Digitale Bibliothek Braunschweig

Towards a Sustainable and Efficient Component-based Information Security Framework

Jörg Uffen
Robert Pomes
Michael H. Breitner

Veröffentlicht in:
Multikonferenz Wirtschaftsinformatik 2012
Tagungsband der MKWI 2012
Hrsg.: Dirk Christian Mattfeld; Susanne Robra-Bissantz

Braunschweig: Institut für Wirtschaftsinformatik, 2012

http://www.digibib.tu-bs.de/?docid=00047553

Towards a Sustainable and Efficient Component-based Information Security Framework

Jörg Uffen, Robert Pomes, Michael H. Breitner

Leibniz Universität Hannover, Institut für Wirtschaftsinformatik, 30167 Hannover,
E-Mail: {uffen | pomes | breitner}@iwi.uni-hannover.de

Abstract

Information security and information systems (IS) security both have top management priority in many companies and organizations. In various information security models researchers recommend several important components to sustainably and efficiently enforce information security. There is little research aiming at approaches that combine theoretically and empirically substantiated principles. To fill this research gap, the aim of this paper is to discuss the adequacy of “academic” information security components, to analyze practical relevance using an empirical study and to consolidate identified factors using a principle component analysis to enhance applicability. Findings suggest two main factors which are identified as short-term and long-term as well as 18 sub-components. The results can assist companies and organizations in sustainably and efficiently implementing information security.

1 Introduction

Today´s companies and organizations (in the following referred to as “organizations”) have become increasingly dependent on information systems (IS) to carry out their business strategies. As a result, ensuring information security has become one of the main top managerial priorities in many organizations [4]. Information security management continuously faces changing requirements in complex situations [18] in consideration of balancing the needs of information access and information protection [5].

Hence, in the last decades the discussion on how to implement efficient and sustainable information security has been promoted by academics and practitioners. As a consequence, numerous information security architectures, frameworks and best-practices have been developed in order to assist organizations in implementing information security. Important academic research papers or best practice frameworks such as COBIT or ISO/IEC 27000-series indicate that information security needs to be implemented in a holistic and multidisciplinary approach, cutting horizontally across units within and over organizational boarders along the entire value-added chain.

Digitale Bibliothek Braunschweig

However, in literature there is consent about the semantic dimensions of information security: confidentiality, integrity and availability (CIA) (see e.g. [10];[17];[6];[16];[18]). In a more extended and human-oriented sense, additional dimensions are responsibility, authenticity and reliability [12]. These dimensions are the basic requirements on which the principal information security strategies have to be designed. Within an information security framework, researchers and practitioners have recommended a number of important information security components such as technical or human security factors (see e.g. [7]) but organizations often face difficulties in managing a concept that considers holistic information security components [10].

In the context of this paper, an information security framework is represented by the interaction of interdisciplinary master- and sub-components, relevant for successful and sustainable implementation of information security. Sub-components in the following are integrated parts of information security frameworks which concretize master components. These components provide a basis for organizations during implementation and maintenance of information security. Sub-components can further be characterized by numerous detailed items.

Given the variety of academic publications on the topic of component-based information security frameworks, there is still a lack of approaches that combine theoretically and empirically substantiated principles. To fill this research gap, the aim of this paper is to evaluate the adequacy of academic information security components and evaluate their practical application using an empirical investigation in order to present a holistic and all-encompassing information security framework. The resulting framework shall assist organizations to ensure a consistent and holistic view in order to properly address the organizational information security requirements [8]. Hence, the **research questions** of this paper are as follows:

1. Which information security components are discussed
   within information security framework literature?
2. How can these components be consolidated considering their practical relevance?

The authors use a structured approach consisting of four steps. During previous step, critical information security success factors are identified using a comprehensive literature review combined with the help of industry experience of the authors. In the second step, the excluded general components are systematically summarized and consolidated. This leads into a comprehensive list of information security components and forms the basis for an empirical investigation with 174 information security managers. Based on the assessment of information security components and using the principle component analysis (PCA) (see e.g. [2]), the results are summarized and interpreted.

2 Related Work on Information Security Frameworks

Researchers have discussed different component-based information security frameworks leading to recommendations on how to efficiently and sustainably implement information security (see e.g. [18];[15];[19];[10]). Therefore reviewing literature on that specific topic is an adequate method for analyzing and synthesizing prior research in order to create a “firm foundation for advancing knowledge” [22]. In our study, we used the literature review method in accordance to [22]. The results will be discussed in the following sections, starting with a brief overview of important information security frameworks.

http://www.digibib.tu-bs.de/?docid=00047553

Digitale Bibliothek Braunschweig

2.1 Existing Research in Information Security Frameworks

The research of [6], using an ontology-based approach for IS security management, recommends a people, law, organization, asset and technology view (PLOAT). These five components have to be considered when implementing an IS security management system (ISMS). Another related approach is presented by [16] contributing the IS security components strategy, technology, organization, people and environment (STOPE) in terms of supporting the use of ISO 17799:2005. Both approaches components are subdivided in more detailed items.

The layered multi-planes model provided by [19] integrates technological, organizational and legal components on a vertical layer. These components need to be addressed by vertical planes such as physical security or human interaction. The model focuses on a more technical view without considering strategic or operational issues (see also [10]). A more comprehensive approach is provided by [15] whose research relies on factors influencing the implementation of information security strategies. Therefore, the authors divide six perspectives based on their features and roles: structural, economical, organizational, environmental, technological and operational factors.

To identify several critical success factors (CSF) [18] use a three dimensional cheese approach, in which each dimension is proposed as a security control. The authors summarize three components – technical, formal and informal – which were consolidated from 12 factors (IS security architecture, business connection, information security awareness, management commitment, staff competence, information security strategy, dynamic evaluation of information security effectiveness, risk assessment, IS security integration, law enforcement and compliance, project accomplishment and security budget) and 76 indicators.

2.2 Information Security Components Deducted from Research Literature

To identify potential security components that influence the efficient and sustainable implementation of information security in organizations, the first step is to identify as many factors as possible from underlying literature. To analyze the underlying literature, the authors used the qualitative content analysis in accordance to [14]. This results in a comprehensive list of factors, which need to be summarized and consolidated into sub-components and master components.

The examination of the factors identified in the above mentioned literature review reveals that information security implementation is dependent on seven master components – technological, organizational, human, economical, compliance and monitoring, cultural and strategical – which were deducted from the identified sub-components. Figure 1 gives a summary of the mentioned security master- and sub-components which will also be briefly presented in the following sub-sections. Note that Figure 1 only lists sub-components which were frequently named and does not include the complete list of all identified items.

Digitale Bibliothek Braunschweig

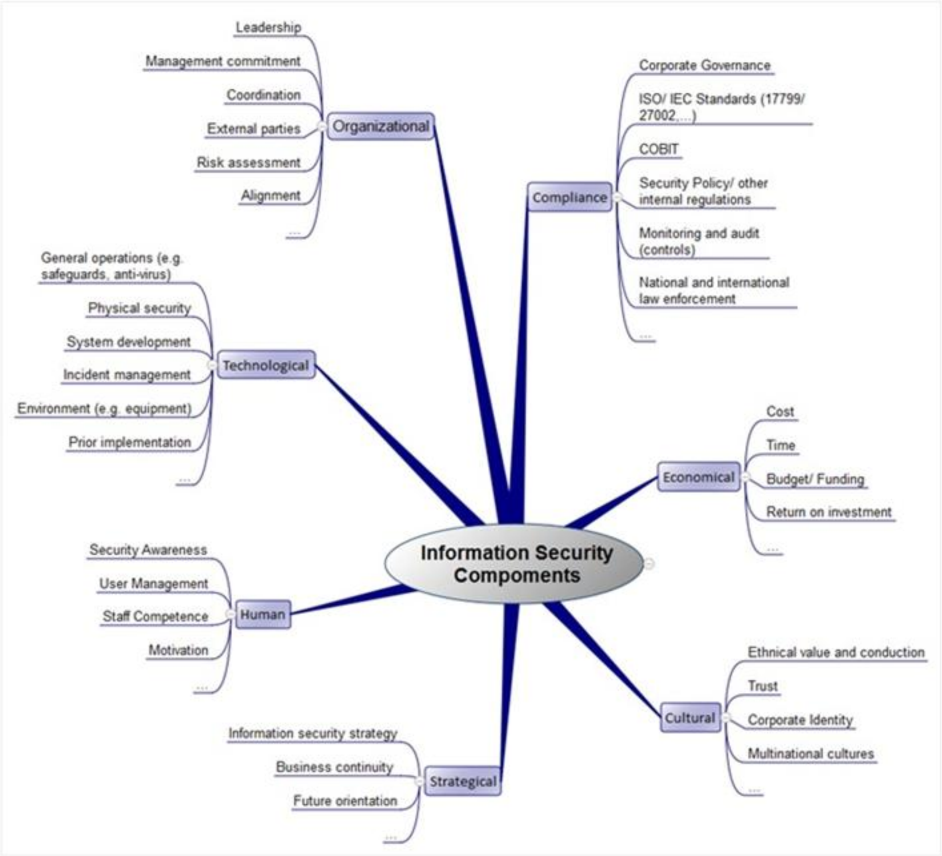


Figure 1: Information Security Components

2.2.1 Technological Component

Growing business interconnections, global networks and real-time communication result in new and complex technological security challenges (see e.g. [10]). In consideration of growing operational sophistication of current security attacks, technological security is the major part of effective information security [15]. Organizations face complex decisions considering the effective implementation of several sub-components such as intrusion detection systems (IDS) or firewalls in its information security architecture [5]. According to [15], practitioners need to reflect how to secure a seamless flow of data under the limitation of technological constraints and the emergence of new and continuously changing security threats. Nevertheless, the implementation of massive technological security components is in vain without complementary other security components [15];[4].

2.2.2 Organizational Component

Organizational components take the managerial perspective into account. Effective implementation of information security requires top-management support, sponsorship and commitment [3]. Management has to define concrete requirements, how to react systematically and methodologically in terms of security breaches. These points are critical since these decisions are accompanied by operational and technological components [18]. The harmonization of enterprise objectives with business and information security strategies is challenging [15]. Further, increasing operation and interaction with external partners require coordination on management level [6].

Digitale Bibliothek Braunschweig

2.2.3 Human Component

During the last few years, research in the human factor of information security has increased (see e.g. [4];[7]) as the most common vulnerability in information security is still the human factor [24]. End-user ignorance, deliberate acts and mistakes can lever every technological solution [4]. Therefore, behavior of the human component has to be directed and monitored to guarantee compliance with organizational security and legal requirements [8]. Appropriate methods to improve security awareness are training, education and motivation programs [23]. Further, selective allocation of authorization in terms of identity and access management has an additional preventive effect [17]. In their empirical study with about 269 employees, [7] verified three security countermeasures to reduce IS misuse: first security policies, second security training, education and awareness and third computer monitoring.

2.2.4 Economical Component

Security strategies have to be developed in order to be cost-effective [15];[17]. In practice, organizations rarely undertake return on investment calculations on completed security investments [18]. IT departments often face challenges in budgetary restrictions [23] but investments in information security are not straightforward [18]. As mentioned above, information security threats are changing rapidly, so security leads to be a time-critical issue [15]. Hence, fast decision-processes with adequate financial resources are indispensable. Consequently information security management faces the challenge to coordinate every security component in an economic way considering the needs of the organization [17].

2.2.5 Compliance and Monitoring Component

The compliance component includes internal factors such as organizational security policy or group´s requirements and guidelines as well as external factors such as information security expectations of stakeholders and other third parties, legal factors such as best-practices, national and international requirements or standards such as ISO/IEC 27002 or COBIT. Further, continuous monitoring as well as auditing procedures are necessary to guarantee that policies, processes and controls comply with the organizational objectives, strategies and visions [8]. Within information security literature there is consent that auditing and monitoring approaches are required for deterring information misuse (see e.g. [7]).

2.2.6 Cultural Component

Information security should be integrated into corporate culture [19], i.e. employees across an organization should actively live and shape the security culture. As one part, ethical conduct, such as not using organizational internet connections for private purpose, has to be regarded as an accepted way of conduct [8]. Further, trust is an established issue in information security culture [20]. Mutual trust between management and its employees is an essential part to implement new information security procedures and instruct end-users through behavioral changes in daily information security operations [8]. Behavioral changes should be embedded in employees' minds. In their research [9] highlight, that employees "become attached to their organization when they incorporate the characteristics they attribute to their organization into their self-concepts". The results of the literature review show, that these points are mostly underrepresented in information security frameworks.

Digitale Bibliothek Braunschweig

2.2.7 Strategic Component

Information security strategies are clear defined plans of organizational future objectives, which in consideration of their resources, give an input of the future development of an IS [18]. The information security strategy should be implemented as an integrated part of corporate strategy. The strategic components are the baseline for IS security management (see e.g. [17];[8]) especially for business continuity management [19], in terms of strategically manage and protect information assets [21]. After putting an information security strategy into operation, the organizations have to evaluate and if needed correct the outcomes [15].

3 Empirical Data Collection and Analysis and Model Development

Based on the definition of security components, the next step is to evaluate the practical application with the use of an empirical investigation. To gain practical implications to the above mentioned components, the authors used a structured survey methodology to collect data from experts in this research field. The questionnaire consists of 54 questions including demographic statistics. These questions cover the above mentioned seven main components and their related sub-components. To generate reliable results, only validated and tested questions were used. To increase content validity the questionnaire first was carried out by 11 independent experts, followed by an improving process based on their feedback. Afterwards, the questionnaire was conducted again by 12 other experts. All questionnaires were provided and completed via a web-based survey. Participants were IS security experts such as Chief (Information) Security Officers (C(I)SO) from German-speaking countries (in the following referred to as “information security managers”), which were identified through information security online communities. During selection of participants, the authors did not focus on any specific businesses in order to give general results to any businesses. Of the 748 preselected participants, the total sum of reliable responses was 174, yielding in a reasonable response rate of more than 23.0%. As the focus of this study is the validation of information security components, the collected data was analyzed using different analysis techniques with the help of the statistic software SPSS.

3.1 Demographic Statistics

Respondents’ organization businesses as well as size of their organization are representatively distributed. The main businesses are consulting, manufacturing (each 8.6%), government (8.0%), telecommunication (6.8%), health care (6.2%), media (5.6%) and education, finance, transport and energy (each 4.9%). The experts belong to small-sized companies with less than 100 employees (22.1%), medium-sized companies with less than 500 employees (30.0%) as well as large-sized organizations with more than 500 employees (47.9%). These issues are important aspects in generalizing the results of the study. Most respondents are middle-aged representing the age 41 to 50 (42.9%) while 25.9% representing the age 51 to 60 and 23.5% representing the age 31 to 40. Furthermore most respondents are in IS security positions represented by CSO, IS Security Specialists, CISO and IT-Reviser. The majority of respondents have a university degree (62.0%).

http://www.digibib.tu-bs.de/?docid=00047553

Digitale Bibliothek Braunschweig

3.2 Findings

As the focus of this research lies on validation of the practical application of the theoretically identified master and sub-components (see section 1), we used the principle component analysis (PCA) with varimax rotation. PCA is a branch of multivariate analysis with the purpose to identify latent variables within a various number of items [2]. Therefore, PCA is the best method to reduce the above mentioned sub-components to a lower and in practice more applicable number of factors which subgroups of variables are based on nearly similar characteristics.

	Factor	Eigenvalue	Variance (%)	Cummulated Variance (%)	Items	Interpretation	Factor loading
Technological	**Technological 1**	3.142	28.566	28.566	T1	Network administration	0.730
					T2		0.696
					T3		0.689
					T4		0.521
	Technological 2	1.351	12.279	40.845	T5	Critical system administration	0.758
					T6		0.680
					T7		0.501
	Technological 3	1.085	9.862	50.707	T8	Cryptography	0.756
					T9		0.606
					T10		0.601
Human	**Human 1**	1.358	27.164	27.164	H1	User management and user awareness	0.743
					H2		0.741
	Human 2	1.146	22.917	50.081	H3	Competency	0.839
					H4		0.687
	Human 3	1.018	20.359	70.440	H5	Access	0.899
Organizational	**Organizational 1**	1.497	29.933	29.933	O1	Top-Management support	0.843
					O2		0.820
	Organizational 2	1.216	24.322	54.255	O3	Leadership and coordination (Middle Management)	0.784
					O4		0.766
	Organizational 3	1.033	20,663	74.918	O5	Effective risk management	0.955
Compliance and Monitoring	**Compliance 1**	2.541	25.408	25.408	C1	Regulatory and legislative standards	0.831
					C2		0.771
	Compliance 2	1.458	14.585	39.993	C3	Control approaches and objectives	0.821
					C4		0.607
					C5		0.510
	Compliance 3	1.248	12.484	52.477	C6	Monitoring	0.793
					C7		0.627
					C8		0.617
					C9		0.527
Economical	**Economical 1**	1.310	32.746	32.746	E1	Monetary aspects	0.797
					E2		0.653
	Economical 2	1.009	25.220	57.966	E3	No-monetary aspects	0.800
					E4		0.579
Cultural	**Cultural 1**	1.244	31.093	31.093	Cu1	Ethical and identification values	0.814
					Cu2		0.637
	Cultural 2	1.036	25.860	56.953	Cu3	Trust	0.707
					Cu4		0.644
Strategical	**Strategical 1**	2.243	44.863	44.863	S1	Information security strategy management	0.872
					S2		0.771
					S3		0.716
	Strategical 2	1.043	20.855	65.718	S4	Business continuity	0.841
					S5		0.763

Table 1: Results of PCA 1 on Sub-component Basis

Digitale Bibliothek Braunschweig

The analysis process consists of two phases. In the first phase, PCA is used for identifying consolidated sub-components within each master component. Second phase is verifying the commonalities within the master components, which means that two kinds of PCA are necessary – one on sub-component level (PCA 1) and one on master component level (PCA 2). To identify a valid number of factors, latent root criterion is used, i.e. only factors with eigenvalues greater than 1 are elected. These variables signify factors with variance greater than 1. The appropriateness is checked using the Kaiser-Meyer-Olkin (KMO) criterion. For each analysis KMO-criterion is above 0.728 which is acceptable to perform factor analysis [13].

However, significance of factor loadings can be used to interpret the factors. All factor loadings exceeded 0.50 which is considered to be very significant [11]. Some items were not taken into account because of poor reliability. Thus, based on the included items and their factor loading, each factor is named and interpreted. To enhance the quality of the findings, the interpretations were presented and discussed with 4 PhD-students and 2 external experts, as all of them possess several years of expertise in the evaluated topic. Table 1 presents an overview of PCA 1 with the resulting factor names, the mentioned eigenvalues, the cumulated variances and the related items.

In total, 42 items loaded properly on the factors. A total of 18 factors were extracted using PCA 1. The cumulated variance in this analysis method varies between 50.0% and 75.0%.

An analysis and discussion of the different factors is shown below. Note that the following results don't represent the complete presentation of each related item. Instead the following content summarizes the most important terms on descending factor loadings on master component level:

- **Technological Factors:** include considerations for realizing technological parts of IS security architecture. Implementation requires: **network administration** which contains application security such as installation, configuration, operation and administration of e.g. firewalls, antivirus, backup and data recovery; **critical system administration** which includes alarm- and fault monitoring systems or risk system access control administration and **cryptography** which specifies built-in encryption, security certificate creation and management or electronic signature and electronic data interchange (EDI) administration.
- **Human Factors:** deal with the reduction of internal misuse of IS resources. Details contain **user management and user awareness**, **competency** and **access**. The main factor considers the raising of awareness which includes trainings or other general behavioral issues; the second factor deals with the promotion of competence on employee level as well as support of management competence in information security related topics. The latter indicates an effective organizational user access management containing authorization or identity management concepts.
- **Organizational Factors:** take the managerial perspective into account. It contains the **top-management support** reflected by top management awareness and involvement, **the leadership and coordination** on a middle management level e.g. delegation or other classical management tasks and an **effective risk management** as part of holistic identification and handling of security risks.

http://www.digibib.tu-bs.de/?docid=00047553

Digitale Bibliothek Braunschweig

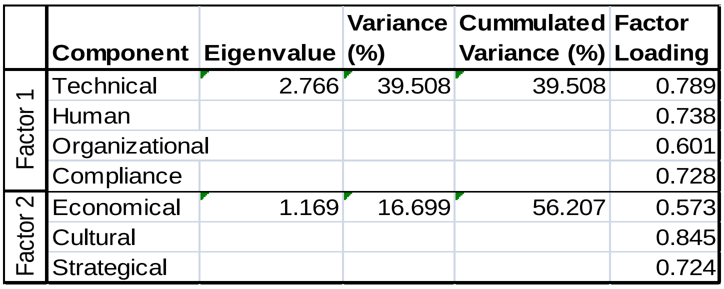
- **Compliance and Monitoring Factors:** describe an organizations legislative, regulatory and contractual environment. The **regulatory and legislative standards** as the main parts of this compliance factors contain security management as well as compliance standards represented in e.g. ISO/IEC 27002. On the other side, **control approaches and objectives** contain general concepts, guidelines and checklists such as internal information security concepts or the implementation of internal controls according to COBIT. The third factor **– monitoring –** includes the monitoring of internal misuse of IS resources, controlling of security systems or interface monitoring.
- **Economical Factors:** take the **financial** and **non-financial factors** into account. First, the protection of information assets has direct financial impacts such as project budgets, running costs or unwanted/ unexpected cost in a case of a security breach. The latter includes aspects which do not have a direct measurable impact. This can be time-related considerations, potential penalties or lost customer orders because of bad reputation.
- **Cultural Factors:** indicate natural understanding of an organizations values, artifacts and norms. Sustainable information security implementation requires **ethical conduct and identification values** as well as **trust**. Identification with the organization and the relating acceptance of corporate principles are important factors for information security implementation which have to be targeted on a long-term basis. On the other side, trust among employees and management has to be generated using, e.g. confidence-building measures.
- **Strategical Factors:** describe the fundamental alignment of organizations current and future IS dimensions. Strategies require an appropriate **management** which contains visions, objectives and goals fixed in writing in regard of current and future orientation. A more specific factor named **business continuity** encompasses emergency plans or security manuals which ensure short recovery times in the case of unavailable IS infrastructure. This is an integral element of information security strategy.

The management of each of these 18 descriptively implied factors has to be considered with a special focus during implementation of information security. Therefore, these factors have to act as a guideline for information security managers, as they will support them to understand the particular information security components that need to be tailored to the characteristics and specifics of each organization. Hence, the above mentioned factors of information security should be taken as a reference which needs to be concretized in a more detailed way.

However, the observation of the information security components identified in this study leads to the assumption that the factors can further be divided into long- and short-term components. To proof this assumption, a second PCA was taken using the seven master security components. The analysis (see Table 2) results into two main factors whose factor loadings vary between 0.573 and 0.845 with a cumulated variance of 56.207%.

http://www.digibib.tu-bs.de/?docid=00047553

Digitale Bibliothek Braunschweig



	Component	Eigenvalue	Variance (%)	Cummulated Variance (%)	Factor Loading
Factor 1	Technical	2.766	39.508	39.508	0.789
	Human				0.738
	Organizational				0.601
	Compliance				0.728
Factor 2	Economical	1.169	16.699	56.207	0.573
	Cultural				0.845
	Strategical				0.724

Table 2: Results of PCA 2 on Master-component Basis

Factor 1 highlights the technical, human, organizational and compliance components with an eigenvalue of 2.766 and a cumulated variance of 39.0% while factor 2 consolidates the economical, cultural and strategic components. This result confirms our assumption. In accordance to that, the authors named the first factor as “ubiquitous factors” which declares a more short-term orientation and the latter the authors named “sustainable factors” which declares the long-term orientation. Ubiquitous factors consist of components which are identified as omnipresent in the research literature (see section 2), in practical application and related standards (e.g. ISO 27002). These items are tangible and part of operational security management. The rationale for the second factor is that sustainable implementation relies on a strategic (long-term) orientation represented through culture as well as strategic goals and future objectives in consideration of economical component.

On the basis of these findings, practitioners should realize the interaction of short-term and long-term security elements to ensure sustainable and efficient implementation of information security. To be effective and timely, operational security decisions are based on organizational culture, their strategic orientation and the organizational global financial and non-financial resources. The short-term view lies on the basic needs towards information security in terms of reducing potential risk elements in a short reaction time. This means, for instance, investments in technical component should be done in consideration of factual necessity and organizational future orientation under the prerequisite of cost-effectiveness. According to [4] there is consent that success in information security considers investigations in both technical and social-organizational resources. These are essential parts of ubiquitous factors. According to our results, the implementation of sustainable factors is as important as the implementation of ubiquitous factors. To implement an acceptable level of information security, the organizations must create and cultivate adequate principles as a part of a security culture.

3.3 Limitations

One limitation of our study relates to the personality of participants. Each answer of participants depends on the individual risk tolerance during implementation of information security (see e.g. [1]). The questions in this study could not be examined with participants who are completely risk-averse. Further, every organization that participated in the study is based in German-speaking countries. Considering differences in the cultural and legal environment, it is likely that information security managers in other countries have different attitudes or reactions towards the implementation factors of information security within organizations.

http://www.digibib.tu-bs.de/?docid=00047553

Digitale Bibliothek Braunschweig

4 Conclusion and Future Research

This paper presents a comprehensive information security framework. This framework can be taken into consideration for implementing sustainable and efficient information security within an organization. Given the variety of academic publications on CSF for implementation and management, there's still a lack of frameworks that combine theoretically and empirically grounded principles. The study presented here aims to close this research gap. Starting with a comprehensive literature review to identify as many CSF as possible and a following structured consolidation, the applicability to the information security implementation and management is confirmed with a survey of 174 information security managers. The results consider a broad spectrum of information security factors which assist information security managers to implement and manage sustainable and efficient information security. The results offer valuable implications for information security practitioners, since the factors can be used to design new - or review existing - information security programs in organizations. For future research, we plan to extend the results to a more international context and compare these results in consideration of cultural differences. Furthermore this study can be extended taking the information security managers´ personality into consideration with personality models.

5 Literature

[1] Anderson, EE; Choobineh, J (2008): Enterprise Information Security Strategies. Computers & Security 27(1): 22-29.

[2] Backhaus, K; Erichson, B; Plinke, W; Weiber, R (2011): Multivariate Analysemethoden: eine anwendungsorientierte Einführung. 13. Auflage Springer Verlag, Berlin.

[3] Broderick, JS (2006): ISMS, security standards and security regulations. Information Security Technical Report II: 26-31.

[4] Bulgurucu, B; Cavusoglu, Ha; Benbasat, I (2010): Information Security Policy Compliance: an Empirical Study of Rationality-based Beliefs and Information Security Awareness. MIS Quarterly 34(3): 523-548.

[5] Cavusoglu, Ha; Raghunathan, S; Cavusoglu, Hu (2009): Configuration of and Interaction Between Information Security Technologies: The Case of Firewalls and Intrusion Detection Systems. Information Systems Research 20(2): 198-217.

[6] Chiang, TJ; Kouh, JS; Chang, R-I (2009): An Ontology-based Approach to the Information Security Management. In: International Journal of Computer Science and Network Security 9(11): 181-189.

[7] D´Arcy, J; Hovav, A; Galetta, D (2008): User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach. Information System Research 20(1): 79-98.

[8] Da Veiga, A; Eloff, JHP (2007): An Information Security Governance Framework. Information Systems Management 24(4): 361-372.

[9] Dutton, JE; Dukerich, JM; Harquail, CV (1994): Organizational Images and Member Identification. Administrative Science Quarterly 39(2): 239-263.

http://www.digibib.tu-bs.de/?docid=00047553

Digitale Bibliothek Braunschweig

[10] Eloff, JHP; Eloff, MM (2005): Information Security Architecture. Computer Fraud & Security 2005(11): 10-16.

[11] Hair, JF Jr.; Black, WC; Babin, BJ; Anderson, RE (2010): Multivariate Data Analysis: a Global Perspective. 7. global ed. Pearson, Upper Saddle River [inter alia].

[12] International Organization for Standardization (2004): Information Technology – Security Techniques – Management of Information and Communications Technology Security – Part 1: Concepts and Models for Information and Communications Technology Security Management (ISO/IEC 13335-1:2004).

[13] Kaiser, HF (1974): An Index of Factorial Simplicity. Psychometrika 39(1): 31-36.

[14] Mayring, P (2004): Qualitative Content Analysis. In: Flick, U; von Kardorff, E; Steinke, I: A Companion to Qualitative Research. Sage Puplications, London.

[15] Park, S; Ahmad, A; Ruighaver, AB (2010): Factors Influencing the Implementation of Information Systems Security Strategies in Organizations. In: *Proceedings of the International Conference on Information Science and Applications (ICISA)*. Seoul, Korea.

[16] Saleh, MS; Alrabiah, A; Bakry, SH (2006): Using ISO 17799:2005 information security management: a STOPE view with six sigma approach. International Journal of Network Management Vol. 17: 85-97.

[17] Tashi, I; Ghernouti-Hélie, S (2009): Information Security Management is not only Risk Management. In: *Proceedings of the 4th International Conference on Internet Monitoring and Protection (ICIMP)*. Venice, Italy.

[18] Torres, JM; Sarriegi, JM; Santos, NS (2006): Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness. In: *Proceedings of the 9th International Conference on Information Security*. Samos Island, Greece.

[19] Trček, D (2003): An Integral Framework for Information Systems Security Management. Computers & Security 22(4): 337-360.

[20] Tudor, JK (2000): Information Security Architecture – An integrated approach to security in an organization. Auerbach Publications, Boca-Raton, FL.

[21] Upfold, CT; Sewry, DA (2005): An Investigation of Information Security in Small and Medium Enterprises (SME´s) in the Eastern Cape. http://icsa.cs.up.ac.za/issa/2005/ Proceedings/Research/ 082_Article.pdf. Accessed: May 19, 2011.

[22] Webster, J; Watson, RT (2002): Analyzing the Past to Prepare for the Future: Writing a Literature Review. MIS Quarterly 26(2): xiii-xxiii.

[23] Werlinger, R; Hawkey, K; Beznosov, K (2009): An integrated view of human, organizational, and technological challenge of IT security management. Information Management & Computer Security 17(1): 4-19.

[24] Yildrim, EY; Akalp, G; Aytac, S; Bayram, N (2011): Factors Influencing Information Security Management in small- and medium-sized enterprises: A case study from Turkey. International Journal of Information Management 31(4): 360-365.

http://www.digibib.tu-bs.de/?docid=00047553