searching just for the title and abstract within information security specific sources because of the underlying diverse topic. The selection of relevant articles out of the first keyword search was done based on the title and abstract. Including criteria was, that there are factors described or mentioned which are influencing information security decisions. The forward and backward search was applied to all selected articles while the forward search was based on the "cited by" function of Google Scholar. The literature identification methodology results in 136 articles. The complete search matrix with the applied source, the keyword-search hits and the selected relevant article numbers is shown in Appendix A.

3.2. Literature analysis

The analysis was done based on the "open-axial-selective" approach of Corbin and Strauss, 1990 which is a grounded theory approach based on Glaser and Strauss (1967) and was recommended as a rigorous method for analyzing literature (Wolfswinkel et al., 2013). This approach has the advantage, that the whole context of an article can be analyzed in order to extract factors. Webster and Watson (2002) also support a literature analysis but with the categorization of a whole article in order to identify gaps in the literature, pointing out the state of the art and explaining past research. To extract specific knowledge and categorize this, the coding on a textual level of articles is more appropriate in this case. The coding follows the following steps:

(1) Assignment of text segments to a "first-order code". For example, the text segment those organizations that have had a systems security function for some time should use these assessment methods to validate the results of other methods and to cross-check that they have not overlooked some important vulnerability" (Wood, 1987) was assigned the cluster "vulnerability assessment" as a factor which influences information security.
(2) Combines synonymous and their meanings to a "second-order code".
(3) Categorize the "second order codes" to clusters based on overlapping meanings (infrastructure overview and asset knowledge), overlapping functions (management support and management standards) or theoretical constructs (confidentiality, integrity, and availability).

3.3. Expert interview

Previous research has been criticized in order of missing support of reliability and validity by empirical studies (Siponen and Willison, 2009; Tu and Yuan, 2014). The first goal of the expert interview was to evaluate the factors of the literature and thus generate MSFs which are relevant in practice. The second and main goal is the exploration of interdependencies between MSFs to develop the comprehensive model of MSFs.

There are various ways to design an expert interview. This study is designed as a semi-structured interview (Bortz and Döring, 1995) to combine the advantages of structured and open interviews. The interviewer is able to give room for explanations but also ensures, that all answers are given. With these considerations, the expert interview itself consists of three steps which are the operationalization of the described goals (chapter 3.3.1), the selection of experts (Section 3.3.2) and the analysis of the expert interviews (Section 3.3.3).

3.3.1. Operationalization

The interview guide gives the interviewer an orientation and an analysis is more comparable than without any structure. To develop the survey instrument, the rules of good expert interviews were considered (Bortz and Döring, 1995). The beginning of the interview was done with an open question on the most important factor, the interviewee considers for the information security in the organization (*Q0*). The following areas were discussed with the experts to support the given goals and control as well as confirm the validity of the factors:

- Evaluationof factors:
  A discussion about the meaning of each factor from a practical perspective was done in order to evaluate the content of the factors (*Q1.1*). The practical relevance was tested by asking about the importance of each factor for the information security of the organization (*Q1.2*).
- Exploration of interdependencies:
  To explore the interdependencies between the factors and get insights into them, a discussion about the practical usage and how the experts deal with each factor was done (*Q2.1*). To crosscheck the given statements, experts were asked for each factor, if the factor has a direct impact on the information security of the organization (*Q2.2*).
- Control questions:
  Questions about the absence of not mentioned important factors (*Q3.1*) and if the experts consider a factor which was discussed to be unimportant (*Q3.2*) are used to control the completeness of the given factors and further confirm the explored results.

3.3.2. Expert selection

An expert is a person with specific practical or experimental knowledge about a particular problem area or subject area and is able to structure this knowledge in a meaningful and action-guiding way for others (Bogner et al., 2014). The selection of interviewees was derived by this definition. Therefore, an expert should have several years of experience in the field of information security which points to specific practical knowledge in the field of information security. The expert should have a leading position within the organization which testifies the ability to the meaningful and action-guiding structuring of the information for others. Also, a leading position supports the underlying comprehensive view which is required for the goal of this research. The selection results in 19 participants. They were mainly chief information security officers (12) and information security officers (4). The

others were one chief executive officer, one chief information officer, and a technical delivery manager. All experts had 5 years of experience at minimum, 16 years at average and 30 years at maximum. This shows, that the selected interviewees meet the requirements and are suitable for this approach. The participants worked in the following industries at this point in time: finance, automotive, diversified, aircraft, metal and electrical, services, hardware and software, and others. All but one organization had more than 2000 employees. This was the result of the requirements for experts which mean, that the organization has to had at minimum an information security team, which is typically not available in small businesses.

3.3.3. Interview analysis

The interviews were analyzed according to Mayring (2015). The basis for each question was a full transcript of the interview. The process contains of the following steps:

1. Paraphrasing
   - Painting of components that do not contribute or have little content.
   - Standardize language level.
   - Generate grammatical short forms.
2. Generalization
   - Generalize paraphrases on an abstract level.
   - Generalize predicates in an equal form.
   - Generate assumptions in case of doubt.
3. Reduction (can be done multiple times)
   - Delete phrases which have the same meaning.
   - Combine phrases of similar meaning.
   - Select phrases that are very content-bearing.
   - Generate assumptions in case of doubt.

To analyze quantitative aspects or interdependencies, Mayring (2015) also suggests two methods which are called "valence or intensity analysis" (V) and "contingency or interrelation analysis" (I) and used to analyze the interviews. Both methods contain mainly the same steps:

1. Formulate a question.
2. Determine the material sample.
3. Define the variables (V) / text modules for interrelation (I)
4. Define the scale (V) / rules for interrelation (I)
5. Coding
6. Analysis
7. Presentation and interpretation

4. Management success factors

The prerequisite for a comprehensive model of MSFs is evaluated MSFs, which have an influence on information security decisions. In Section 4.1, the results of the literature analysis are shown. These are factors which have an influence on information security decisions from the literature perspective. After that, the factors have to be evaluated and proved for their relevance in practice which results in evaluated MSFs. These results are shown in Section 4.2.

4.1. Factors derived from the literature

The analysis of 136 relevant articles from the search methodology resulted in 188 first-order codes. A code is a tuple of "factor in literature"-"author". So for each author, the different impact factors were coded. These codes appear in the following situations:

(1) They appear **directly** within the literature. An example is the following sentence of Atoum et al. (2014) "enrich the framework in other related dimensions such as *human resource, organization structures, global governance, regulation regimes, awareness programs* and thus provide a more detailed framework". This result directly in the corresponding list of first order codes. Most of these direct codes appear in enumerations within the introduction or future work sections of the analyzed literature and are not further explained.

(2) The first order codes are part of a **theory**. The first order codes are part of a hypothesis construct with a underlying theory and are tested with quantitative or qualitative studies. A example work is Kankanhalli et al. (2003) which describes the impact of the organizational size, the top management support and the industry type on the information systems security effectiveness. This example results in the corresponding first-order codes.

(3) **Indirectly** within the articles or because of their focus. These appearances are derived from the overall classification of the articles or some descriptions within the text which are not directly mention the first order code but the meaning was chosen to name it. The article with the title "design and validation of information security culture framework" (AlHogail, 2015) is named "security culture" as a first-order code. A other example for indirect mentions is those organizations that have had a systems security function for some time should use these assessment methods to validate the results of other methods and to cross-check that they have not overlooked some important vulnerability" (Wood, 1987) which is "vulnerability assessment" as a first-order code.

The aggregation of the 188 first-order codes results in 44 second-order codes. The following aggregation criteria were identified:

(1) Articles describe often, that the codes have the **same meaning**. An example is given by Jafari et al. (2010) which described "Safeguards: Protective measures prescribed to meet the security requirements [...], synonymous with countermeasures". This in conjunction with "improving the overall information security state by selecting the best security countermeasures (controls) to protect their information assets" (Yulianto et al., 2016) are safeguards, countermeasures, and controls a second-order code.

(2) Certain first-order codes are **part of** or included in other first-order codes which results in a second-order code. Examples in literature are "Value delivery (i.e. cost optimization and proving the value of information security)" (Yaokumah, 2014), "aside from the personnel measures which focus on human behavior" (Sowa and Gabriel, 2009) or "threats, which form part of such risk" (Willison and Backhouse, 2006). This indicates, that threats are part of risks.

(3) First-order codes are aggregated in order of their **underlying object**. An example is "organizational size", "industry type" and "organizational structure" which are all features of an organization and thus are aggregated to the second-order code "organizational factors".

The aggregation of the second-order codes to clusters and thus the overall factors, influencing security decisions, is based on common theories in literature. An example is the theory of the protection goals of information security which is supported by various authors: "with a goal to compromise Confidentiality, Integrity, and Availability (CIA)" or "it also coincides with the Confidentiality-Integrity-Availability (CIA) framework" (Goldstein et al., 2011) or "one view, which gained especially wide popularity, is called C-I-A triad" (Zalewski et al., 2014). This theory results in the consolidation of protection goals in the factor "CIA".

The result of the literature analysis is 12 factors influencing security decisions, namely: "Vulnerability", "Compliance & Policy",

"Risk", "Physical security", "Continuity", "Infrastructure", "CIA", "Security management", "Awareness", "Resources", "Access control" and "Organizational factors". The detailed codes and the aggregation steps are available in Appendix B.

The literature analysis confirms the assertions made in Section 2.3 which say that various individual factors are mentioned, enumerated or examined. However, up to now, there has been no comprehensive view on them, a discussion of the practical relevance is missing and the interdependencies of the factors among each other are not described. The result of this chapter gives an abstract view of current factors in literature, influencing information security decisions.

4.2. Evaluation of Factors

The explored factors of the last Section 4.1 are the basis for the following evaluation and therefore to transform these factors to MSFs for information security decision-makers. In Section 4.2.1 the practical view of experts on the factors is compared to the literature view which is derived out of the literature analysis in Section 4.1. In addition, challenges of practitioners are supported for each factor. The result of the relevance validation is present in Section 4.2.2. Section 4.2.3 contains the result of the control questions and thus confirm the validity and relevance of the explored factors.

4.2.1. Content validation of MSFs

The relevance of the factors in practice and their validity makes them to MSFs. The general context analysis (Section 3.3) was used to determine the practical usage and meaning of the different factors out of the literature. To analyze them, the scope was set to the whole interview transcripts while the main answers are given by the guiding question *Q1.1* of the interview guide. Because of the methodology design of a semi-structured interview, the challenges and problems of each factor in practice is a side-result and also reported here. The following itemization shows each MSF with a description of the literature view, a consolidated practical view and the challenges practitioners face regarding each MSF. The literature view is a consolidation of definitions and opinions out of the literature analysis 3.3.3. The practical view and the descriptions of the challenges are a consolidation of the main opinion of all 19 experts.

- **Vulnerability**
  1. **Literature:** The definition of a vulnerability in literature is generally a "weakness of an asset or control that can be exploited by one or more threats" (ISO/IEC, 2018). This definition is very generic and can be technical as well as non-technical. NIST gives a more detailed definition as a "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source" (NIST, 2018a). Common usage of the term in the analyzed literature is, that vulnerabilities are technical in nature. More specifically, "a vulnerability is a software defect or weakness in the security system which might be exploited by a malicious user causing loss or harm" (Joh and Malaiya, 2011).
  2. **Practice:** Vulnerabilities from the management perspective are always technical in nature. Specifically, known vulnerabilities within systems and software are meant by them. The common understanding of the experts was that vulnerability is a topic of patch management and a problem of not patched systems. All organizations do have patch management in place and try to minimize the vulnerabilities in the infrastructure. The assessment of them is done with vulnerability-scanners, penetration-tests, automatic scans, audits and the definition of toxic software which is detected on systems. Patching and the elimination of vulnerabilities are done based on the given assessment methods.
  3. **Challenges:** A problem is, that the vulnerabilities have to be known first. Not just the knowledge of the vulnerabilities is a problem but also the knowledge of the assets and the whole infrastructure of an organization is a challenge in practice. Just if an organization knows the whole assets and infrastructure, it is possible to determine, if there are known vulnerabilities or not.
- **Infrastructure**
  1. **Literature:** Infrastructure does have different aspects. Components are technical systems which itself try to protect the underlying assets or are there to identify attacks. Examples are firewalls, intrusion detection systems, information visibility, compromise detection, defense modeling, and other solutions. A second important concern is the prevention of attacks without any known vulnerabilities. This includes architectural decisions to segment the network, limit open access points or external connections, harden the systems, encrypt the communication or clean configuration issues. Since these are no specific vulnerabilities but considered as weaknesses, this topic is a stand-alone factor.
  2. **Practice:** Some of the experts see this factor as a vulnerability-topic but most of them associate more than that with the infrastructure factor. It is about knowing all systems and software as well as the connections between them and if they are secured or not. It is also about the "hardening" of all available systems, make threat models and secure the infrastructure in each network layer. To accomplish that, the experts use hardening-guidelines, secure deployment, installation routines, design reviews and configuration management databases.
  3. **Challenges:** Problems are the complexity of the activity, that it is difficult to check the wright implementation of the hardening guidelines and the above-mentioned problem of the difficulty to know all available systems and their connections.
- **Compliance & Policy**
  1. **Literature:** Security policies are an "aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information" (NIST, 2013). All activities concerning compliance and policies like policy deployment, policy effectiveness, legal compliance, and regulatory requirements are subsumed in this factor. The literature describes also multiple characteristics for good and bad policies and controls which have an influence on the information security of organizations.
  2. **Practice:** This factor means the implementation of requirements which are given from external and internal. These include laws, policies from the management and requirements from standards to get certificates. Practitioners use frameworks to implement them and audits as well as self-assessments to check them. This frameworks and policies help organizations which have not the common knowledge to consider all aspects of security.
  3. **Challenges:** 100% compliance does not mean 100% secure. This factor alone does not help in case of security but without, it is not possible to make audits or push measures through.
- **Security management**
  1. **Literature:** This factor subsumes all process activities within the information security management system and operational tasks like change management, incident management, process effectiveness measurement and the implementation of security standards. All aspects of the Plan-Do-Check-Act

approach of the ISO/IEC 27000 (ISO/IEC, 2018) are part of the security management factor. The other part are strategic topics like goal definition, top management support, governance, and strategic alignment as well as the documentation of these activities. Also, an important aspect in literature is the communication with employees and the top management. The ISO/IEC 27000 defines security management as a "systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives" (ISO/IEC, 2018). This definition shows that the monitoring part is also established within this factor. There are different methods and processes described to continuously improve the information security of an organization. This covers the implementation of metrics and the topic of compromise detection.

2. **Practice:** There are two management approaches in place. The risk-based and the control-based approach. There are various processes in place to support the two different approaches. Therefore the experts control their management processes with audits and using the Plan-Do-Check-Act framework from the ISO/IEC 27000 (ISO/IEC, 2018). The next important aspect for the interviewees was the business (top) management support and their understanding of the risks the organization is facing.
3. **Challenges:** A problem is the missing knowledge of concepts behind the security processes and also the lack of knowledge of available actions for improvements. The security management does not have an impact on the security of an organization without this knowledge.

- **Awareness**
  1. **Literature:** The definition of awareness in literature is to be aware of security concerns (NIST, 2013). Awareness in academic literature is discussed in different subjects. Including in this factor are behavioral topics like employee behavior, user activities, user interaction but also user reaction, user errors, and faults. All parts depending on knowledge like skills, education, training, and competence are also including in the awareness factor. Awareness in literature is not just about peoples behavior but also the personal needs of them, privacy issues, trust concerns as well as cultural thoughts and the social environment.
  2. **Practice:** All topics that concerning people and can not be treated with technology are subsumed by awareness. Typical understanding is the employee as a vulnerability with human errors, human behavior or not enough knowledge. A typical countermeasure is web-based and conventional training. Practitioners test their employees with own phishing-campaigns or check click-rates on their proxy-servers. Cultural and privacy concerns are not often taken into consideration.
  3. **Challenges:** Challenge in practice is, that awareness activities are very resource heavy and the effects are not that huge. Countermeasures often do not lead to measurable effects, they lead to annoyed employees and therefore, employees more often fail the same tests.
- **Risk**
  1. **Literature:** The risk factor is discussed as an overall risk management concern with possible threats, the likelihood of their occurrence and the possible impact on the organization. Literature mostly discusses the risk management process and the possible handling of present risks like prevention, tolerance, exposure, prediction, and perception. A comprehensive definition is given by the NIST SP800-37: "A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence" (NIST, 2018a).
  2. **Practice:** Experts use the same definition and understanding of risk as in literature. A risk is a severity and likelihood combined with an issue. Information security is the applied risk management because it is used to prioritize and define countermeasures. Therefore, all of the experts have risk management based on certain standards like ISO/IEC 27000 or NIST in place.
  3. **Challenges:** Not all risks can be mitigated, because of missing resources or other restrictions. Some managers also have problems to define risks which are understandable for technical employees or even for the top management. Also, the availability of the underlying data is a challenge in practice. An example of this is the consolidated view on possible threats. There are various technical solutions like threat intelligence platforms available on the market which helps to consolidate these data. The problem comes with the combination of the different factors to define the risk. A possible threat alone is not important for the information security management. The challenge is to analyze the underlying assets and their vulnerabilities and check if the threat can exploit one of these. After this combination, the risk can be defined and is useful for an information security manager.
- **Access control**
  1. **Literature:** Access control is not mentioned as a part of countermeasures. This topic is such important that it often emerges as an independent and important factor for security. Access control contains account management, software access control as well as access rights. It means "to ensure that access to assets is authorized and restricted based on business and security requirements" (ISO/IEC, 2018).
  2. **Practice:** Access control is the management and regulation of access to systems, applications, data, and infrastructure. It is not just about the access but also the key management, role administration, classification of data and the management of the identities within organizations. Therefore the experts have procedures per applications, try to implement the common principles like the need-to-know- or the least-privilege-principle. They check the available accesses, have identity and access management in place and use tools to monitor them.
  3. **Challenges:** Challenges occur in case of on-, off-boarding and department changes as well as the more and more open culture of organizations with "bring your own device" and "cloud infrastructure". Not just the open culture but also technologies and trends like the "internet of things" and "mobile devices" are increasingly a problem for this factor because each of these devices also has an identity. This increases the complexity of managing access control and has to be considered by choosing such technologies.
- **CIA**
  1. **Literature:** This factor is based on the overall theoretical construct of the protection goals of information security. Therefore the codings confidentiality, integrity, availability, as well as underlying goals like the non-repudiation, are subsumed in this factor. Articles about security metrics and security success are mostly based on this factor and plays a huge role in the security discussion.
  2. **Practice:** In practice, this factor is a theoretical construct with the same definition as in literature. It is used to communicate with the business management, to classify the need for protection or is not used in practice at all.
  3. **Challenges:** The problem in practice is that these classes can not be uniquely assigned to countermeasures. Many experts

consider this factor as an academic construct, which is outdated and not really practicable.

- **Organizational factors**
  1. **Literature:** The organizational factor itself means the properties of an organization which has an influence on the security of this organization. There are multiple authors which mentioned the influence of several factors like the organizational size, the industry type or the internal and external structure of the organization.
  2. **Practice:** These factor has the same meaning in practice like in literature. Most of the experts are not dealing with it because there are no possibilities to change the characteristic of the organization from their perspective. But it is considered in other factors like risks or in consideration of the implementation countermeasures. Practitioners say, that it might influence the possibilities of an organization.
  3. **Challenges:** A challenge is, that some attack surfaces are not influenced by any type of character an organization could have. A good example of this is ransomware which does not even look at the victim they attack.
- **Physical security**
  1. **Literature:** This factor have influence in reducing the opportunity to access assets physically in form of physical entry controls, the protection of the environment, building security with fences or other countermeasures, travel security and all activities around this. The literature does not mention this factor very often but consider it as really important for organizations and their management.
  2. **Practice:** Physical security is the physical protection of buildings, offices, servers, and hardware. It also contains the protection of the environment, persons, traveling and environmental disasters. Interviewees do work together with other departments dealing with this factor. It is mainly not the part of the security department of an organization.
  3. **Challenges:** The topic gets less important in times of the changing environment like mobile offices, roaming-users, home offices and cloud computing. This change brings with it other challenges.
- **Continuity**
  1. **Literature:** Continuity is split in business continuity and IT continuity. In case of cyber security, the term "refers to the ability to continuously deliver the intended outcome despite adverse cyber events" (Björck et al., 2015). The business continuity is on a more abstract level than cyber or it continuitiy and is defined as a "predetermined set of instructions or procedures that describe how an organization's mission-essential functions will be sustained [...] before returning to normal operations" (NIST, 2013). Resilience is not often represented in the literature and has already been identified as a research gap (Diesch et al., 2018).
  2. **Practice:** This factor is understood as the goal of the business as well as a partial goal of information security. Important is a continuous IT and a disaster and recovery plan which should be tested from time to time. There are opposite opinions in relation to business continuity management (BCM). Some experts say, that requirements come from the BCM to the information security management and others say, that they are being submitted to the BCM.
  3. **Challenges:** A challenge is finding a common understanding and effective communication between BCM and IT continuity.
- **Resources**
  1. **Literature:** Resources are not just money but also the availability of good skilled and well-educated employees. More general resources are "information and related resources, such as personnel, equipment, funds, and information technology" (NIST, 2013). The literature describes this factor as a limitation and mostly in a negative way. The perspective is given that, if you do not have enough resources, the organization is not able to implement security which as a negative influence. A second part is the cost-effectiveness of countermeasures and the return on security investments (ROSI).
  2. **Practice:** In practice, this factor is mostly addicted to budget, which has to be given by business management. A small part is also the number of employees with good knowledge and a appropriate education. Therefore, experts have applied budget-processes and recruitment campaigns. Cost-effectiveness and ROSI is not mentioned by the practitioners.
  3. **Challenges:** Problems are often in place of buying expensive tools and equipment in the security field and the argumentation of their adding value. It is often a tension between business management and security management.

Table 1
Importance of MSFs for the information security of organizations (number of experts).

MSF	not imp	rather not imp	rather imp	imp
Vulnerability	0	0	7	12
Resources	0	0	7	12
Awareness	1	0	6	12
Access Control	0	1	8	10
Physical Security	1	0	11	7
Infrastructure	0	1	12	6
Risk	0	1	12	6
Continuity	1	1	13	4
Security Management	3	1	8	7
Organizational	3	4	11	1
CIA Triad	7	1	8	3
Compliance & Policy	6	3	7	3

Partial aspects of individual factors are not covered by the literature or are not considered in practice. However, the contents and the understanding of the factors from the literature analysis agree with those of the experts. The challenges are not supported by all of the experts, because this was no explicit question. Thus, they were just included, if there are more than 2 mentions of the same challenge. The challenges further indicate, that a comprehensive model of them could help, improving the understanding of information security within organizations and also to help, improving specific factors.

4.2.2. Relevance validation of MSFs

The "valence or intensity analysis" (Section 3.3) was used to not just validate the factors concerning their content but also to determine their relevance in practice to the information security of an organization. Therefore, the scope of the analysis was also set to the whole interview transcripts but the main question supporting this validation is *Q1.2*. A 4-point Likert-scale which points out the importance of the factor for the information security of the organization is used. The coding of the scale is from not important (not imp) to important (imp). Table 1 shows an assorted view of the result. The assortion is based on the sum of the codings for "not important" and "rather not important" in conjunction with the sum of the coding "rather important" and "important", descending by the importance of the MSFs.

This result support, that all factors are relevant in practice. The last three factors are "Organizational factors", "CIA" and "Compliance & Policy". For all of them, the experts do have an explanation, why they are less important than the other factors. "Compliance & Policy" are not important for the information security of the organization itself but are necessary to comply with the law, to enforce countermeasures and to align the top management of the organization. The "CIA" factor is a goal factor and is useful to com-

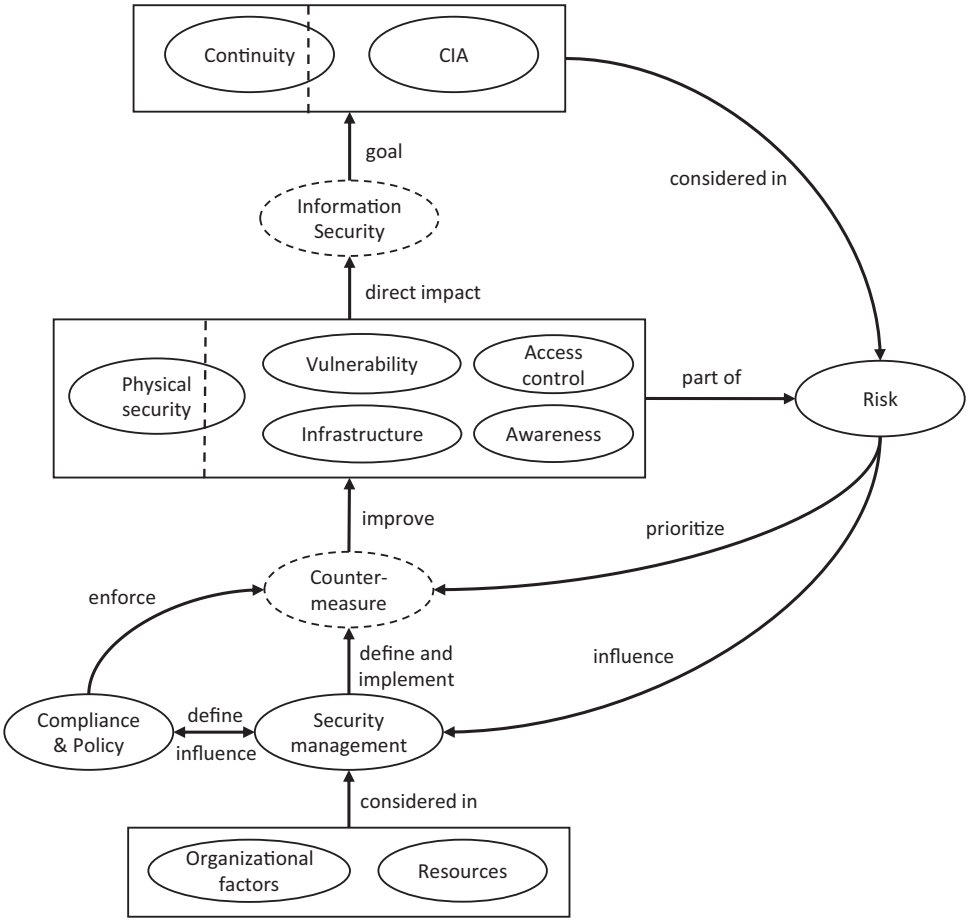

Fig. 2. A comprehensive model of MSFs for information security decision-makers.

municate and explain different risks or attacks and their impacts. "Organizational factors" are less important because there are cases, in which these factors are important but there are also attack scenarios in which this factor is not important. The management has to consider all the factors in order to make good decisions. The proposed factors are valid in their context as well as relevant in practice for decision-makers and thus are now called management success factors (MSFs).

4.2.3. Control questions

The main control questions *Q3.1* and *Q3.2* are used to ask for factors, which are important to make decisions and are not present in the interview guide as well as a consideration of the most unimportant factor. The most experts (12) do not have a factor, which is really unimportant. The only mentions of factors were the "Compliance & Policy" as well as "CIA" which agree with the ranking on the previous result. The question of missing factors results in a similar situation like before. 10 experts do not mention missing factors. The other factors which are missing are "management support", "external interfaces", "threat landscape" and "strategy" which are part of the coding and thus included in the aggregation of the literature analysis.

5. A comprehensive model of MSFs

The purpose of this research was the development of a comprehensive model of MSFs for information security decision makers. This result section combines the previous results with evaluated and relevant MSFs and adds interdependencies between them. The interdependencies were explored with the help of the "contingency or interrelation analysis" method (Section 3.3). The scope is the whole interview which was analyzed. The following text modules are examples to identify interrelations:

- ...have a direct impact on...
- ...is a basis to...
- ...is essential for...
- ...is the goal from...
- ...is considered in...

Fig. 2 shows all MSFs with their interrelations based on the expert interview. Solid ovals are representatives for the MSFs. Dotted ovals are representatives of concepts necessary to explain certain interdependencies. In this case, "Information security" is the representative for the information security status of an organization. The statement behind this is, that certain factors do have a direct impact on the information security status of the organization. The dotted oval "Countermeasures" is a part of the factor "Security management" but have important interdependencies which are explained by the experts. Thus, the security management itself does not have a huge impact on other factors, but they define and implement countermeasures which do have an influence on the MSFs given in the figure. Rectangles within the picture clusters multiple MSFs with the same interdependency to other MSFs. The dotted line within the rectangles indicates, that all MSFs which are left of this line, are not the primary part of the information security department of an organization. They are from other departments like the cooperate-security in the case of "Physical security" and the business continuity in case of "Continuity". However, the collabo-

ration between the departments is very close and the MSFs must certainly be considered in information security as well.

Key security indicators. The term key security indicator is not present in literature but is mentioned by practitioners. Key security indicators are MSFs, which have a direct impact on the security status of the organization. Therefore, the rectangle which includes the MSFs "Physical security", "Vulnerability", "Access control", "Awareness" and "Infrastructure" are key security indicators. Because of the direct connection to the information security concept, these factors are considered as indicators of the actual information security status of an organization. Security management has to implement countermeasures to actively improve these factors. These are the most important factors because of their direct impact.

Security goals. The MSFs "Continuity" and "CIA" are the protection goals of information security. This cluster is considered in the "Risk" MSF by data classification as well as a communication instrument which describes the impact of certain risks to top managers or technical employees. Disasters and continuity thoughts are also considered as risks which are the basis for recovery plans. The security goals are considered as the least important part of the MSF model by experts (Section 4.2.2) because they do not actively improve the security status and just help by prioritizing risks and communicate them to the business management.

Risk. The MSF "Risk" have the most interrelations and is the basic input for "security management". It uses security goals like described before. A prerequisite and a part of risks are key security indicators. They show the current information security status of which weaknesses were deriving. This, in combination with possible threats, the impact on the organization, and the likelihood of occurrence is a risk. Risks are influencing the "Security management" and is a basis to prioritize and define "Countermeasures". The management mostly uses standards and best practices like the ISO/IEC 27000 (ISO/IEC, 2018), NIST SP800-30 (NIST, 2015), NIST SP800-37 (NIST, 2018a) or others to deal with risks and derive countermeasures in a structured way.

Security management. The cluster with "Organizational factors" as well as "Resources" are MSFs which cannot be directly influenced by the experts. They are either given in case of "Organizational factors" or are set by the business management in case of "Resources". They are considered in the "Security management" in conjunction with the "Risk" MSF which are the basis to develop and implement countermeasures which should improve the key security indicators. "Compliance & Policy" are aids which help to enforce countermeasures with employees and are necessary to comply with laws. "Compliance & Policy" is split into external and internal rules which causes the interdependency in both ways to and from the "Security management" MSF. "Security management" define rules and external rules are influencing the "Security management". These rules are considered as the least important by the experts (Section 4.2.2) because they are not actively improving the security situation but are helpful to enforce countermeasures and help to deal with the topic.

6. Discussion and future research

The results of this research propose a comprehensive model of MSFs with their interdependencies for information security decision-makers. The MSFs were supposed based on the literature and are evaluated by experts from practice. These interviews also support interdependencies between the MSFs. The combination of these results in the development of the comprehensive model of MSFs.

Practitioners, as well as the literature, stated the need for a comprehensive view of the information security of organizations. The proposed model does support an abstract and comprehensive view of the complex topic of information security from the management perspective. The different MSFs are not explained in great detail but the interdependencies between them and the overall decision-making process are present in this research. The model gives a basis to decision-makers, which with information security management and help to decide if certain countermeasures are necessary or even useful. It is not just a basis for security managers but also for the business management as well as technical employees. With the help of this model, they are able to understand the difficulties and retrace certain decisions better. A better understanding also leads to better alignment and awareness.

The results are related to several other studies. Past literature does support a great explanation and study of different factors in detail and stated the importance of them. Studies also deal with models of different factors like awareness and their components. This research supports a comprehensive overview of high-level factors (MSFs) and a validation of them as well as a discussion of the relevance of these factors which has been criticized as missing in past articles. The research adds value to the research community by exploring interdependencies between the evaluated MSFs and propose a comprehensive model from the perspective of information security decision-makers. Best practices and standards are very generic and mostly describe processes. But, a complete implementation does not necessarily lead to better security and the standards have been criticized, also by experts in the interview, that they are just frameworks to be compliant. The interdependencies of the comprehensive model in this research help to decide which countermeasures are appropriate and which are not necessary. The standards and best practices give action proposals for improvements of the MSFs and thus complete this research with the next step after the decision was made.

Current standards and best practices, for example, the ISO/IEC 27000-series, the NIST SP800-series or the ISF are important to structure the processes of improving the information security of an organization. These documents either describe processes based on a risk management approach to implement countermeasures or define controls which have to be implemented to comply with the standard. The most experts in the interviews said that they combine two or more of them and uses the concepts they need or are appropriate for them to improve the information security status of the organization. The proposed model in this research contributes to these standards by improving the overall understanding and the interdependencies between the concepts described in the standards. Also, the model is a possibility to report the information security status based on the MSFs. Such a reporting is missing in the current standards and best practices as well as in research articles. The missing reporting standard or suggestions for that is a need which all of the interviewed experts have. Experts also struggle to report the information security decisions and status to the business management in an abstract and understandable way. The current solution of the interviewed experts is that they develop their own reporting standard. These reports do not contain aspects which can be compared with other businesses or even business units. The results of this research support these needs and can be used as a basis for such a reporting standard. Experts also looking for dedicated technical solutions like threat intelligence platforms, security incident management systems and information on indicators of compromise to mention just three. These technologies help to consolidate various information and present them to the management. Each technology is useful for a specific area. This research can help to argue the implementation of specific technologies, to illustrate their role in the overall security context and to identify gaps within the security landscape of an organization in which technologies could help.

The result can also be interpreted from the perspective of the information security status of an organization. From this perspective, the model indicates, that the key security indicators are important to improve the information security status of the organization. This interpretation in mind, small- and medium-sized businesses with fewer resources and not that much competence could implement light-weight countermeasures, which focus on the key security indicators. It could be a quick-win for the decisions in those organizations to focus on the key security indicators. This does not mean, that the standards and best practices or even the other factors of the model should be ignored by small- and medium-sized business. To continuously improve and monitor the information security status in a structured way, the processes and concepts of these standards have to be implemented and used. The proposed model can help these businesses and their management with less expertise in the field of security to understand the interdependencies between relevant concepts, understand which factors are influential and also which factors a manager has to consider by making decisions. Even which factors have to keep in mind to make well-informed decisions.

This study uses a mixed method approach with a literature analysis followed by a semi-structured interview to generate the results. Although a rigorous methodology was used, the study has several limitations. Despite the validation and the discussion with experts, a bias in the interpretation of the texts and the creation of the codes cannot be excluded. Surveyed experts are mainly active in large organizations. Some of them were previously employed in smaller businesses, but the inclusion of opinions from managers of smaller organizations could change the outcomes and importance of individual factors.

The results give many opportunities for future research. The proposed model is based on interdependencies, which are explored by a qualitative study. The interdependencies should be further tested with quantitative approaches to ensure their validity. Certain MSFs were clustered into rectangles. There could be interdependencies between the containing MSFs on deeper levels, which are not be explored in this study. Also, a look deeper within the certain proposed MSFs would be a possibility for future research. Open question from past literature could be solved with a more focused approach based on this results. Leon and Saxena (2010) identified a gap of the security metrics approach, which was not goal-focused in the past and suggested the development of a goal-list which could improve further security metrics development. This comprehensive model and their MSFs could be considered as a list of security goals from the management perspective and thus can be the basis of such research. Also, past metric approaches are mainly based on the individual security processes and thus is not appropriate for cross-organizational comparisons (Bayuk, 2013). A metrics approach based on a comprehensive model could be suitable for this. Also, the interview partner requested a dashboard and reporting standard for key security indicators which is not present in standards, best practices or research articles. To reduce the shortcomings, a future study is possible, which includes small- and medium-sized businesses and integrate them in the proposed model.

Information security managers should consider all the explored MSFs by taking decisions. The countermeasures and processes should not only be adopted because of their appearance in standards and best practices, but they should appropriate in the given situation. A common practice is also the fallback to risk acceptance (Bayuk, 2013) which do not improve the security status at all but is very easy to implement. The results of this study facilitate the understanding of the complex topic of information security and enable more people to make appropriate decisions and take the right actions within their current situation.

7. Conclusion

This research is suggesting a comprehensive model of management success factors (MSFs) for information security decision-makers. Therefore, a literature analysis with an open-axial-selective approach of 136 articles is used to identify factors which have an influence on the information security decisions of managers. A validation of these factors, as well as the check for their relevance, was supported by conducting an interview series of 19 experts from practice. This results in 12 MSFs. To finally develop the comprehensive model, the interviews are the basis to explore interdependencies between the MSFs.

This research suggests that “Physical security”, “Vulnerability”, “Access control”, “Infrastructure” and “Awareness” are key security indicators which have a direct impact on the information security status of an organization. The “Security management” have to consider “Risks”, “Organizational factors” and available “Resources” in order to generate countermeasures, which have an influence on the key security indicators. “Compliance & Policy” is an aid to enforce countermeasures and be compliant with laws. The well discussed MSF “Risk” is considering the security goals “CIA” and “Continuity” and also is using key security indicators to determine a risk level which is used to prioritize countermeasures.

This research offers a high-level view of the complex topic of information security decision-making from the perspective of security management experts. The comprehensive model of MSFs helps them and other employees as well as the business management to better understand the security needs and certain decisions in this context and thus improve their awareness. Future development of goal-oriented metrics and methods to quantify the status of information security as well as methods to aggregate them based on the key security indicators are not just interesting in research but also asked by practitioners.

Declaration of Competing Interests

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.

Appendix A

Table 2
Literature search matrix.

Resource	Hits	Relevant
MIS Quarterly	7	1
European Journal of Information Systems	20	3
Information Systems Journal	27	4
Information Systems Research	22	5
Journal of AIS	11	5
Journal of Information Technology	25	0
Journal of Management Information Systems	1	0
Journal of Strategic Information Systems	14	5
Journal of Management Information Systems	26	2
Decision Sciences	18	2
Information & Management	53	5
Information and Computer Security	99	10
IEEE Trans. on Dependable & Secure Computing	8	1
IEEE Trans. on Information Forensics and Security	7	0
Computers & Security	84	15
Google Scholar	100	11
ScienceDirect	41	6
OpacPlus	110	19
Backward		10
Forward		32
SUM	**673**	**136**

Appendix B

Table 3
Vulnerability.

First-order code	Second-order code	Cluster
technical vulnerabilities (Arora et al., 2010; Boss et al., 2009; Dzazali et al., 2009; Kraemer et al., 2009; NIST, 2008; Premaratne et al., 2008; Sowa and Gabriel, 2009; Straub and Welke, 1998; Sunyaev et al., 2009; Tashi and Ghernaouti-Hélie, 2008; Yeh and Chang, 2007) **vulnerability assessment** (Coronado et al., 2009; Gosavi and Bagade, 2015; Jafari et al., 2010; Siponen and Willison, 2009; Wood, 1987) **network vulnerability** (Gao and Zhong, 2015; Geer et al., 2003; Idika and Bhargava, 2012) **system vulnerability** (Boyer and McQueen, 2007; Dogaheh, 2010; Goldstein et al., 2011; Hayden, 2010; Holm and Afridi, 2015; Jean Camp and Wolfram, 2004; Lee and Larsen, 2009; Norman and Yasin, 2013; Pendleton et al., 2017; Pudar et al., 2009) **vulnerability disclosure** (Ransbotham and Mitra, 2009) **host vulnerability** (Idika and Bhargava, 2012) **security problem** (Straub and Welke, 1998) **vulnerability**(Alavi et al., 2016; Alqahtani, 2015; Ashenden, 2008; Azuwa et al., 2017; Bayuk and Mostashari, 2013; Bayuk, 2013; Ben-Aissa et al., 2012; Crossler and Belanger, 2012; Fenz et al., 2014; 2013; Hajdarevic and Allen, 2013; Hajdarevic et al., 2012; Herzog et al., 2007; Hua and Bapna, 2013; Ifinedo, 2012; Johnson and Goetz, 2007; Leon and Saxena, 2010; Mazur et al., 2015; Mermigas et al., 2013; Muthukrishnan and Palaniappan, 2016; Nazareth and Choi, 2015; Posey et al., 2015; Savola and Heinonen, 2011; Tanna et al., 2005; Vaughn et al., 2003; Verendel, 2009; von Solms and van Niekerk, 2013; Wang et al., 2013; Yeh and Chang, 2007; Young et al., 2016; Zalewski et al., 2014)	technical vulnerabilities	Vulnerability
it security (Björck et al., 2015; Manhart and Thalmann, 2015; Willison and Backhouse, 2006) **technology** (AlHogail, 2015; Ashenden, 2008; Goel and Chengalur-Smith, 2010; Goldstein et al., 2011; Gonzalez and Sawicka, 2002; Hall et al., 2011; Herrera, 2005; Jafari et al., 2010; Katos and Adams, 2005; Kraemer et al., 2009; Leon and Saxena, 2010; Merete Hagen et al., 2008; Nazareth and Choi, 2015; Norman and Yasin, 2013; Trèek, 2003; Yulianto et al., 2016) **technical security** (Azuwa et al., 2017; Coronado et al., 2009; Crossler et al., 2013; Dinev et al., 2009; Fenz et al., 2014; Gao and Zhong, 2015; Gosavi and Bagade, 2015; Hajdarevic et al., 2012; Hedström et al., 2011; Ifinedo, 2012; Manhart and Thalmann, 2015; Montesdioca and Maçada, 2015; Savola, 2007; Savola and Heinonen, 2011; Soomro et al., 2016; Sowa and Gabriel, 2009; Tu and Yuan, 2014; Uffen and Breitner, 2013; Vaughn et al., 2003; Veiga and Eloff, 2007; von Solms and von Solms, 2004; von Solms et al., 1994)	technical security	
application defect (Geer et al., 2003) **application security** (Anderson and Moore, 2006; Bayuk, 2013; Dzazali et al., 2009; Fenz et al., 2014; Goel and Chengalur-Smith, 2010; Hajdarevic and Allen, 2013; Hajdarevic et al., 2012; Joh and Malaiya, 2011; Mazur et al., 2015; Mijnhardt et al., 2016; Muthukrishnan and Palaniappan, 2016; Yeh and Chang, 2007) **feature security** (Ransbotham and Mitra, 2009) **patch coverage** (Arora et al., 2010; Bayuk, 2013; Crossler and Belanger, 2012; Geer et al., 2003; Joh and Malaiya, 2011; Muthukrishnan and Palaniappan, 2016; Pendleton et al., 2017; Ransbotham and Mitra, 2009) **software problem** (Gupta and Hammond, 2005)	application security	

Table 4
Physical security.

First-order code	Second-order code	Cluster
physical security (Collier et al., 2016; Dzazali et al., 2009; Ernest Chang and Ho, 2006; Fenz et al., 2014; Goldstein et al., 2011; Gosavi and Bagade, 2015; Hajdarevic and Allen, 2013; Hajdarevic et al., 2012; Hong et al., 2003; Kankanhalli et al., 2003; Mazur et al., 2015; Mijnhardt et al., 2016; Narain Singh et al., 2014; Norman and Yasin, 2013; Pudar et al., 2009; Sowa and Gabriel, 2009; Trèek, 2003; Tu and Yuan, 2014; von Solms et al., 1994; Wang and Wulf, 1997; Willison and Backhouse, 2006) **physical access** (LeMay et al., 2011; Trèek, 2003) **physical environment** (Jafari et al., 2010; Smith et al., 2010; Veiga and Eloff, 2007; Yeh and Chang, 2007)	physical security	Physical security

Table 5
Compliance & Policy.

First-order code	Second-order code	Cluster
organizational compliance (Jean Camp and Wolfram, 2004) **policy compliance** (Crossler et al., 2013; Hall et al., 2011; Hong et al., 2003; Hu et al., 2012; Ifinedo, 2012; Johnston et al., 2016; Smith et al., 2010; Trèek, 2003) **policy** (Abu-Musa, 2010; Alavi et al., 2016; Ashenden, 2008; Bayuk and Mostashari, 2013; Boss et al., 2009; Cavusoglu et al., 2004; Dzazali et al., 2009; Ernest Chang and Ho, 2006; Goel and Chengalur-Smith, 2010; Hayden, 2010; Hedström et al., 2011; Herath and Rao, 2009; Herrera, 2005; Hong et al., 2003; Horne et al., 2017; Idika and Bhargava, 2012; Jafari et al., 2010; Johnson and Goetz, 2007; Katos and Adams, 2005; Knapp et al., 2009; Kotenko and Bogdanov, 2009; Kotulic and Clark, 2004; Kraemer et al., 2009; Lowry and Moody, 2015a; 2015b; Merete Hagen et al., 2008; Mijnhardt et al., 2016; Mishra and Chasalow, 2011; Montesdioca and Maçada, 2015; Narain Singh et al., 2014; Nazareth and Choi, 2015; Norman and Yasin, 2013; Ransbotham and Mitra, 2009; Sharman et al., 2004; Soomro et al., 2016; Straub and Welke, 1998; Tashi and Ghernaouti-Hélie, 2008; Tsiakis and Stephanides, 2005; Tu and Yuan, 2014; Uffen and Breitner, 2013; Vaughn et al., 2003; Veiga and Eloff, 2007; von Solms and von Solms, 2004; von Solms et al., 1994; Wang et al., 2013; Willison and Backhouse, 2006; Wood, 1987; Yeh and Chang, 2007) **security compliance** (Crossler et al., 2013; Dzazali et al., 2009; Ernest Chang and Ho, 2006; Fenz et al., 2014; 2013; Hayden, 2010; Herath and Rao, 2009; Ifinedo, 2012; Karjalainen and Siponen, 2011; Kraemer et al., 2009; Lowry and Moody, 2015a; Mijnhardt et al., 2016; Narain Singh et al., 2014; Sharman et al., 2004; Soomro et al., 2016; Tu and Yuan, 2014; Willison and Backhouse, 2006; Yulianto et al., 2016)	policy	Compliance & Policy
legal requirements (Alavi et al., 2016; Dzazali et al., 2009; Knapp et al., 2009; Kraemer et al., 2009; Manhart and Thalmann, 2015; Savola and Heinonen, 2011; Sunyaev et al., 2009; Uffen and Breitner, 2013; von Solms and von Solms, 2004) **law compliance** (Hall et al., 2011; Hong et al., 2003; Johnson and Goetz, 2007; Leon and Saxena, 2010; Merete Hagen et al., 2008; Tariq, 2012; Veiga and Eloff, 2007; Yeh and Chang, 2007) **legislation** (Tashi and Ghernaouti-Hélie, 2008; Trèek, 2003) **regulatory requirements** (Abu-Musa, 2010; Atoum et al., 2014; Bayuk and Mostashari, 2013; Fenz et al., 2013; Norman and Yasin, 2013) **regulatory compliance** (Horne et al., 2017; Narain Singh et al., 2014)	compliance	

Table 6
Risk.

First-order code	Second-order code	Cluster
risk management (Ashenden, 2008; Bayuk and Mostashari, 2013; Bayuk, 2013; Beresnevichiene et al., 2010; Collier et al., 2016; Coronado et al., 2009; Ernest Chang and Ho, 2006; Fenz et al., 2014; 2013; Gao and Zhong, 2015; Geer et al., 2003; Hajdarevic and Allen, 2013; Hajdarevic et al., 2012; Hall et al., 2011; Horne et al., 2017; Kotulic and Clark, 2004; Leon and Saxena, 2010; Lowry and Moody, 2015a; Manhart and Thalmann, 2015; Mazur et al., 2015; Merete Hagen et al., 2008; Mijnhardt et al., 2016; Nazareth and Choi, 2015; NIST, 2008; Norman and Yasin, 2013; Ransbotham and Mitra, 2009; Savola, 2007; 2009; Savola and Heinonen, 2011; Sowa and Gabriel, 2009; Straub and Welke, 1998; Tu and Yuan, 2014; von Solms et al., 1994; Wang et al., 2013; Wilkin and Chenhall, 2010; Yaokumah, 2014; Yeh and Chang, 2007) **risk prevention** (Hall et al., 2011; Veiga and Eloff, 2007) **risk tolerance** (Liang and Xue, 2009) **risk exposure** (Mermigas et al., 2013) **risk prediction** (Fenz et al., 2014) **software risk** (Boss et al., 2009; Tanna et al., 2005) **system risk** (Chai et al., 2011; Pendleton et al., 2017; Willison and Backhouse, 2006) **risk perception** (Vance et al., 2014) **risk assessment** (Abu-Musa, 2010; Alavi et al., 2016; Azuwa et al., 2017; Cavusoglu et al., 2004; Chai et al., 2011; Dogaheh, 2010; Fenz et al., 2014; Goldstein et al., 2011; Gonzalez and Sawicka, 2002; Gosavi and Bagade, 2015; Hayden, 2010; Hong et al., 2003; Jean Camp and Wolfram, 2004; Joh and Malaiya, 2011; Johnson and Goetz, 2007; Knapp et al., 2009; Siponen and Willison, 2009; Straub and Welke, 1998; Sunyaev et al., 2009; Tashi and Ghernaouti-Hélie, 2008; Veiga and Eloff, 2007; Verendel, 2009; von Solms et al., 1994) **risk analysis** (Goel and Chengalur-Smith, 2010; Hua and Bapna, 2013; Kumar et al., 2008; Pudar et al., 2009; Sunyaev et al., 2009; Tsiakis and Stephanides, 2005; Young et al., 2016; Zobel and Khansa, 2012)	risk management	Risk
local threats (Willison and Backhouse, 2006) **threat impact** (Alqahtani, 2015; Holm and Afridi, 2015) **available exploits** (Holm and Afridi, 2015; Premaratne et al., 2008) **possible threats** (Abu-Musa, 2010; Alqahtani, 2015; Azuwa et al., 2017; Bayuk and Mostashari, 2013; Bayuk, 2013; Ben-Aissa et al., 2012; Boss et al., 2009; Collier et al., 2016; Coronado et al., 2009; Crossler and Belanger, 2012; Crossler et al., 2013; Dogaheh, 2010; Fenz et al., 2014; 2013; Gao and Zhong, 2015; Gosavi and Bagade, 2015; Gupta and Hammond, 2005; Hajdarevic and Allen, 2013; Hajdarevic et al., 2012; Hall et al., 2011; Herath et al., 2014; Herzog et al., 2007; Hu et al., 2012; Hua and Bapna, 2013; Ifinedo, 2012; Jafari et al., 2010; Johnston et al., 2016; Jones and Horowitz, 2012; Knapp et al., 2009; Lee and Larsen, 2009; Mazur et al., 2015; Muthukrishnan and Palaniappan, 2016; Nazareth and Choi, 2015; Norman and Yasin, 2013; Pendleton et al., 2017; Posey et al., 2015; Purboyo et al., 2011; Sowa and Gabriel, 2009; Sunyaev et al., 2009; Tariq, 2012; Tran et al., 2016; Trèek, 2003; Tsiakis and Stephanides, 2005; Tu and Yuan, 2014; Uffen and Breitner, 2013; Verendel, 2009; von Solms and van Niekerk, 2013; Young et al., 2016; Zobel and Khansa, 2012)	threats	

Table 7
Continuity.

First-order code	Second-order code	Cluster
business continuity (Dzazali et al., 2009; Hong et al., 2003; Horne et al., 2017; Narain Singh et al., 2014; Smith et al., 2010; Sowa and Gabriel, 2009; Tashi and Ghernaouti-Hélie, 2008; Trèek, 2003; Veiga and Eloff, 2007) **business continuity plan** (Ernest Chang and Ho, 2006; Mijnhardt et al., 2016; Tariq, 2012)	business continuity	Continuity
resilience (Björck et al., 2015; Collier et al., 2016; Fenz et al., 2013; Johnson and Goetz, 2007; Tran et al., 2016; Zalewski et al., 2014; Zobel and Khansa, 2012) **survivability** (Katos and Adams, 2005; Vaughn et al., 2003) **contingency plan** (Abu-Musa, 2010; von Solms et al., 1994; Wood, 1987) **power failure** (Gupta and Hammond, 2005) **acts of god** (Björck et al., 2015; Willison and Backhouse, 2006) **natural disaster** (Gupta and Hammond, 2005)	it continuity	
restorability (Bayuk and Mostashari, 2013; Boyer and McQueen, 2007) **disaster recovery** (Crossler and Belanger, 2012; Hall et al., 2011; Kumar et al., 2008; Savola, 2009; Tariq, 2012; von Solms et al., 1994; Wilkin and Chenhall, 2010)	recovery	

Table 8
Infrastructure.

First-order code	Second-order code	Cluster
infrastructure administration (Hua and Bapna, 2013; Savola and Heinonen, 2011; Wood, 1987) **secure environment** (Abu-Musa, 2010; AlHogail, 2015; Ernest Chang and Ho, 2006; Gonzalez and Sawicka, 2002; Herath and Rao, 2009; Herrera, 2005; Liang and Xue, 2009; Mijnhardt et al., 2016; Narain Singh et al., 2014; Norman and Yasin, 2013; Posey et al., 2015; Trèek, 2003; von Solms et al., 1994; Wood, 1987) **infrastructure security** (Crossler and Belanger, 2012; Hong et al., 2003; Katos and Adams, 2005; Trèek, 2003) **ict infrastructure** (Cavusoglu et al., 2004; Fenz et al., 2013; Horne et al., 2017; Soomro et al., 2016) **equipment** (Sharman et al., 2004) **hardware security** (Yeh and Chang, 2007)	infrastructure overview	Infrastructure
network security (Azuwa et al., 2017; Bayuk and Mostashari, 2013; Bayuk, 2013; Gosavi and Bagade, 2015; Kotenko and Bogdanov, 2009; Mazur et al., 2015) **secure network communication** (Azuwa et al., 2017; Fenz et al., 2014; Herzog et al., 2007; Premaratne et al., 2008; Ransbotham and Mitra, 2009; Smith et al., 2010; Yeh and Chang, 2007) **cryptography** (Geer et al., 2003; Herzog et al., 2007; Trèek, 2003; Wang and Wulf, 1997) **encryption** (Chai et al., 2011; Gosavi and Bagade, 2015; Gupta and Hammond, 2005; Ifinedo, 2012) **network hardening** (Idika and Bhargava, 2012) **secure protocol** (Ransbotham and Mitra, 2009)	network security	
asset identification (Bayuk and Mostashari, 2013; Ernest Chang and Ho, 2006; Fenz et al., 2014; Jafari et al., 2010; Merete Hagen et al., 2008; NIST, 2008; Sharman et al., 2004; Trèek, 2003; von Solms and van Niekerk, 2013) **asset assessment** (Boyer and McQueen, 2007; Gao and Zhong, 2015; Hajdarevic et al., 2012; Herzog et al., 2007; Jafari et al., 2010; Kraemer et al., 2009; Montesdioca and Maçada, 2015; Purboyo et al., 2011; Smith et al., 2010) **asset management** (Crossler et al., 2013; Hall et al., 2011; Hong et al., 2003; Horne et al., 2017; Ifinedo, 2012; Mijnhardt et al., 2016; Smith et al., 2010; Soomro et al., 2016; Veiga and Eloff, 2007) **asset classification** (Narain Singh et al., 2014)	asset knowledge	
system configuration (Alavi et al., 2016; Bayuk, 2013; Geer et al., 2003; Hua and Bapna, 2013; Jafari et al., 2010; Jones and Horowitz, 2012; Kotenko and Bogdanov, 2009; Kraemer et al., 2009; Leon and Saxena, 2010; Muthukrishnan and Palaniappan, 2016) **system maintenance** (Alavi et al., 2016; Ernest Chang and Ho, 2006; Hong et al., 2003; Ifinedo, 2012; Narain Singh et al., 2014; Nazareth and Choi, 2015; NIST, 2008; Smith et al., 2010; Sowa and Gabriel, 2009; Trèek, 2003; Veiga and Eloff, 2007; Wood, 1987) **system weakness** (Goldstein et al., 2011; LeMay et al., 2011; Purboyo et al., 2011; Vaughn et al., 2003)	system hardening	
technology architecture (Björck et al., 2015; Cavusoglu et al., 2004; Johnson and Goetz, 2007; Knapp et al., 2009; Mijnhardt et al., 2016) **firewall architecture** (Sharman et al., 2004) **system architecture** (Jones and Horowitz, 2012; Soomro et al., 2016; Yeh and Chang, 2007)	architectural factors	
connections with public network (Johnson and Goetz, 2007; Sharman et al., 2004) **access points** (NIST, 2008) **external system connections** (Pudar et al., 2009; von Solms and van Niekerk, 2013)	external connections	

Table 9
Access control.

First-order code	Second-order code	Cluster
identity (Gosavi and Bagade, 2015; Mijnhardt et al., 2016; Savola and Heinonen, 2011; Wang and Wulf, 1997) **account management** (Anderson and Moore, 2006; Osvaldo De Sordi et al., 2014) **access control** (Abu-Musa, 2010; Azuwa et al., 2017; Bayuk and Mostashari, 2013; Beresnevichiene et al., 2010; Boyer and McQueen, 2007; Chai et al., 2011; Crossler and Belanger, 2012; Dhillon and Torkzadeh, 2006; Dogaheh, 2010; Dzazali et al., 2009; Ernest Chang and Ho, 2006; Geer et al., 2003; Herzog et al., 2007; Holm and Afridi, 2015; Hong et al., 2003; Ifinedo, 2012; Jafari et al., 2010; Mijnhardt et al., 2016; Narain Singh et al., 2014; Ransbotham and Mitra, 2009; Trèek, 2003; Veiga and Eloff, 2007; Willison and Backhouse, 2006) **access rights** (Sharman et al., 2004) **software access control** (LeMay et al., 2011; Smith et al., 2010; Wang and Wulf, 1997)	identity management access control	Access control

Table 10
Awareness.

First-order code	Second-order code	Cluster
personnel security (Ernest Chang and Ho, 2006; Goel and Chengalur-Smith, 2010; Herath and Rao, 2009; Herrera, 2005; Kankanhalli et al., 2003; Narain Singh et al., 2014; Ransbotham and Mitra, 2009; Smith et al., 2010; Sowa and Gabriel, 2009; Trèek, 2003; Uffen and Breitner, 2013; Vaughn et al., 2003; von Solms and von Solms, 2004; von Solms et al., 1994; Yeh and Chang, 2007) **awareness** (Abu-Musa, 2010; Alavi et al., 2016; Alqahtani, 2015; Ashenden, 2008; Atoum et al., 2014; Coronado et al., 2009; Dhillon and Torkzadeh, 2006; Dinev et al., 2009; Dzazali et al., 2009; Gao and Zhong, 2015; Hall et al., 2011; Hong et al., 2003; Jafari et al., 2010; Johnson and Goetz, 2007; Kankanhalli et al., 2003; Karjalainen and Siponen, 2011; Knapp et al., 2009; Kraemer et al., 2009; Manhart and Thalmann, 2015; Merete Hagen et al., 2008; Narain Singh et al., 2014; Norman and Yasin, 2013; Pendleton et al., 2017; Sharman et al., 2004; Soomro et al., 2016; Sowa and Gabriel, 2009; Straub and Welke, 1998; Tran et al., 2016; Tu and Yuan, 2014; Veiga and Eloff, 2007; Velki et al., 2014; von Solms and von Solms, 2004; Wang et al., 2013; Wilkin and Chenhall, 2010; Willison and Backhouse, 2006; Yeh and Chang, 2007; Zobel and Khansa, 2012) **people** (AlHogail, 2015; Gonzalez and Sawicka, 2002; Hall et al., 2011; Horne et al., 2017; Sharman et al., 2004; Yulianto et al., 2016) **technology awareness** (Dinev and Hu, 2007; Herath et al., 2014)	awareness	Awareness
training (AlHogail, 2015; Ashenden, 2008; Dogaheh, 2010; Karjalainen and Siponen, 2011; Lowry and Moody, 2015a; Merete Hagen et al., 2008; NIST, 2008; Posey et al., 2015; Sharman et al., 2004; Tran et al., 2016) **skills** (Alavi et al., 2016) **user knowledge** (Abu-Musa, 2010; Alqahtani, 2015; Fenz et al., 2014; Hajdarevic et al., 2012; Horne et al., 2017; Johnson and Goetz, 2007; Lowry and Moody, 2015b; Manhart and Thalmann, 2015; Nazareth and Choi, 2015; Posey et al., 2015; Veiga and Eloff, 2007; Wood, 1987) **education** (Kraemer et al., 2009; Willison and Backhouse, 2006) **it competence** (Ernest Chang and Ho, 2006; Tu and Yuan, 2014)	user knowledge	
user activities (Björck et al., 2015; Geer et al., 2003; Vance et al., 2014) **human interaction** (Kotenko and Bogdanov, 2009; Trèek, 2003) **human error** (Alavi et al., 2016; Kraemer et al., 2009; Vaughn et al., 2003) **user error** (Gupta and Hammond, 2005) **user/human behavior** (Boss et al., 2009; Crossler et al., 2013; Dinev et al., 2009; Dinev and Hu, 2007; Dogaheh, 2010; Gonzalez and Sawicka, 2002; Hedström et al., 2011; Herath and Rao, 2009; Hua and Bapna, 2013; Ifinedo, 2012; Johnston et al., 2016; Karjalainen and Siponen, 2011; Kraemer et al., 2009; Liang and Xue, 2009; Lowry and Moody, 2015a; Merete Hagen et al., 2008; Montesdioca and Maçada, 2015; Narain Singh et al., 2014; Soomro et al., 2016; Sowa and Gabriel, 2009; Uffen and Breitner, 2013; Vance et al., 2014; Veiga and Eloff, 2007; Velki et al., 2014; von Solms and van Niekerk, 2013) **criminal behavior** (Kankanhalli et al., 2003) **attack behavior** (Gao and Zhong, 2015; Pudar et al., 2009)	behavior	
ethical dimension (von Solms and von Solms, 2004) **work ethic** (Dhillon and Torkzadeh, 2006) **ethical environment** (Dhillon and Torkzadeh, 2006; Veiga and Eloff, 2007) **work situation** (Dhillon and Torkzadeh, 2006)	ethical factors	
security culture (Alavi et al., 2016; AlHogail, 2015; Ashenden, 2008; Boss et al., 2009; Collier et al., 2016; Dinev et al., 2009; Herath and Rao, 2009; Hu et al., 2012; Johnson and Goetz, 2007; Knapp et al., 2009; Kraemer et al., 2009; Merete Hagen et al., 2008; Narain Singh et al., 2014; Norman and Yasin, 2013; Tu and Yuan, 2014; Veiga and Eloff, 2007) **philosophical culture** (Yulianto et al., 2016)	culture	
personal privacy (Ben-Aissa et al., 2012; Boss et al., 2009; Coronado et al., 2009; Dhillon and Torkzadeh, 2006; Dogaheh, 2010; Fenz et al., 2013; Savola, 2009; Tariq, 2012; Wilkin and Chenhall, 2010) **trust** (Boss et al., 2009; Coronado et al., 2009; Dhillon and Torkzadeh, 2006; Dogaheh, 2010; Dzazali et al., 2009; Gao and Zhong, 2015; Horne et al., 2017; Johnston et al., 2016; Lowry and Moody, 2015b; Sowa and Gabriel, 2009; Tariq, 2012; Veiga and Eloff, 2007) **personal needs** (Dhillon and Torkzadeh, 2006) **individual belief** (Hu et al., 2012) **individual impact** (Norman and Yasin, 2013)	personal security	
usefulness / easy to use (Dinev et al., 2009; Dinev and Hu, 2007; Osvaldo De Sordi et al., 2014) **usability** (Bayuk, 2013; Dinev and Hu, 2007; Lee and Larsen, 2009; Verendel, 2009)	usability	

Table 11
CIA.

First-order code	Second-order code	Cluster
reliability (Ben-Aissa et al., 2012; Savola and Heinonen, 2011; Verendel, 2009; Wang and Wulf, 1997; Zalewski et al., 2014) **authenticity** (Azuwa et al., 2017; Ben-Aissa et al., 2012; Gosavi and Bagade, 2015; Holm and Afridi, 2015; Jafari et al., 2010; Katos and Adams, 2005; Savola, 2009; Savola and Heinonen, 2011; Trèek, 2003; Tsiakis and Stephanides, 2005; Wang and Wulf, 1997) **accountability** (Dhillon and Torkzadeh, 2006; Leon and Saxena, 2010; Wood, 1987) **non-repudiation** (Ben-Aissa et al., 2012; Jafari et al., 2010; Purboyo et al., 2011; Savola, 2009; Trèek, 2003; Tsiakis and Stephanides, 2005; Wang and Wulf, 1997)	protection goals	CIA
data integrity (Boyer and McQueen, 2007; Dhillon and Torkzadeh, 2006; Gupta and Hammond, 2005; Tariq, 2012) **transaction integrity** (Gupta and Hammond, 2005) **process/organizational integrity** (Dhillon and Torkzadeh, 2006) **integrity** (Abu-Musa, 2010; Ashenden, 2008; Bayuk and Mostashari, 2013; Ben-Aissa et al., 2012; Beresnevichiene et al., 2010; Cavusoglu et al., 2004; Dzazali et al., 2009; Ernest Chang and Ho, 2006; Goel and Chengalur-Smith, 2010; Goldstein et al., 2011; Hajdarevic and Allen, 2013; Hall et al., 2011; Hedström et al., 2011; Herath et al., 2014; Holm and Afridi, 2015; Hong et al., 2003; Horne et al., 2017; Hu et al., 2012; Hua and Bapna, 2013; Jafari et al., 2010; Joh and Malaiya, 2011; Knapp et al., 2009; Leon and Saxena, 2010; Mijnhardt et al., 2016; Mishra and Chasalow, 2011; Muthukrishnan and Palaniappan, 2016; Nazareth and Choi, 2015; Posey et al., 2015; Pudar et al., 2009; Purboyo et al., 2011; Savola, 2009; Savola and Heinonen, 2011; Sowa and Gabriel, 2009; Tariq, 2012; Tashi and Ghernaouti-Hélie, 2008; Trèek, 2003; Tsiakis and Stephanides, 2005; Tu and Yuan, 2014; Uffen and Breitner, 2013; von Solms and van Niekerk, 2013; Wang and Wulf, 1997; Wilkin and Chenhall, 2010; Yaokumah, 2014; Zalewski et al., 2014)	integrity	
available information (Dhillon and Torkzadeh, 2006) **availability** (Abu-Musa, 2010; Ashenden, 2008; Bayuk and Mostashari, 2013; Ben-Aissa et al., 2012; Beresnevichiene et al., 2010; Cavusoglu et al., 2004; Dogaheh, 2010; Dzazali et al., 2009; Ernest Chang and Ho, 2006; Goel and Chengalur-Smith, 2010; Goldstein et al., 2011; Gupta and Hammond, 2005; Hajdarevic and Allen, 2013; Hall et al., 2011; Hedström et al., 2011; Herath et al., 2014; Holm and Afridi, 2015; Horne et al., 2017; Hu et al., 2012; Jafari et al., 2010; Joh and Malaiya, 2011; Knapp et al., 2009; Kraemer et al., 2009; Leon and Saxena, 2010; Mijnhardt et al., 2016; Mishra and Chasalow, 2011; Muthukrishnan and Palaniappan, 2016; Nazareth and Choi, 2015; Norman and Yasin, 2013; Posey et al., 2015; Pudar et al., 2009; Purboyo et al., 2011; Savola, 2009; Sowa and Gabriel, 2009; Tashi and Ghernaouti-Hélie, 2008; Tu and Yuan, 2014; Uffen and Breitner, 2013; von Solms and van Niekerk, 2013; Wang and Wulf, 1997; Zalewski et al., 2014)	availability	
confidentiality (Abu-Musa, 2010; Ashenden, 2008; Bayuk and Mostashari, 2013; Ben-Aissa et al., 2012; Beresnevichiene et al., 2010; Cavusoglu et al., 2004; Dogaheh, 2010; Dzazali et al., 2009; Ernest Chang and Ho, 2006; Goel and Chengalur-Smith, 2010; Goldstein et al., 2011; Hajdarevic and Allen, 2013; Hall et al., 2011; Hedström et al., 2011; Herath et al., 2014; Holm and Afridi, 2015; Hong et al., 2003; Horne et al., 2017; Hu et al., 2012; Jafari et al., 2010; Joh and Malaiya, 2011; Knapp et al., 2009; Leon and Saxena, 2010; Mijnhardt et al., 2016; Mishra and Chasalow, 2011; Muthukrishnan and Palaniappan, 2016; Nazareth and Choi, 2015; Osvaldo De Sordi et al., 2014; Posey et al., 2015; Pudar et al., 2009; Purboyo et al., 2011; Savola, 2009; Sowa and Gabriel, 2009; Tashi and Ghernaouti-Hélie, 2008; Trèek, 2003; Tsiakis and Stephanides, 2005; Tu and Yuan, 2014; Uffen and Breitner, 2013; von Solms and van Niekerk, 2013; Wang and Wulf, 1997; Yaokumah, 2014; Zalewski et al., 2014)	confidentiality	

Table 12
Organizational factors.

First-order code	Second-order code	Cluster
organization size (Coronado et al., 2009; Ernest Chang and Ho, 2006; Kankanhalli et al., 2003; Kotulic and Clark, 2004; Lee and Larsen, 2009; Lowry and Moody, 2015b; Narain Singh et al., 2014; Norman and Yasin, 2013) **organizational factors** (AlHogail, 2015; Fenz et al., 2014; Herath and Rao, 2009; Hong et al., 2003; Kraemer et al., 2009; Leon and Saxena, 2010; Manhart and Thalmann, 2015; Savola, 2007; Soomro et al., 2016; Sowa and Gabriel, 2009; Sunyaev et al., 2009; Trèek, 2003; Tu and Yuan, 2014; Vaughn et al., 2003; Veiga and Eloff, 2007; von Solms and von Solms, 2004) **organization structure** (Abu-Musa, 2010; Atoum et al., 2014; Kotulic and Clark, 2004; Tu and Yuan, 2014; Yeh and Chang, 2007) **industry type** (Coronado et al., 2009; Dzazali et al., 2009; Ernest Chang and Ho, 2006; Kankanhalli et al., 2003; Narain Singh et al., 2014; Norman and Yasin, 2013; Yeh and Chang, 2007)	organizational factors	Organizational factors
external conditions (Sharman et al., 2004) **reputation** (Gao and Zhong, 2015; Osvaldo De Sordi et al., 2014; Tu and Yuan, 2014)	external factor	

Table 13
Security management.

First-order code	Second-order code	Cluster
countermeasures (measures) (Alavi et al., 2016; Crossler et al., 2013; Fenz et al., 2014; 2013; Herzog et al., 2007; Kotulic and Clark, 2004; Kumar et al., 2008; Leon and Saxena, 2010; Mermigas et al., 2013; Pendleton et al., 2017; Pudar et al., 2009; Ransbotham and Mitra, 2009; Tashi and Ghernaouti-Hélie, 2008) **security control** (Alavi et al., 2016; Ashenden, 2008; Atoum et al., 2014; Azuwa et al., 2017; Bayuk and Mostashari, 2013; Cavusoglu et al., 2004; Collier et al., 2016; Fenz et al., 2013; Goldstein et al., 2011; Hajdarevic and Allen, 2013; Hedström et al., 2011; Hong et al., 2003; Horne et al., 2017; Johnson and Goetz, 2007; Jones and Horowitz, 2012; Knapp et al., 2009; Leon and Saxena, 2010; Lowry and Moody, 2015a; 2015b; Mazur et al., 2015; Narain Singh et al., 2014; Savola, 2007; Savola and Heinonen, 2011; Siponen and Willison, 2009; Sowa and Gabriel, 2009; Sunyaev et al., 2009; Tsiakis and Stephanides, 2005; Young et al., 2016; Zalewski et al., 2014; Zobel and Khansa, 2012) **control recommendation/implementation** (Wood, 1987) **safeguards** (Dzazali et al., 2009; Fenz et al., 2014; Ifinedo, 2012; Liang and Xue, 2009; Tashi and Ghernaouti-Hélie, 2008; Willison and Backhouse, 2006; Yulianto et al., 2016)	control development	Security management
incident response (Abu-Musa, 2010; Alavi et al., 2016; Alqahtani, 2015; Bayuk and Mostashari, 2013; Hajdarevic et al., 2012; Hall et al., 2011; Ifinedo, 2012; Jafari et al., 2010; Jean Camp and Wolfram, 2004; Sowa and Gabriel, 2009; Veiga and Eloff, 2007) **incident handling** (Johnson and Goetz, 2007; Sharman et al., 2004) **compromise detection** (Boyer and McQueen, 2007; Ransbotham and Mitra, 2009; Savola, 2007) **breach investigation** (Wood, 1987) **incident management** (Mijnhardt et al., 2016; Muthukrishnan and Palaniappan, 2016; Narain Singh et al., 2014; Tran et al., 2016) **fraud detection** (Goldstein et al., 2011; Tran et al., 2016)	incident management	
compliance check (Wood, 1987) **evaluation (measurement)** (Azuwa et al., 2017; Gosavi and Bagade, 2015; Pendleton et al., 2017; Savola, 2013; Tu and Yuan, 2014; Wood, 1987; Yaokumah, 2014; Zalewski et al., 2014) **surveillance** (Sharman et al., 2004) **monitoring** (Bayuk and Mostashari, 2013; Mazur et al., 2015; Nazareth and Choi, 2015; Savola, 2013; Sharman et al., 2004) **auditing** (Ashenden, 2008; Atoum et al., 2014; Azuwa et al., 2017; Bayuk and Mostashari, 2013; Jafari et al., 2010; Katos and Adams, 2005; Knapp et al., 2009; Leon and Saxena, 2010; Mishra and Chasalow, 2011; Narain Singh et al., 2014; Ransbotham and Mitra, 2009; Savola, 2009; Sharman et al., 2004; Trèek, 2003; von Solms and von Solms, 2004) **certification** (Savola, 2007; Sowa and Gabriel, 2009; Veiga and Eloff, 2007; von Solms and von Solms, 2004)	monitor and check	
operational processes (Ashenden, 2008; Hayden, 2010; Jafari et al., 2010; Johnson and Goetz, 2007; Sowa and Gabriel, 2009; Trèek, 2003) **administrative security** (Kankanhalli et al., 2003; Yeh and Chang, 2007) **procedures** (Boss et al., 2009; Cavusoglu et al., 2004; Dzazali et al., 2009; Hedström et al., 2011; Herath and Rao, 2009; Hong et al., 2003; Karjalainen and Siponen, 2011; Kotulic and Clark, 2004; Merete Hagen et al., 2008; Montesdioca and Maçada, 2015; Osvaldo De Sordi et al., 2014; Tashi and Ghernaouti-Hélie, 2008; Tsiakis and Stephanides, 2005; Veiga and Eloff, 2007) **processes** (Abu-Musa, 2010; Bayuk and Mostashari, 2013; Goel and Chengalur-Smith, 2010; Goldstein et al., 2011; Hajdarevic et al., 2012; Hall et al., 2011; Horne et al., 2017; Kotulic and Clark, 2004; Mazur et al., 2015; Montesdioca and Maçada, 2015; Norman and Yasin, 2013; Purboyo et al., 2011; Ransbotham and Mitra, 2009; Tsiakis and Stephanides, 2005; Vaughn et al., 2003; Yulianto et al., 2016; Zalewski et al., 2014) **operational readiness**(Vaughn et al., 2003) **process documentation** (Sowa and Gabriel, 2009; Yulianto et al., 2016)	operational rules	
standards (best practices) (Abu-Musa, 2010; Azuwa et al., 2017; Fenz et al., 2013; Goldstein et al., 2011; Hajdarevic and Allen, 2013; Hajdarevic et al., 2012; Knapp et al., 2009; Leon and Saxena, 2010; Mermigas et al., 2013; Mijnhardt et al., 2016; Norman and Yasin, 2013; Smith et al., 2010; Sunyaev et al., 2009; Tu and Yuan, 2014; Uffen and Breitner, 2013; von Solms and von Solms, 2004; Wang et al., 2013; Yulianto et al., 2016) **ISMS** (Azuwa et al., 2017; Hajdarevic and Allen, 2013; Hajdarevic et al., 2012; Herrera, 2005; Mijnhardt et al., 2016; Savola, 2007) **management implementation** (Ernest Chang and Ho, 2006) **management system** (Ashenden, 2008) **governance** (Abu-Musa, 2010; Atoum et al., 2014; Horne et al., 2017; Knapp et al., 2009; Kotulic and Clark, 2004; Norman and Yasin, 2013; von Solms and von Solms, 2004; Yaokumah, 2014)	standards	
communication management (Alavi et al., 2016; AlHogail, 2015; Dhillon and Torkzadeh, 2006; Johnson and Goetz, 2007; Kraemer et al., 2009; Narain Singh et al., 2014; Norman and Yasin, 2013; Smith et al., 2010; Trèek, 2003; Veiga and Eloff, 2007) **security enforcement** (Savola, 2009) **deterrence** (Johnston et al., 2016; Mishra and Chasalow, 2011) **sanctions** (Johnston et al., 2016; Lowry and Moody, 2015b)	communication	
responsibility (Abu-Musa, 2010; Dhillon and Torkzadeh, 2006; Dzazali et al., 2009; Horne et al., 2017; Kraemer et al., 2009; Posey et al., 2015; Sowa and Gabriel, 2009; Wood, 1987) **ownership** (AlHogail, 2015; Dhillon and Torkzadeh, 2006; Sharman et al., 2004)	responsibility	

Table 14
Resources.

First-order code	Second-order code	Cluster
cost (Alavi et al., 2016; Arora et al., 2010; Ben-Aissa et al., 2012; Geer et al., 2003; Hayden, 2010; Ifinedo, 2012; Jafari et al., 2010; Lee and Larsen, 2009; LeMay et al., 2011; Liang and Xue, 2009; Mishra and Chasalow, 2011; Nazareth and Choi, 2015; Tariq, 2012; Tashi and Ghernaouti-Hélie, 2008; Verendel, 2009; Zobel and Khansa, 2012) **cost-benefit/effectiveness** (Cavusoglu et al., 2004; Gonzalez and Sawicka, 2002; Ransbotham and Mitra, 2009; Savola, 2007; Sowa and Gabriel, 2009) **possible cost** (Trèek, 2003) **ROSI** (Alavi et al., 2016; Cavusoglu et al., 2004; Chai et al., 2011; Coronado et al., 2009; Dzazali et al., 2009; Fenz et al., 2013; Gao and Zhong, 2015; Goldstein et al., 2011; Hayden, 2010; Hua and Bapna, 2013; Leon and Saxena, 2010; Lowry and Moody, 2015b; Merete Hagen et al., 2008; Muthukrishnan and Palaniappan, 2016; Nazareth and Choi, 2015; Posey et al., 2015; Pudar et al., 2009; Tashi and Ghernaouti-Hélie, 2008; Tsiakis and Stephanides, 2005; Veiga and Eloff, 2007; Wang et al., 2013; Young et al., 2016)	investment balance	Resources
human resources (Atoum et al., 2014; Dhillon and Torkzadeh, 2006; Kankanhalli et al., 2003; Kraemer et al., 2009; Mijnhardt et al., 2016; Savola, 2007; Soomro et al., 2016; Veiga and Eloff, 2007; Willison and Backhouse, 2006)	human resources	
financial resources (Kankanhalli et al., 2003; Muthukrishnan and Palaniappan, 2016; Sowa and Gabriel, 2009; Tu and Yuan, 2014) **cost control** (Anderson and Moore, 2006) **financial aspect** (Dogaheh, 2010; Ernest Chang and Ho, 2006) **security budget** (Alavi et al., 2016; Beresnevichiene et al., 2010; Horne et al., 2017; Johnson and Goetz, 2007; Kraemer et al., 2009; Lee and Larsen, 2009; Montesdioca and Maçada, 2015; NIST, 2008; Smith et al., 2010; Willison and Backhouse, 2006)	financial resources	
resource support (Abu-Musa, 2010; AlHogail, 2015; Ransbotham and Mitra, 2009; Sowa and Gabriel, 2009; Vaughn et al., 2003; Wilkin and Chenhall, 2010; Zalewski et al., 2014) **economic factors** (Coronado et al., 2009; Fenz et al., 2013; Horne et al., 2017; Hua and Bapna, 2013; Sunyaev et al., 2009; Verendel, 2009) **resource strategy** and value delivery (Yaokumah, 2014)	resource strategy	

References

Abu-Musa, A., 2010. Information security governance in saudi organizations: an empirical study. Inf. Manag. Comput. Secur. 18 (4), 226–276. doi:10.1108/09685221011079180.

AIS Members, 2011. Senior scholars' basket of journals. URL: https://aisnet.org/page/SeniorScholarBasket Last checked: 04.12.2018.

Alavi, R., Islam, S., Mouratidis, H., 2016. An information security risk-driven investment model for analysing human factors. Inf. Comput. Secur. 24 (2), 205–227. doi:10.1108/ICS-01-2016-0006.

AlHogail, A., 2015. Design and validation of information security culture framework. Comput. Human Behav. 49, 567–575. doi:10.1016/j.chb.2015.03.054.

Alqahtani, A., 2015. Towards a framework for the potential cyber-terrorist threat to critical national infrastructure. Inf. Comput. Secur. 23 (5), 532–569. doi:10.1108/ICS-09-2014-0060.

Anderson, R., Moore, T., 2006. The economics of information security. Science (New York, N.Y.) 314, 610–613. doi:10.1126/science.1130992.

Arora, A., Krishnan, R., Telang, R., Yang, Y., 2010. An empirical analysis of software vendors' patch release behavior: impact of vulnerability disclosure. Inf. Syst. Res. 21 (1), 115–132. doi:10.1287/isre.1080.0226.

Ashenden, D., 2008. Information security management: a human challenge? Inf. Secur. Tech. Rep. 13 (4), 195–201. doi:10.1016/j.istr.2008.10.006.

Atoum, I., Otoom, A., Abu Ali, A., 2014. A holistic cyber security implementation framework. Inf. Manag. Comput. Secur. 22 (3), 251–264. doi:10.1108/IMCS-02-2013-0014.

Azuwa, M.P., Sahib, S., Shamsuddin, S., 2017. Technical security metrics model in compliance with iso/iec 27001 standard. Int. J. Cyber-Secur. Digital Forens. (IJCSDF) 1 (4), 280–288.

Bayuk, J., Mostashari, A., 2013. Measuring systems security. Syst. Eng. 16 (1), 1–14. doi:10.1002/sys.21211.

Bayuk, J.L., 2013. Security as a theoretical attribute construct. Comput. Secur. 37, 155–175. doi:10.1016/j.cose.2013.03.006.

Ben-Aissa, A., Abercrombie, R.K., Sheldon, F.T., Mili, A., 2012. Defining and computing a value based cyber-security measure. Inf. Syst. e-Business Manag. 10 (4), 433–453. doi:10.1007/s10257-011-0177-1.

Beresnevichiene, Y., Pym, D., Shiu, S., 2010. Decision support for systems security investment. In: 2010 IEEE/IFIP Network Operations and Management Symposium workshops, pp. 118–125. doi:10.1109/NOMSW.2010.5486590.

Bernard, T. S., Cowley, S., 2017. Equifax breach caused by lone employee's error, former c.e.o. says. URL: https://www.nytimes.com/2017/10/03/business/equifax-congress-data-breach:html, Last checked: 01.12.2018.

Björck, F., Henkel, M., Stirna, J., Zdravkovic, J., 2015. Cyber resilience – fundamentals for a definition. In: Rocha, A., Correia, A.M., Costanzo, S., Reis, L.P. (Eds.), New Contributions in Information Systems and Technologies. In: Advances in Intelligent Systems and Computing, 353. Springer International Publishing, Cham, pp. 311–316. doi:10.1007/978-3-319-16486-1_31.

Boehm, J., Merrath, P., Poppensieker, T., Riemenschnitter, R., Stähle, T., 2017. Cyber risk measurement and the holistic cybersecurity approach. URL: https://www.mckinsey.com/business-functions/risk/our-insights/cyber-risk-measurement-and-the-holistic-cybersecurity-approach Last checked: 03.12.2018.

Bogner, A., Littig, B., Menz, W., 2014. Interviews mit Experten: Eine praxisorientierte Einführung. Qualitative Sozialforschung. Springer Fachmedien Wiesbaden.

Bortz, J., Döring, N., 1995. Forschungsmethoden und Evaluation. Springer-Lehrbuch, Springer Berlin Heidelberg.

Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A., Boss, R.W., 2009. If someone is watching, i'll do what i'm asked: Mandatoriness, control, and information security. Eur. J. Inf. Syst. 18 (2), 151–164. doi:10.1057/ejis.2009.8.

Boyer, W., McQueen, M., 2007. Ideal based cyber security technical metrics for control systems. In: Critical information infrastructures security, pp. 246–260. doi:10.1007/978-3-540-89173-421.

Cavusoglu, H., Mishra, B., Raghunathan, S., 2004. A model for evaluating it security investments. Commun. ACM 47 (7), 87–92. doi:10.1145/1005817.1005828.

Chai, S., Kim, M., Rao, H.R., 2011. Firms' information security investment decisions: Stock market evidence of investors' behavior. Decis. Support Syst. 50 (4), 651–661. doi:10.1016/j.dss.2010.08.017.

Cisco Systems Inc., 2018. Cisco 2018: annual cybersecurity report. Technical Report. Cisco Systems Inc.

Collier, Z.A., Panwar, M., Ganin, A.A., Kott, A., Linkov, I., 2016. Security metrics in industrial control systems. In: Colbert, E.J.M., Kott, A. (Eds.), Cyber-Security of SCADA and Other Industrial Control Systems. In: Advances in Information Security. Springer, Switzerland, pp. 167–185. doi:10.1007/978-3-319-32125-7_9.

Corbin, J., Strauss, A., 1990. Grounded theory research: procedures, canons and evaluative criteria. Zeitschrift für Soziologie 19 (6), 418–427 doi:10.1515/zfsoz-1990-0602.

Coronado, A.S., Mahmood, M.A., Pahnila, S., Luciano, E.M., 2009. Measuring effectiveness of information systems security: an empirical research. In: 15th Americas Conference on Information Systems, pp. 282–290.

Crossler, R., Belanger, F., 2012. The quest for complete security protection: an empirical analysis of an individual's 360 degree protection from file and data loss. In: 18th Americas Conference on Information Systems, pp. 1–6.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R., 2013. Future directions for behavioral information security research. Comput. Secur. 32, 90–101. doi:10.1016/j.cose.2012.09.010.

DeLone, W.H., McLean, E.R., 1992. Information systems success: the quest for the dependent variable. Inf. Syst. Res. 3 (1), 60–95. doi:10.1287/isre.3.1.60.

Dhillon, G., Torkzadeh, G., 2006. Value-focused assessment of information system security in organizations. Inf. Syst. J. 16 (3), 293–314. doi:10.1111/j.1365-2575.2006.00219.x.

Diesch, R., Pfaff, M., Krcmar, H., 2018. Prerequisite to measure information security: a state of the art literature review. In: 4th International Conference on

Information Systems Security and Privacy (ICISSP), pp. 207–215. doi:10.5220/0006545602070215.
Dinev, T., Goo, J., Hu, Q., Nam, K., 2009. User behaviour towards protective information technologies: the role of national cultural differences. Inf. Syst. J. 19 (4), 391–412. doi:10.1111/j.1365-2575.2007.00289.x.
Dinev, T., Hu, Q., 2007. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. J. Assoc. Inf. Syst. 8 (7), 386–408.
Dogaheh, M.A., 2010. Introducing a framework for security measurements. In: IEEE International Conference on Information Theory and Information Security, pp. 638–641. doi:10.1109/ICITIS.2010.5689505.
Dzazali, S., Sulaiman, A., Zolait, A.H., 2009. Information security landscape and maturity level: case study of malaysian public service (mps) organizations. Gov. Inf. Q. 26 (4), 584–593. doi:10.1016/j.giq.2009.04.004.
Ernest Chang, S., Ho, C.B., 2006. Organizational factors to the effectiveness of implementing information security management. Indus. Manag. Data Syst. 106 (3), 345–361. doi:10.1108/02635570610653498.
Fenz, S., Heurix, J., Neubauer, T., Pechstein, F., 2014. Current challenges in information security risk management. Inf. Manag. Comput. Secur. 22 (5), 410–430. doi:10.1108/IMCS-07-2013-0053.
Fenz, S., Neubauer, T., Accorsi, R., Koslowski, T., 2013. Forisk: formalizing information security risk and compliance management. In: 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop, pp. 1–4. doi:10.1109/DSNW.2013.6615533.
Gao, X., Zhong, W., 2015. Information security investment for competitive firms with hacker behavior and security requirements. Annal. Oper. Res. 235 (1), 277–300. doi:10.1007/s10479-015-1925-2.
Geer, D., Hoo, K.S., Jaquith, A., 2003. Information security: why the future belongs to the quants. IEEE Secur. Privacy Mag. 1 (4), 24–32. doi:10.1109/MSECP.2003.1219053.
Glaser, B.G., Strauss, A.L., 1967. The discovery of grounded theory: strategies for qualitative research. AldineTransaction, New Brunswick.
Goel, S., Chengalur-Smith, I.N., 2010. Metrics for characterizing the form of security policies. J. Strategic Inf. Syst. 19 (4), 281–295. doi:10.1016/j.jsis.2010.10.002.
Goldstein, J., Chernobai, A., Benaroch, M., 2011. An event study analysis of the economic impact of it operational risk and its subcategories. J. Assoc. Inf. Syst. 11 (9), 606–631.
Gonzalez, J.J., 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, pp. 1871–1877.
Gosavi, H.R., Bagade, A.M., 2015. A review on zero day attack safety using different scenarios. Eur. J. Adv. Eng. Technol. 2 (1), 30–34.
Gupta, A., Hammond, R., 2005. Information systems security issues and decisions for small businesses. Inf. Manag. Comput. Secur. 13 (4), 297–310. doi:10.1108/09685220510614425.
Hajdarevic, K., Allen, P., 2013. A new method for the identification of proactive information security management system metrics. In: 36th International Convention on Information & Communication Technology, Electronics & Microelectronics, pp. 1121–1126.
Hajdarevic, K., Pattinson, C., Kozaric, K., Hadzic, A., 2012. Information security measurement infrastructure for kpi visualization. In: Proceedings of the 35th International Convention MIPRO, pp. 1543–1548.
Hall, J.H., Sarkani, S., Mazzuchi, T.A., 2011. Impacts of organizational capabilities in information security. Inf. Manag. Comput. Secur. 19 (3), 155–176. doi:10.1108/09685221111153546.
Hayden, L., 2010. IT security metrics: a practical framework for measuring security & protecting data. McGraw Hill, New York.
Hedström, K., Kolkowska, E., Karlsson, F., Allen, J.P., 2011. Value conflicts for information security management. J. Strateg. Inf. Syst. 20 (4), 373–384. doi:10.1016/j.jsis.2011.06.001.
Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., Rao, H.R., 2014. Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. Inf. Syst. J. 24 (1), 61–84. doi:10.1111/j.1365-2575.2012.00420.x.
Herath, T., Rao, H.R., 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. Inf. Syst. 18 (2), 106–125. doi:10.1057/ejis.2009.6.
Herrera, S., 2005. Information security management metrics development. In: 39th Annual 2005 International Carnahan Conference on Security Technology, pp. 51–56. doi:10.1109/CCST.2005.1594818.
Herzog, A., Shahmehri, N., Duma, C., 2007. An ontology of information security. Int. J. Inf. Secur. Privacy 1 (4), 1–23. doi:10.4018/jisp.2007100101.
Holm, H., Afridi, K.K., 2015. An expert-based investigation of the common vulnerability scoring system. Comput. Secur. 53, 18–30. doi:10.1016/j.cose.2015.04.012.
Höne, K., Eloff, J., 2002. Information security policy — what do international information security standards say? Comput. Secur. 21 (5), 402–409. doi:10.1016/S0167-4048(02)00504-7.
Hong, K.-S., Chi, Y.-P., Chao, L.R., Tang, J.-H., 2003. An integrated system theory of information security management. Inf. Manag. Comput. Secur. 11 (5), 243–248. doi:10.1108/09685220310500153.
Horne, C.A., Maynard, S.B., Ahmad, A., 2017. Information security strategy in organisations: review, discussion and future research. Aust. J. Inf. Syst. 21. doi:10.3127/ajis.v21i0.1427.
Hu, Q., Dinev, T., Hart, P., Cooke, D., 2012. Managing employee compliance with information security policies: the critical role of top management and organizational culture. Decis. Sci. 43 (4), 615–660. doi:10.1111/j.1540-5915.2012.00361.x.
Hua, J., Bapna, S., 2013. The economic impact of cyber terrorism. J. Strateg. Inf. Syst. 22 (2), 175–186. doi:10.1016/j.jsis.2012.10.004.
Idika, N., Bhargava, B., 2012. Extending attack graph-based security metrics and aggregating their application. IEEE Trans. Depend. Secure Comput. 9 (1), 75–85. doi:10.1109/TDSC.2010.61.
Ifinedo, P., 2012. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput. Secur. 31 (1), 83–95. doi:10.1016/j.cose.2011.10.007.
ISACA, 2012. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. ISACA.
ISF, 2018. Standard of good practice for information security. Technical Report. Information Security Forum Limited. (ISF).
ISO/IEC, 2018. ISO/IEC 27000:2018(E): Information technology - Security techniques - Information security management systems - Overview and vocabulary. Standard. ISO/IEC, Switzerland.
Jafari, S., Mtenzi, F., Fitzpatrick, R., O'Shea, B., 2010. Security metrics for e-healthcare information systems: a domain specific metrics approach. Int. J. Digital Soc. (IJDS) 1 (4), 238–245.
Jean Camp, L., Wolfram, C., 2004. Pricing security: vulnerabilities as externalities. Econ. Inf. Secur. 12, 17–34. doi:10.1007/1-4020-8090-5_2.
Joh, H., Malaiya, Y.K., 2011. Defining and assessing quantitative security risk measures using vulnerability lifecycle and cvss metrics. In: The 2011 International Conference on Security and Management, pp. 10–16.
Johnson, M.E., Goetz, E., 2007. Embedding information security into the organization. IEEE Secur. Privacy Mag. 5 (3), 16–24. doi:10.1109/MSP.2007.59.
Johnston, A.C., Warkentin, M., McBride, M., Carter, L., 2016. Dispositional and situational factors: influences on information security policy violations. Eur. J. Inf. Syst. 25 (3), 231–251. doi:10.1057/ejis.2015.15.
Jones, R.A., Horowitz, B., 2012. A system-aware cyber security architecture. Syst. Eng. 15 (2), 225–240. doi:10.1002/sys.21206.
Kankanhalli, A., Teo, H.-H., Tan, B.C., Wei, K.-K., 2003. An integrative study of information systems security effectiveness. Int. J. Inf. Manag. 23 (2), 139–154. doi:10.1016/S0268-4012(02)00105-6.
Karjalainen, M., Siponen, M., 2011. Toward a new meta-theory for designing information systems (is) security training approaches. J. Assoc. Inf. Syst. 12 (8), 518–555.
Katos, V., Adams, C., 2005. Modelling corporate wireless security and privacy. J. Strateg. Inf. Syst. 14 (3), 307–321. doi:10.1016/j.jsis.2005.07.006.
Knapp, K., Marshall, T., Rainer, R.K., Morrow, D., 2006. The top information security issues facing organizations: what can government do to help? Inf. Syst. Secur. 15 (4), 51–58. doi:10.1201/1086.1065898X/46353.15.4.20060901/95124.6.
Knapp, K.J., Franklin Morris, R., Marshall, T.E., Byrd, T.A., 2009. Information security policy: an organizational-level process model. Comput. Secur. 28 (7), 493–508. doi:10.1016/j.cose.2009.07.001.
Kotenko, I., Bogdanov, V., 2009. Proactive monitoring of security policy accomplishment in computer networks. In: Proceedings of the 5th IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems, Technology and Applications, pp. 364–369. doi:10.1109/IDAACS.2009.5342961.
Kotulic, A.G., Clark, J.G., 2004. Why there aren't more information security research studies. Inf. Manag. 41 (5), 597–607. doi:10.1016/j.im.2003.08.001.
Kraemer, S., Carayon, P., Clem, J., 2009. Human and organizational factors in computer and information security: pathways to vulnerabilities. Comput. Secur. 28 (7), 509–520. doi:10.1016/j.cose.2009.04.006.
Kumar, R.L., Park, S., Subramaniam, C., 2008. Understanding the value of countermeasure portfolios in information systems security. J. Manag. Inf. Syst. 25 (2), 241–280. doi:10.2753/MIS0742-1222250210.
Lee, C.H., Geng, X., Raghunathan, S., 2016. Mandatory standards and organizational information security. Inf. Syst. Res. 27 (1), 70–86. doi:10.1287/isre.2015.0607.
Lee, Y., Larsen, K.R., 2009. Threat or coping appraisal: determinants of smb executives' decision to adopt anti-malware software. Eur. J. Inf. Syst. 18 (2), 177–187. doi:10.1057/ejis.2009.11.
LeMay, E., Ford, M.D., Keefe, K., Sanders, W.H., Muehrcke, C., 2011. Model-based security metrics using adversary view security evaluation (advise). In: Eighth International Conference on Quantitative Evaluation of SysTems, pp. 191–200. doi:10.1109/QEST.2011.34.
Leon, P.G., Saxena, A., 2010. An approach to quantitatively measure information security. In: 3rd India Software Engineering Conference.
Liang, H., Xue, Y., 2009. Avoidance of information technology threats: a theoretical perspective. MIS Q. 33 (1), 71–90.
Lowry, P.B., Moody, G.D., 2015. Proposing the control-reactance compliance model (crcm) to explain opposing motivations to comply with organisational information security policies. Inf. Syst. J. 25 (5), 433–463. doi:10.1111/isj.12043.
Lowry, P.B., Moody, G.D., 2015. Proposing the control-reactance compliance model (crcm) to explain opposing motivations to comply with organisational information security policies. Inf. Syst. J. 25 (5), 433–463. doi:10.1111/isj.12043.
Manhart, M., Thalmann, S., 2015. Protecting organizational knowledge: a structured literature review. J. Know. Manag. 19 (2), 190–211. doi:10.1108/JKM-05-2014-0198.
May, T.A., 1997. The death of roi: re–thinking it value measurement. Inf. Manag. Comput. Secur. 5 (3), 90–92. doi:10.1108/09685229710175756.
Mayring, P., 2015. Qualitative Inhaltsanalyse: Grundlagen und Techniken. Beltz Pädagogik. Beltz.
Mazur, K., Ksiezopolski, B., Kotulski, Z., 2015. The robust measurement method for security metrics generation. Comput. J. 58 (10), 2280–2296. doi:10.1093/comjnl/bxu100.

Merete Hagen, J., Albrechtsen, E., Hovden, J., 2008. Implementation and effectiveness of organizational information security measures. Inf. Manag. Comput. Secur. 16 (4), 377–397. doi:10.1108/09685220810908796.

Mermigas, D., Patsakis, C., Pirounias, S., 2013. Quantification of information systems security with stochastic calculus. In: Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop, pp. 1–9. doi:10.1145/2459976.2460030.

Mijnhardt, F., Baars, T., Spruit, M., 2016. Organizational characteristics influencing sme information security maturity. J. Comput. Inf. Syst. 56 (2), 106–115. doi:10.1080/08874417.2016.1117369.

Mishra, S., Chasalow, L., 2011. Information security effectiveness: a research framework. Iss. Inf. Syst. 7 (1), 246–255.

Montesdioca, G.P.Z., Maçada, A.C.G., 2015. Measuring user satisfaction with information security practices. Comput. Secur. 48, 267–280. doi:10.1016/j.cose.2014.10.015.

Muthukrishnan, S.M., Palaniappan, S., 2016. Security metrics maturity model for operational security. In: IEEE Symposium on Computer Applications and Industrial Electronics, pp. 101–106. doi:10.1109/ISCAIE.2016.7575045.

Narain Singh, A., Gupta, M.P., Ojha, A., 2014. Identifying factors of "organizational information security management". J. Enterp. Inf. Manag. 27 (5), 644–667. doi:10.1108/JEIM-07-2013-0052.

Nazareth, D.L., Choi, J., 2015. A system dynamics model for information security management. Inf. Manag. 52 (1), 123–134. doi:10.1016/j.im.2014.10.009.

NIST, 2008. NIST SP 800-55r1: performance measurement guide for information security. Technical Report. National Institute of Standards and Technology.

NIST, 2013. NISTIR 7298r2: glossary of key information security terms. Technical Report. National Institute of Standards and Technology.

NIST, 2015. NIST SP 800-30r1: risk management guide for information technology systems. Technical Report. National Institute of Standards and Technology.

NIST, 2018. NIST SP 800-37r2: risk management framework for information systems and organizations. Technical Report. National Institute of Standards and Technology.

NIST, 2018b. Nist special publication 800-series general information. URL: https://www.nist.gov/itl/nist-special-publication-800-series-general-information Last checked: 07.05.2019.

Norman, A.A., Yasin, N.M., 2013. Information systems security management (issm) success factor: retrospection from the scholars. African J. Bus. Manag. 7 (27), 2646–2656. doi:10.5897/AJBM11.2479.

Osvaldo De Sordi, J., Meireles, M., Carvalho de Azevedo, M., 2014. Information selection by managers: priorities and values attributed to the dimensions of information. Online Inf. Rev. 38 (5), 661–679. doi:10.1108/OIR-01-2014-0006.

Pendleton, M., Garcia-Lebron, R., Cho, J.-H., Xu, S., 2017. A survey on systems security metrics. ACM Comput. Surv. 49 (4), 1–35. doi:10.1145/3005714.

Ponemon Institute LLC, 2018. 2018 cost of a data breach study: global overview. Technical Report. Ponemon Institute LLC.

Posey, C., Roberts, T.L., Lowry, P.B., 2015. The impact of organizational commitment on insiders' motivation to protect organizational information assets. J. Manag. Inf. Syst. 32 (4), 179–214. doi:10.1080/07421222.2015.1138374.

Premaratne, U., Samarabandu, J., Sidhu, T., Beresh, B., Tan, J.-C., 2008. Application of security metrics in auditing computer network security: acase study. In: 4th International Conference on Information and Automation for Sustainability, pp. 200–205. doi:10.1109/ICIAFS.2008.4783996.

Pudar, S., Manimaran, G., Liu, C.-C., 2009. Penet: a practical method and tool for integrated modeling of security attacks and countermeasures. Comput. Secur. 28 (8), 754–771. doi:10.1016/j.cose.2009.05.007.

Purboyo, T.W., Rahardjo, B., Kuspriyanto, 2011. Security metrics: a brief survey. In: 2011 2nd International Conference on Instrumentation, Communications, Information Technology and Biomedical Engineering, pp. 79–82. doi:10.1109/ICICI-BME.2011.6108598.

Ransbotham, S., Mitra, S., 2009. Choice and chance: a conceptual model of paths to information security compromise. Inf. Syst. Res. 20 (1), 121–139. doi:10.1287/isre.1080.0174.

Savola, R., 2007. Towards a security metrics taxonomy for the information and communication technology industry. In: International Conference on Software Engineering Advances (ICSEA), p. 60. doi:10.1109/ICSEA.2007.79.

Savola, R.M., 2009. A security metrics taxonomization model for software-intensive systems. J. Inf. Process. Syst. 5 (4), 197–206. doi:10.3745/JIPS.2009.5.4.197.

Savola, R.M., 2013. Quality of security metrics and measurements. Comput. Secur. 37, 78–90. doi:10.1016/j.cose.2013.05.002.

Savola, R.M., Heinonen, P., 2011. A visualization and modeling tool for security metrics and measurements management. In: 2011 Information Security for South Africa, pp. 1–8. doi:10.1109/ISSA.2011.6027518.

Sharman, R., Rao, R., Upadhyaya, S., 2004. Metrics for information security: a literature review. In: 10th Americas Conference on Information Systems, pp. 1437–1440.

Silic, M., Back, A., 2014. Information security: critical review and future directions for research. Inf. Manag. Comput. Secur. 22 (3), 279–308. doi:10.1108/IMCS-05-2013-0041.

Siponen, M., Willison, R., 2009. Information security management standards: problems and solutions. Inf. Manag. 46 (5), 267–270. doi:10.1016/j.im.2008.12.007.

SJR, 2018. Sjr: Scientific journal rankings. URL: https://www.scimagojr.com/journalrank.php Last checked: 04.12.2018.

Smith, S., Winchester, D., Bunker, D., Jaimeson, R., 2010. Circuits of power: a study of mandated compliance to an information systems security de jure standard in a government organization. MIS Q. 34 (3), 463–486.

Soomro, Z.A., Shah, M.H., Ahmed, J., 2016. Information security management needs more holistic approach: a literature review. Int. J. Inf. Manag. 36 (2), 215–225. doi:10.1016/j.ijinfomgt.2015.11.009.

Sowa, S., 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. IEEE, pp. 750–755. doi:10.1109/ARES.2009.26.

Straub, D.W., Welke, R.J., 1998. Coping with systems risk: security planning models for management decision making. MIS Q. 22 (4), 441. doi:10.2307/249551.

Sunyaev, A., Tremmel, F., Mauro, C., LeimeisterJ. M. & Krcmar, H., 2009. A re-classification of is security analysis approaches. In: 15th Americas Conference on Information Systems, pp. 1–10.

Tanna, G.B., Gupta, M., Rao, H.R., Upadhyaya, S., 2005. Information assurance metric development framework for electronic bill presentment and payment systems using transaction and workflow analysis. Decis. Support Syst. 41 (1), 242–261. doi:10.1016/j.dss.2004.06.013.

Tariq, M.I., 2012. Towards information security metrics framework for cloud computing. Int. J. Cloud Comput. Serv. Sci. (IJ-CLOSER) 1 (4). doi:10.11591/closer.v1i4.1442.

Tashi, I., Ghernaouti-Hélie, S., 2008. Efficient security measurements and metrics for risk assessment. In: The Third International Conference on Internet Monitoring and Protection, pp. 131–138. doi:10.1109/ICIMP.2008.34.

Thycopic Software Ltd., 2017. The 2017 state of cybersecurity metrics annual report. Technical Report. Thycopic Software Ltd.

Tran, H., Campos-Nanez, E., Fomin, P., Wasek, J., 2016. Cyber resilience recovery model to combat zero-day malware attacks. Comput. Secur. 61, 19–31. doi:10.1016/j.cose.2016.05.001.

Trèek, D., 2003. An integral framework for information systems security management. Comput. Secur. 22 (4), 337–360. doi:10.1016/S0167-4048(03)00413-9.

Tsiakis, T., Stephanides, G., 2005. The economic approach of information security. Comput. Secur. 24 (2), 105–108. doi:10.1016/j.cose.2005.02.001.

Tu, C.Z., Yuan, Y., Archer, N., Connelly, C.E., 2018. Strategic value alignment for information security management: a critical success factor analysis. Inf. Comput. Secur. 26 (2), 150–170. doi:10.1108/ICS-06-2017-0042.

Tu, Z., Yuan, Y., 2014. Critical success factors analysis on effective information security management: a literature review. In: 20th Americas Conference on Information Systems, pp. 1874–1886.

Uffen, J., Breitner, M.H., 2013. Management of technical security measures: an empirical examination of personality traits and behavioral intentions. In: 46th Hawaii International Conference on System Sciences, pp. 4551–4560. doi:10.1109/HICSS.2013.388.

Vance, A., Eargle, D., Anderson, B.B., Kirwan, C.B., 2014. Using measures of risk perception to predict information security behavior: insights from electroencephalography (eeg). J. Assoc. Inf. Syst. 15, 679–722.

Vaughn, R.B., Henning, R., 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 doi:10.1109/HICSS.2003.1174904.

Veiga, A.D., Eloff, J.H.P., 2007. An information security governance framework. Inf. Syst. Manag. 24 (4), 361–372. doi:10.1080/10580530701586136.

Velki, T., Solic, K., 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), pp. 1417–1421. doi:10.1109/MIPRO.2014.6859789.

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, pp. 37–50. doi:10.1145/1719030.1719036.

von Solms, B., von Solms, R., 2004. The 10 deadly sins of information security management. Comput. Secur. 23 (5), 371–376. doi:10.1016/j.cose.2004.05.002.

von Solms, R., van der Haar, H., von Solms, S.H., Caelli, W.J., 1994. A framework for information security evaluation. Inf. Manag. 26 (3), 143–153. doi:10.1016/0378-7206(94)90038-8.

von Solms, R., van Niekerk, J., 2013. From information security to cyber security. Comput. Secur. 38, 97–102. doi:10.1016/j.cose.2013.04.004.

Wang, C., Wulf, W.A., 1997. Towards a framework for security measurement. In: 20th National Information Systems Security Conference, pp. 522–533.

Wang, T., Kannan, K.N., Ulmer, J.R., 2013. The association between the disclosure and the realization of information security risk factors. Inf. Syst. Res. 24 (2), 201–218. doi:10.1287/isre.1120.0437.

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

Wilkin, C.L., Chenhall, R.H., 2010. A review of it governance: a taxonomy to inform accounting information systems. J. Inf. Syst. 24 (2), 107–146. doi:10.2308/jis.2010.24.2.107.

Willison, R., Backhouse, J., 2006. Opportunities for computer crime: considering systems risk from a criminological perspective. Eur. J. Inf. Syst. 15 (4), 403–414. doi:10.1057/palgrave.ejis.3000592.

Wolfswinkel, J.F., Furtmueller, E., Wilderom, C.P.M., 2013. Using grounded theory as a method for rigorously reviewing literature. Eur. J. Inf. Syst. 22 (1), 45–55. doi:10.1057/ejis.2011.51.

Wood, C.C., 1987. Information systems security: management success factors. Comput. Secur. 6 (4), 314–320. doi:10.1016/0167-4048(87)90066-6.

Yaokumah, W., 2014. Information security governance implementation within ghanaian industry sectors. Inf. Manag. Comput. Secur. 22 (3), 235–250. doi:10.1108/IMCS-06-2013-0044.

Yeh, Q.-J., Chang, A.J.-T., 2007. Threats and countermeasures for information system security: a cross-industry study. Inf. Manag. 44 (5), 480–491. doi:10.1016/j.im.2007.05.003.

Young, D., Lopez, J., Rice, M., Ramsey, B., McTasney, R., 2016. A framework for incorporating insurance in critical infrastructure cyber risk strategies. Int. J. Crit. Infrastruct. Protect. 14, 43–57. doi:10.1016/j.ijcip.2016.04.001.

Yulianto, S., Lim, C., Soewito, B., 2016. Information security maturity model: a best practice driven approach to pci dss compliance. In: 2016 IEEE Region 10 Symposium, pp. 65–70. doi:10.1109/TENCONSpring.2016.7519379.

Zalewski, J., Drager, S., McKeever, W., Kornecki, A.J., 2014. Measuring security: a challenge for the generation. In: 2014 Federated Conference on Computer Science and Information Systems, pp. 131–140. doi:10.15439/2014F490.

Zobel, C.W., Khansa, L., 2012. Quantifying cyberinfrastructure resilience against multi-event attacks. Decis. Sci. 43 (4), 687–710. doi:10.1111/j.1540-5915.2012.00364.x.

Rainer Diesch received the degree of M.Sc. from the Ludwig-Maximilians-University of Munich, 2016. At present, he is a member of a research team at the fortiss GmbH, an affiliated institute of the Technical University of Munich. Rainer Diesch is currently doing his Ph.D. in Business Informatics at the Technical University of Munich on the Cair of Information Systems. His research interest includes information security management, security measurement and information management.

Matthias Pfaff received his PhD degree (Dr. rer nat.) in 2018 from the Technical University of Munich in the topic of semantic data integration. He previously studied computer science at the Goethe University Frankfurt (degree Dipl.-Inf). Since 2011 he is working at fortiss, he heads the competence field æbusiness model & service engineeringg (BM&SE) and is responsible for the fortiss Application Center for AI. His research interests include semantic technologies for data integration and ontologies especially for business applications.

Helmut Krcmar studied business management in Saarbrÿucken and obtained his doctorate in 1983. He worked as a postdoctoral fellow at the IBM Los Angeles Scientific Center and as assistant professor of information systems at the New York University and the City University of New York. Since 2002 he holds the Chair for Information Systems at the Technical University of Munich. From 2010 to 2013, he served as Dean of the Faculty of Computer Science.