Human Factors in Cybersecurity, Vol. 53, 2022, 92–101
https://doi.org/10.54941/ahfe1002206

A Coherence Model to Outline Obstacles and Success Factors for Information Security from the CISO's Point of View

Erfan Koza and Asiye Öztürk

Clavis Institute for Information Security, Niederrhein University of Applied Sciences, Germany

ABSTRACT

Against the backdrop of the progressive digitalization of Critical Infrastructures (CRITIS), especially within the socio-technical fields, this paper addresses the identification of obstacles as well as critical, technical, and human success factors, which play an essential role in efficient information security management. Furthermore, the focus is also put on the crystallization of differentiated views regarding the meaningfulness and usefulness of laws. To this end, we conducted a study with 86 chief information security officers, including CRITIS with 76% participation and non-CRITIS with 24% participation, data center operators (14), water and wastewater utilities (25), energy supply companies (33), and healthcare stakeholders (14) in Germany. The study is based on a methodological pluralistic orientation in which, in addition to the integration of quantitative methods for empirical data collection, other analytical approaches are used to determine coherence and correlation. As an artifact, the empirically validated factors are compiled intersectoral in a coherence model and related in terms of causality.

Keywords: Information security, CRITIS, ISMS, CISO, Coherence model, ISO/IEC 27001

INTRODUCTION

In the context of socio-technical systems, the term "information security" is composed of the three coherent topics: Technology, human, and organization. This interpretation focuses on the complementary behaviors and interactivity of these three subject areas, whose interaction can be stated according to the holistic solution approach in an information security management system (ISMS). The development of national efforts to increase the resilience of IT systems and to initiate legal liabilities to information security can basically be traced back to the period between 2005 and 2019. The development of individual initiatives and legal foundations was carried out incrementally during the indicated period and is currently continuing. Following the adoption of the first cyber security strategy by the German cabinet in 2011, the IT Security Act (IT-SA) was passed in 2015 as an article law in the chronological order. Initiated by the critical infrastructure (CRITIS) strategy of the federal government with its legal anchoring in Article 1 Number 2 and Number 7, the IT

SA makes relevant changes within the law on the Federal Office for Information Security (BSIG) for operators of CRITIS [BMI, 2009], [GB, 2009], [GB, 2015], [BSI, 2017]. In this context, operators of CRITIS are required to "(...) take appropriate technical and organizational precautions to prevent disruptions to the availability, integrity, authenticity and confidentiality of their information technology systems, components, or processes (...)" (Section 8a (1) sentence 1 BSIG), [GB, 2009]. Thus, CRITIS should have been dealing with the implementation, the realization of the continuous improvement processes Plan-Do-Check-Act (PDCA) cycle and the certification and auditing of ISM systems for about five years and should have generated valuable empirical and practical impressions from this, which are of high value for the research [BMI, 2016].

Thus, this paper represents a work relevant to the field of information security management in the form of a well-founded study. It is suitable to show weaknesses and risks as well as the chances of an implementation of an information security management system based on the international standard ISO/IEC 27001 under consideration of user-related perception in a socio-technical environment (human-based) in a transparent and fact-based way and offers room for further research. Regulators and legislators can also benefit from this work by adapting the requirements of different regulators, thus making them more feasible for companies to implement. Furthermore, the empirical survey, which has already been published in a national language publication [Koza, 2021], can be used to explain relationships on a sound scientific and international basis with new knowledge. For example, the results regarding the fundamental diffuse perception of cyber dangers and the relevance of information security from the perspective of management, the lack of time and personnel resource capacities in IT security, and the failure to consider the IT supply chain of CRITIS represent a very important basis for future legislative and scientific measures.

Due to the similar process structure of companies within the CRITIS industries in international comparison, the similar depth and scope of the degree of digitalization and automation dominated using standardized technologies, as well as the intersectoral and international character of ISO/IEC 27001, the results of this study in international comparison can be transformed to any company regardless of geographical location that deals with the topic of information and IT security in detail. Thus, the coherence model represents a good way of interpreting and presenting the results in terms of an overall view and, in this context, can enrich the state of research in this area.

METHODOLOGY

To operationalize the research study, the first step is to select the fields to be investigated (ICT: data center operators, water: drinking water supply and wastewater disposal companies, energy: plant and network operators, and healthcare: Hospitals and university clinics) were selected. In a second step, as part of a methodologically pluralistic approach, in addition to the integration of quantitative methods with the "fully structured online survey," methods for structural and content analysis are also planned in order to retain the possibility of validating the knowledge gained from the online survey in a structured format according to the respective sector affiliation (distribution of statements in the respective sector) and according to the respective cross-sectoral commonalities and, if necessary, to be able to deepen these. The designed topic blocks and questions address obstacles to information security (15 questions), success factors of an ISMS (18 questions) and relevance of legislation (10 questions). To this end, a survey was conducted with 86 chief information security officers, including CRITIS with 76% participation and non-CRITIS with 24% participation, data center operators (14), water and wastewater utilities (25), energy utilities (33), and healthcare stakeholders (14) in Germany. The addressees were selected in such a way that a heterogeneous corporate landscape could be involved to be able to address small and medium-sized enterprises (SMEs) as well as large companies and corporations equally in the online survey. The business landscape involved in the study also shows a certain heterogeneity, in which all the classifications made by the European Union, except for micro enterprises (<10), occur in terms of the definitional interpretation of SMEs. 13% of respondents indicate that they have 10-49 employees. Also, another 13% say they have 50-249 employees in their company. 250-1000 employees employ 39% of respondents. Also, 35% of respondents indicate that they have over 1000 employees in their company. As an artifact, the empirically validated factors are compiled and causally related across industries in a coherence model. The designed model for information security outlines the correlative relationships and summarizes the technical influences with their respective degrees of effectiveness to contrast the obstacles and the critical success factors to create an overall picture.

RESULTS

To identify obstacles and success factors for information security, various statements with different focal points were integrated into the written online survey, as shown in Fig. 1 and Fig. 2. The greatest intersectoral obstacle to sustainable and resource-efficient information security in operational structures is the increased personnel and time required so that the requirements defined in the ISMS can only be met with a high level of internal and/or increased external effort (76 companies, 88%). The requirements defined in ISO/IEC 27001 (114 controls in Annex A) must be projected and individually specified in the statement of applicability to the respective area of application. The application area under consideration usually consists of several centralized and decentralized IT systems and network components that are set up in separate network segments with different communication protocols, as well as software and hardware technologies to fulfill differentiated tasks. The increasing complexity and heterogeneity of IT systems and IT network landscapes are cited as the second greatest intersectoral obstacle to information security by around 74 companies, i.e., 86% of respondents. In view of numerous legal and self-imposed requirements, companies must set up and continuously develop several management systems simultaneously. This results in a permanent personnel overload, which is caused by the strong

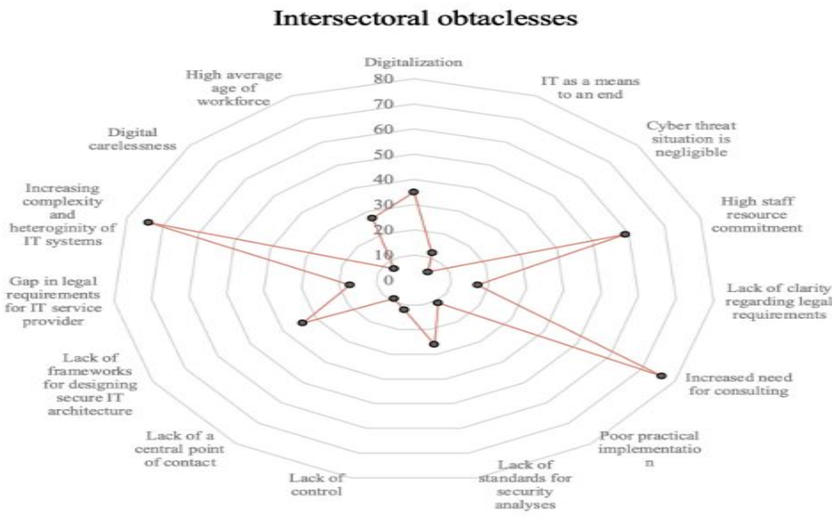

Figure 1: Intersectoral obstacles for information security.

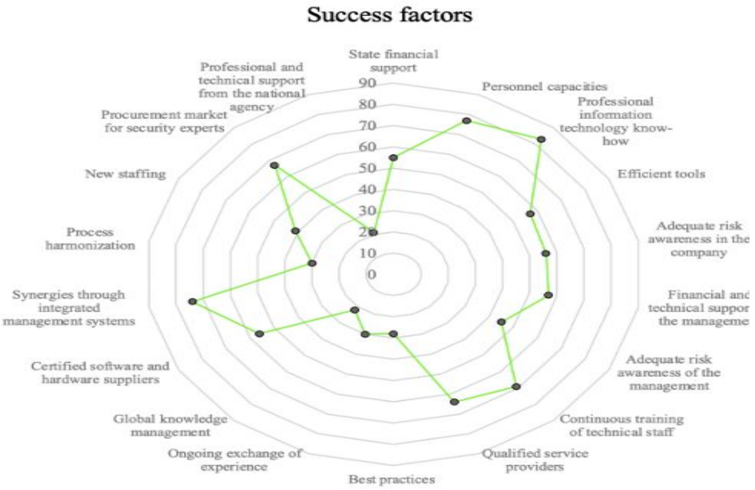

Figure 2: Success factors for information security.

commitment of personnel resources. For example, ISMS-dedicated tasks are broken down as on-top tasks to regular organizational units, because of which they are effectively overloaded with tasks. 59 companies (69%) indicated that they consider high staff resource commitments (=overload) to be the third biggest obstacle.

In addition to the identified intersectoral obstacles to sustainable information security, research is also conducted into the critical success factors for resource-efficient and efficient operation of an ISMS. 83 companies (97%) see the internal availability of specialist, IT know-how as the most important critical success factor. The thematic characteristics of information security are diverse and address a broad spectrum of several differentiated subject areas, including conception, implementation, and ongoing monitoring which

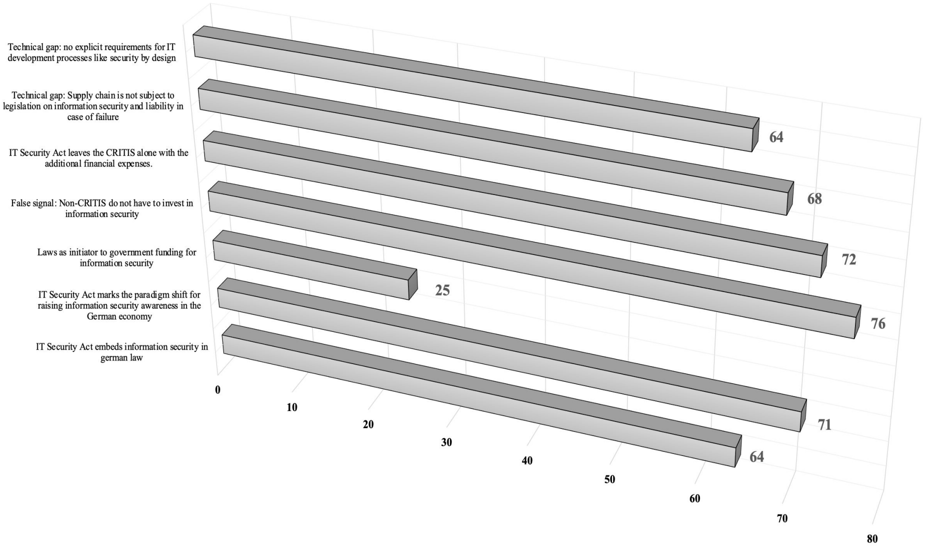

Figure 3: Effects of legislation for information security.

require a deeper understanding of information technology. However, the existence of information technology know-how is directly linked to the existence of internal specialist resources. For example, 77 companies (90%) stated that personnel capacities, sometimes through the integration of a chief information security officer as well as through the integration of additional security specialists, represent the second most important critical success factor for an efficient and sustainable ISMS. However, integration of internal resources requires the financial and professional management support. Against this background, 57 companies (66%), make the statement that the technical and financial support of management is essential for the success of an ISMS. Overall, 55 companies (64%) stated that financial government support is also a critical success factor. In total, 72 companies (83%) also complain that although the IT SA declares the right issues, it leaves the CRITIS alone with the additional financial expense incurred by meeting the legal requirements (Fig. 3). The third critical success factor can be associated with integrated management systems. The so-called "common structure of ISO standards" for management systems makes it possible to harmonize management systems with different focal points with the aid of their common intersection, so that multiple workloads and documentary redundancies can be avoided.

This success factor can thus be directly defined as an efficiency-increasing instrument for eliminating the strong ties between personnel resources (see third-largest obstacle) due to the many regulations and generating synergies from this. Thus, 74 companies with a percentage share of 86% make the statement that the synergies achieved through the synchronization and harmonization of the management systems (quality management system, technical safety management system, ISMS, environmental management system, energy management system, etc.) represent the third most important critical success factor for resource-saving and efficient operation of an

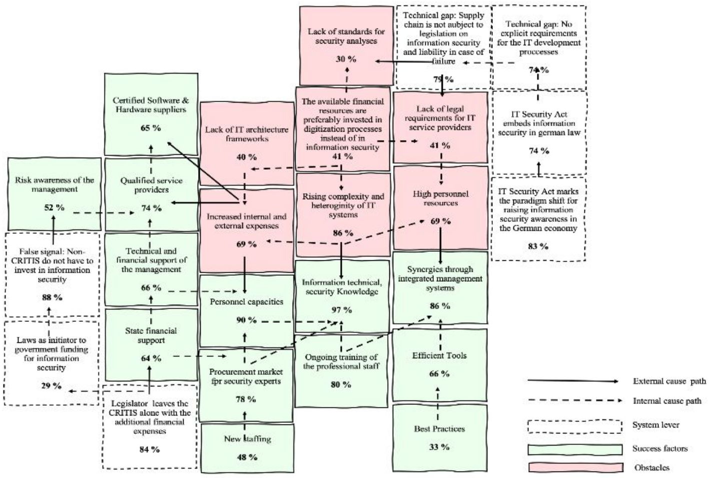
Lack of standards for security analyses
30 %
Technical gap: Supply chain is not subject to legislation on information security and liability in case of failure
79 %
Technical gap: No explicit requirements for the IT development processes
74 %
Certified Software & Hardware suppliers
65 %
Lack of IT architecture frameworks
40 %
The available financial resources are preferably invested in digitization processes instead of in information security
41 %
Lack of legal requirements for IT service providers
41 %
IT Security Act embeds information security in german law
74 %
Risk awareness of the management
52 %
Qualified service providers
74 %
Increased internal and external expenses
69 %
Rising complexity and heteroginity of IT systems
86 %
High personnel resources
69 %
IT Security Act marks the paradigm shift for raising information security awareness in the German economy
83 %
False signal: Non-CRITIS do not have to invest in information security
88 %
Technical and financial support of the management
66 %
Personnel capacities
90 %
Information technical, security Knowledge
97 %
Synergies through integrated management systems
86 %
Laws as initiator to government funding for information security
29 %
State financial support
64 %
Procurement market fpr security experts
78 %
Ongoing training of the professional staff
80 %
Efficient Tools
66 %
Legislator leaves the CRITIS alone with the additional financial expenses
84 %
New staffing
48 %
Best Practices
33 %
External cause path
Internal cause path
System lever
Success factors
Obstacles

Figure 4: Coherence model with obstacles and success factors.

ISMS. However, if the human resources are not available, they must first be acquired at great expense on the procurement market. Thus, a total of 67 companies (78%) considers the availability of adequate security experts to be the fourth most important success factor to be able to adequately map the topic of new staffing in information security. In addition, the availability of software-based solutions and support tools plays a relevant role, e.g., to map the documentary and analytical processes of an ISMS more efficiently and in a way that conserves resources (57 companies, 66%). Furthermore, another 56 companies (65%) stated that the use of certified software and hardware products is to be defined as a further intersectoral critical success factor to be able to achieve the defined security level in the network. The results are summarized below in a cause-and-effect model.

CONSOLIDATION IN A COHERENCE MODEL

The coherence model (Fig. 4) designed for information security outlines the correlative relationships and summarizes the specialist influences with the respective degree of effectiveness to contrast the obstacles and critical success factors and create an overall picture from this.

Digitization and investments in digitization trends preferred by companies (41%) are considered as initial obstacles in this context. The dilemma here is that existing financial resources are generally preferred to be invested in digitization and automation trends rather than information security. These investments are used directly to optimize or increase the efficiency (reduction of process and personnel costs) of existing business processes. This can spark a discussion about the added value of information security, as the benefits of information security cannot be measured in monetary terms using conventional methods and metrics and is therefore an abstract entity for many decision-makers. Another circumstance that can lead to the deterioration of this view is the fact that the designed redundancies and fallback levels are misused as an argumentative chain to reject further investments in information security. Here, the consequences of a cyber threat are denounced with the compensation capability of the conceived fallback levels, i.e., with the reactive and corrective capabilities. The relevance of information security in terms of prevention is not properly considered here. In essence, this view means that, irrespective of the existing fallback levels (reactive or corrective measures), the hazards and effects are dealt with, and, in the sense of prevention, measures are designed to reduce the probability of hazards occurring. The reason for such an inappropriate perception of security also has primarily relates to the fact that users usually make IT risks and IT hazards based on their practical experience already gained in the field of supply security and risk management. This can be fundamentally related to the fact that the existing sense of security is pronounced by the fact that no widespread and serious IT security incidents and information security incidents have occurred or have not been detected so far that could jeopardize operational capability. This deceptive sense of security is an implication because it is possible that many the organizations have not integrated detecting and offensive security systems that reveal their IT system vulnerabilities or detect incidents before misuse that would otherwise have gone undetected. The existence of a relevant understanding of security (success factor: Risk awareness of the management: 52%) on the part of the decision-makers can help to ensure that the necessary financial and human resources to fulfill these tasks can even be released on a voluntary basis irrespective of the legal requirements. To this end, the IT SA serves as a stimulus to mark the beginning of the paradigm shift and, in this context, to sensitize the German business community to the issue of information security by ratifying IT SA. To this end, it embeds the issue of "information security" in national law. However, companies complain that despite the importance of the declaration of the IT SAs, it leaves companies alone with the additional financial burden resulting from the requirements defined in the IT SA. Therefore, it may be that the possibility of receiving financial support in the form of subsidies is also a positive stimulus that can encourage management's willingness to make information security investments.

Such impulses can currently be observed in the healthcare sector, where hospitals and university clinics that do not explicitly fall under the BSIG regime can apply for dedicated funding for selective improvements in IT security up to the holistic optimization and introduction of an ISMS until the end of 2021, based on the defined funding pools under the KHZG (Hospital Future Act) with § 19 KHZG in conjunction with § 19 KHSFV para. 1 sentence 1 nos. 1 to 10 KHSFV (regulation on the management of the structural fund in the hospital sector). While adequate risk awareness on the part of management is seen as an elementary prerequisite for planning and releasing resources, as well as monitoring and controlling measures, risk awareness on the part of employees is a fundamental prerequisite for information security awareness to be able to generate an appropriate security culture in the organizational structure in the long term. The obstacle that acts as a counterforce here can be traced back to demographic change, in which the average higher age structure in the workforce (digital carelessness) leads to vulnerability of the human factor, whereby the weakness of the human firewall is exploited as a gateway by social engineering. In addition, the technical gaps within the legal frameworks are criticized, as these generally define a few legal requirements for IT service providers. This technical gap is of great importance because organizations, regardless of their sector affiliation, generally work with external IT service providers in software and hardware technologies and thus must rely on products and services that may not have any security-related features. In this context, it must be stated that potential security gaps in hardware and software components cannot be analyzed and eliminated independently by companies due to a lack of capacity and knowledge. Instead, organizations must rely on the security analyses, development processes and test procedures of IT service providers, whereby their product liabilities generally do not include security-related deficits. Thus, the transfer of IT security to the component level is missing. Already in the development phase, care should be taken to ensure that the smartness of software and hardware components is not used in isolation for productivity benefits but also as early detection units and for the detection and correction of cyber-attacks. In sum, IT security must be incorporated into the design, planning and manufacture of IT components, and thus into the corporate infrastructure.

CONCLUSION

Obstacles in information security concern the holistic approach, which can be found within the triangulation of information security (IT security, organizational security, and human factors). According to this interpretation, human factors can be divided into two basic areas from the perspective of a CISO. This differentiation primarily concerns the human factor as a strategic decision-maker.

CISOs usually work with a fixed budget and must make strategic decisions that are economically sustainable and executed properly in terms of investment protection. However, they must also consider finite time and human resources and thus make their decision-making processes dependent on their own resource capacities and level of knowledge. Thus, this primary consideration of the human factor must be combined with the secondary factor of “humans as operational employees in the first line of defense.” The two primary and secondary consideration are usually in a multilateral interaction and are consequently fully dependent on each other. Thus, the possibility of integrating intelligent security approaches, even if this view is very often neglected, is a question of time and technical resource capacity and knowledge level. For example, many market-accessible intrusion detection systems (IDS) for attack detection can currently be procured for a fee and implemented in the company’s own network landscape, either hardware-based or as an appliance. However, from the CISO’s perspective, the integration of technical solutions is only half the story. The other half of the reality concerns the fact that, for example, every incident calls a response. If the CISO does not have his own free resources (time and technical), he will receive many events and incidents, which he cannot adequately process and eliminate. This may leave many vulnerable points still open. On paper, the CISO has an IDS solution.

However, the effectiveness of a measure can only be determined by visible and security-compliant system behavior and user behavior, which is not the case in this illustration. This argumentative execution ultimately represents the significance of the human factors. In this context, intelligent technical solutions, methods, and procedures are only tools which humans use to achieve and optimize a better level of security. It is therefore foolish to believe that smart technical solutions are the answer to progressively increasing cyber threats. This statement is relevant in the sense that networked computer technology still takes place in a socio-technical environment, i.e., within human-computer interaction. However, the human factor in its entirety is influenced by the monetary clout of the organizations and the market-accessible experts. Internationally operating organizations and those that can ignite a designated financial force are usually better able to make sufficient investments in information security. These investments are used both to hire new cybersecurity engineers and thus increase the level of knowledge and to integrate approaches to ensure the state of the art in terms of IS. In contrast to the companies listed above, however, there are also many SMEs that focus or prefer to focus their financial efforts on digital solutions.

Looking at the German corporate landscape, for example, SMEs dominate this German corporate landscape with more than 90%. If one follows this fact, in conjunction with the above premise, one also recognizes that such companies may need financial government support. In particular, the possibility of state financial support and tax advantages for CRITIS and non-CRITIS, which are to be defined as SMEs, then plays a significant role. This understanding in its generality and at the individual levels of argumentation is of great importance.

With this understanding, digitization and information security are understood as parallel processes that are executed successively and iteratively and do not represent an isolated state. According to the derivation principle, the world of cyber threats can be better and sustainably combated if CISOs could be given the fundamental and comprehensive understanding: **First axiom:** Digitalization is an enabler for innovation. Information Security (IS) is an enabler for digitalization. **Second axiom:** Investments in digitalization must be underpinned in parallel with investments in IS. **Third axiom:** However, investments in IS can also be made independently of investments in digitalization.

REFERENCES

BMI, (2009), Federal Ministry of the Interior: National Strategy for Critical Infrastructure Protection (CRITIS-Strategy), 2009.

BMI, (2016), Federal Ministry of the Interior: Draft of the Federal Ministry of the Interior. Draft Ordinance on the Designation of Critical Infrastructures under the BSI Act (BSI Critical Infrastructure Ordinance - BSI Critical Infrastructure Ordinance), 2016.

BSI, (2017), Federal Office for Information Security: Implementation of the IT Security Act from the BSI's Perspective, 2017.

GB, (2009), German Bundestag: Law on the Federal Office for Information Security (BSIG- BSI-Law), (BGBI. I. p. 2821) Berlin, 2009.

GB, (2015), German Bundestag: Draft Act on Enhancing the Security of Information Technology Systems (IT Security Act). Federal Government Bill, Printed Paper 18/4096, Berlin, 2015.

Koza, (2021), E. Eine empirische Kontentanalyse zur Ermittlung von praxisorientierten Optimierungsfeldern und Ansätzen zur Erhöhung der Resilienz der IT-Systeme im Sinne der ganzheitlichen Betrachtung der Informationssicherheit, 2021, Gesellschaft für Informatik, Conference paper Informatik21, in Lecture Notes in Informatics (LNI), Berlin, 2021.