A Framework to Achieve Cybersecurity Accountability of Critical Infrastructure Providers – A Design Science Research Approach

Barbara Krumay[1](✉), Edward W. N. Bernroider[2], and Roman Walser[2]

[1] JKU Linz, Science Park 3 – 1, Altenberger Straße 69, 4040 Linz, Austria
barbara.krumay@jku.at
[2] WU Vienna, Building D2, Entrance C, Welthandelsplatz 1/D2/C, 1020 Vienna, Austria
{edward.bernroider,roman.walser}@wu.ac.at

Abstract. Today's pervasive use of information systems (IS) not only comes with many opportunities but also with considerable risks especially in relation to cyberattacks, which become increasingly sophisticated and dangerous. Especially organizations providing critical infrastructures are at risk, which are held to account by governments to ensure sufficient protection. Governments request information to monitor cybersecurity levels of critical infra-structure providers over time, which are today subject to respective nation-wide legislation in developed economies. Following guidelines of design science research, this study offers a generic framework that supports continuous monitoring and benchmarking of an organization's cybersecurity status. It is generic allowing application by different critical infrastructure providers and usage by government institutions to help achieve oversight of the nation-al cybersecurity status. Our design proposition is supported by an extensive review of academic literature, the consultation of relevant industry standards, and two main rounds of field interactions. The framework includes 15 major risk areas, and a collection of associated metrics and controls, which cover material and social mechanisms. We would like to note that our domain of study would require more design work that targets knowledge accumulation spanning academic research and industry practice.

Keywords: Cybersecurity · Critical infrastructures · Design science research

1 Introduction

The ubiquitous use of information systems (IS) has changed the world as a whole. We depend on IS in our daily life as governments and societies rely on IS in many ways. Not surprisingly, IS are particularly threatened by attacks from the cyberspace and therefore require adequate protection [1]. From the viewpoint of governments, a special group of organizations, called critical infrastructure providers, are of particular importance to the society, such as hospitals, energy providers, and internet service providers [2, 3]. These

S. Za et al. (Eds.): ItAIS 2020, LNISO 50, pp. 233–248, 2022.
https://doi.org/10.1007/978-3-030-86858-1_14

organizations need to operate on external accountability [4]. Meaning, critical infrastructure providers are held to account to implement the required measures to improve cybersecurity and also report on their current state of cybersecurity. Such measures, however, are manifold and exist in a vast number, either as stand-alone measures or as part of well-established frameworks, guidelines or standards. What is more, existing frameworks and standards seem to run short in specifically helping such organizations to assess how well they are prepared to protect against cyberattacks [5]. In this study, supported by a governmental funding scheme, we therefore aimed at developing a framework to help these organizations to assess their current cybersecurity status and to ensure those insights can be used by the government to gain oversight about the nationwide cybersecurity status of critical infrastructures.

Specifically, our objectives were to (i) to design and test a framework that can help to provide transparency in terms of the preparedness of critical infrastructure providers against cyberattacks, (ii) which allows for combining the results of all participating organizations applying the framework. The former objective (i) is internally oriented to allow organizations, in particular critical infrastructure providers, to assess their cybersecurity status regarding their main risk areas. For this purpose, we focused on assessing threats, vulnerabilities and their level of preparedness. The second objective (ii) is externally oriented and should allow governmental authorities to compile the information into a landscape showing and comparing the status of cybersecurity among critical infrastructure providers. The scope of factors considered was intentionally not limited to technical perspectives, but also includes additional social and contextual (e.g. environmental) aspects, which are likely to have an influence on cybersecurity.

In terms of methodology, we followed a design science research (DSR) approach [6, 7]. We started with a structured literature review to identify indicators related to our assessment related objectives in relation to cybersecurity. Based on this and further empirical sources and methods (i.e. workshops, focus groups), we designed and evaluated the framework in multiple iterations. Additionally, we observed how experts from the field (i.e., security experts from business) were able to apply the framework in practice and observed them while operating it.

2 Conceptual Background

2.1 Cybercrime and Cyberattacks

Hardly any organization has not fallen victim to attacks out of the cyberspace, and even private people are not untroubled by such attacks. The resulting costs for the society seem to be enormous, however, hard to measure [8, 9]. Of course, cybercrime is a complex phenomenon, as it is global with no boundaries, it is innovative, as cybercriminals seem always to be one step ahead and it is ubiquitous, as it may target and compromise any computer [2, 3, 8, 10]. New technologies and services, such as the Internet of Things (IoT), cloud computing, blockchain or smart grids [11–13] increase the complexity of protection, as newly adopted technologies are less proven and thus often more vulnerable. Besides, terms like cyberterrorism or cyber espionage [14] blur the understanding of what cybercrime is. Cybercrime covers “different criminal activities where computers and IS are involved either as a primary tool or as a primary target” [15]. Cybercrime reflects on one hand traditional crime (e.g., theft, fraud, discrimination), often with a specific IS-related component (e.g., theft of cryptocurrency) but also crime uniquely related to IS and the infrastructure of such (e.g., distributed denial of service attacks, malware, ransomware) [15–17]. Since computers have become ubiquitous and smart systems control substantial parts of the production, logistics and industrial systems [18–20], the number of targets is constantly growing. Cyberterrorism is mainly related to bringing down the infrastructure of a nation to put pressure on a government, but could also occur with terroristic intentions [14, 15]. Recent statistics show that attacks from cyberspace against different targets have not only increased in quantity, but also in severity [21]. Cyberattacks, defined as any "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks" [22], try to exploit vulnerabilities of organizations on different levels. Vulnerabilities in this context have been defined as "a weakness in design, implementation, operation or internal control" [23]. This definition seems to focus mainly on the technical level, such as built-in software and hardware problems [24, 25]. However, the individual (personal) level is at least equally important since flourishing techniques such as social engineering and phishing make use of limited knowledge, low awareness and laxness regarding cybersecurity issues [26–29].

2.2 Cybersecurity and Risk Management

Measures to fight cybercrime are often subsumed under the term cybersecurity or information security. However, it has been argued that the difference between the two is the human dimension: in information security, the human factor is bound to the process, whereas cybersecurity integrates human beings as targets that have to be protected [30]. According to the International Telecommunications Union (ITU), "cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's asset" [31]. As this is a very holistic definition, it covers not only technological but also social, organizational and legal aspects. Therefore, it is necessary to form activities addressing these threats in a holistic way, covering relevant social, organizational and legal aspects. The NIST framework further divides activities into different groups: "Identify, Protect, Detect, Respond, Recover" [32]. It can be argued that these activities show a chronological relationship with cyberattacks, in particular pre-attack (prepare, prevent, deter, identify), during the attack (protect, defend, respond) and post-attack (repair, recover) activities. The framework AVOIDIT differentiates attacks according to their attack vector, operational impact, defense, informational impact and target [33]. An often-used approach is to identify activities in relation to confidentiality, integrity and availability of information [34]. Besides the already mentioned NIST framework, other frameworks aim to support organizations in handling the complexity of information security and cybersecurity management. The ISO 2700x family [35] is a widely adopted framework with standards for implementing an information security management system to measure, analyze and evaluate information security issues and activities. In central Europe and German-speaking countries, in particular, the so-called BSI IT baseline protection ("Grundschutzkatalog") [36] was the de-facto standard methodology to identify and implement computer security measures in organizations for a long time. Anyway, a more holistic approach is needed to handle the increasingly challenging task of assuring a reasonable level of cybersecurity. With regard to technical threats, numerous measures are reflected by frameworks and applied by professionals, from encryption to access management, from firewalls to software updates. Putting the human being as a major ‘weak point’ more into focus, awareness building activities and training seem to be the appropriate approach [28, 37]. What the frameworks have in common is the idea of measuring indicators to be able to manage the challenges [1]. This is a challenging endeavor, as IS highly depend on and influence each other, hence testing and assessing where the problem is, is a complex task [9]. Again, frameworks and guidelines provide metrics or so-called Key Risk Indicators, which should be selected based on distinct criteria such as impact, effort to implement, measure and report, reliability and sensitivity [23]. However, measuring or assessing the organizations’ cybersecurity status is also a precondition for calculating their risk. In the current version of ISO 31000, risk is described as “effects of uncertainty on objectives” [9]. An often stressed basic formula for calculating risk is the combination of likelihood times consequences [38]. Regarding cybersecurity, the relationship between threats and vulnerabilities and factors like consequences, asset value or likelihood and impact on the organization [39–42]. Besides assessing the risk level, there are several ways to cope with risk, such as risk avoidance, risk reduction or mitigation, risk-sharing or transfer as well as risk acceptance [23]. In the NIST Special Publication 800–30, risk mitigation is defined as “a systematic methodology used by senior management to reduce mission risk” [41]. The possibilities include risk assumption, avoidance, limitation, planning, transference as well as research and acknowledgment [41]. Whereas most of the risk mitigation possibilities are clearly within the scope of organizations, transferring and sharing risks extend the scope beyond the companies’ boarders. On one hand, it integrates supply chain partners for sharing the risk, on the other risk insurances have become a common instrument of transferring risks [43, 44]. Summing up, organizations have to invest in cybersecurity activities on all levels – hardware, software, and employee - to reduce IS vulnerabilities [45].

2.3 Critical Infrastructure

Although cybersecurity is an issue for all organizations, it becomes a menace to the public when attacks negatively impact infrastructure supporting our daily life, such as power grids [46], hospitals [47], or smart cities [48]. This shift from a rather company or micro-level to a wider and global macro level induced governments but also organizations like the European Union to strengthen their efforts towards fighting cyberattacks, in particular when threatening critical infrastructure providers [49–51]. What defines a critical infrastructure is its importance for a nation when failure or reduction of service may menace security, economy, public health or safety [5, 32]. This includes energy (electricity, oil and gas), transport, banking, financial market infrastructures, healthcare, water supply as well as digital infrastructure such as internet exchange points [5]. Organizations – obliged to it or not - follow these frameworks in order to establish their internal cybersecurity activities and risk management. In our further examination, we focus on the two already mentioned directives, published by the US government and the European Commission due to their importance. The NIST Cybersecurity Framework has first been published in 2014, the current version (1.1) dates back to April 2018, aiming at supporting providers of critical infrastructures to handle cybersecurity-related issues holistically [32]. Consisting of best practices, standards and guidelines for appropriate action, it has soon been adopted not only by providers of critical infrastructures but also IT and security professionals in general [52]. The NIST framework comprises of five functions (identify, protect, detect, respond, recover), consisting of 23 categories and 108 subcategories, structuring activities in accordance with the functions. In Europe, on the other hand, the European Union had published the so-called EU NIS Directive on cybersecurity in 2016, which had to be implemented by Member States 2018 [5]. It obliges providers of critical infrastructures to continuously monitor threats from cyberspace, assess imminent risks and implement according technical and organizational activities to secure their IS. The NIS Directive sets goals on three levels, in particular increased cooperation at EU-level, improved cybersecurity capabilities at the national level, as well as the implementation of incident reporting and risk management obligations for providers of critical infrastructures at the organization level. The derivative duty of the national government includes identifying providers of critical infrastructures (by November 2018) and improving their cybersecurity capabilities. This is, of course, a very complex endeavor, as the basis are the organizations doing business in the country, and their internal and external circumstances, interdependencies and not at least IS are heterogeneous. Breaking it down to the organizational level, as requested by the NIS Directive [5] means requesting providers of critical infrastructures to measure their cybersecurity status based on specific criteria. At the most detailed level, this means measuring activities' performance in absolute (e.g., number of employees entrusted with security activities), relational (e.g., number of attacks per device) or time-related (e.g., money spent on security issues per year) indicators, be they monetarized or not. They have to be aggregated and reported to the according governmental or non-governmental point to allow for a further assessment of the nation's current cybersecurity status.

3 Methodology

As the goal of this study is to design and test a framework to allow organizations considered as critical infrastructure providers to assess their cybersecurity status, a Design Science Research (DSR) approach was an appropriate choice [6, 53]. The so-developed framework can be considered an artifact based on design as the research maxim, being relevant, as it is designed to solve real-world problems and rigorous, as it is rooted in the existing knowledge base [6, 53]. This requires iterative circles of design and evaluation regarding validity, utility, quality and efficacy [53]. In our problem-centered approach, we adopted the well-established six-step DSR process proposed by Peffers et al. [7]. The six steps include problem identification and motivation (step 1), definition of objectives for a solution (step 2), design and development (step 3), demonstration (step 4), evaluation (step 5) and communication (step 6) [7]. The research process involved different sources and methods, developing two different versions of the framework, both through several iterations within each sub-process. However, for the sake of clarity, we describe the first iteration (for developing framework V1) and second iteration (for developing framework V2) in a linear way. Iteration 1 mainly covers the first four steps in the process and involves a structured literature review of academic sources, resulting in more than 50 academic sources related to the topic. Next, we analyzed documents from non-academic sources (standards, guidelines, regulations). This rich knowledge set was the foundation for a workshop with ten participants from different fields (i.e., academia (3), private research institution (4), representatives of the ministry (1), security experts from business (2)), with the aim to develop the first version of the framework. In the workshop, we used the term impact area, which is defined for this study as the interrelationship between metrics and controls for specific cybersecurity issues. In addition, the consequences of impact areas for the organization or society are at least on medium level. Next, we identified three dimensions – (A) hardware and software supplier or manufacturer, (B) provider of critical infrastructure, (C) government – reflecting the context or to be more precise, who can influence the context or is most directly influenced by it. For example, the impact area 'Cyberwarfare' is related mainly to the government. Overall, 40 different impact areas were defined in this first iteration. However, in the workshop, the experts came to the conclusion that the framework should focus on impact areas influencing dimension B - the critical infrastructure provider - directly. Based on the result of the workshop, iteration 2 required going back to the literature and reflecting our findings. In parallel, we started the process of mapping and further defining the impact areas. We split up the impact areas into four groups and assigned each of it to two team members of the funded project. After four weeks, we discussed the results and designed a refined draft of the impact areas regarding definitions and indicators. Next, we conducted two focus groups with five to six experts. In the first focus group, we aimed at selecting impact areas with medium to high consequences, leading to 15 impact areas and assigned according indicators from academic and non-academic literature to it. In the second focus group, we demonstrated the 15 impact areas and tested it regarding utility, reliability, validity and efficacy. Although this testing is normally related to evaluation [53], we decided to integrate it into the demonstration step, but to retest it during the evaluation. Results from the focus groups were used to further shape the framework. None of the impact areas had to be excluded, but definitions and indicators were adopted. Another result from the focus groups was a discussion about who is applying the framework, as not all indicators may be assessed correctly on all levels of people involved. Therefore, the following roles were designed: Chief Executive Officer (CEO), Chief Information Security Officer (CISO), IT technician and auditor. In accordance with role descriptions, indicator sets were assigned to the impact areas per role. For example, business-related indicators such as the assessment of monetary aspects of cybersecurity issues are assigned to the roles of CEO, cybersecurity management indicators are assigned to CISO whereas indicators covering technical issues such as downtime of a system to the role of the IT security expert or the technician. The auditor role has been assigned more or less with the same indicators as the CISO, but from an external perspective. As the final step in this iteration, we invited experts from academia and business to apply the second version of the framework, observed them and conducted a post-hoc interview based on an interview guideline. We were aiming at balancing experts from academia and business per role, resulting in nine experts (Table 1). First, the participants received a short introduction including a declaration of confidentiality and the information that they will be observed. They were asked to express verbally what comes to their mind while applying the framework. This so-called think-aloud method provides more information compared to standard observations [54]. Verbally expressed thoughts as well as the whole process were documented by the observer in an observation protocol. After this, a post-hoc interview based on a rough interview guideline was conducted to further evaluate utility, reliability, validity and efficacy of the framework with according questions, such as comprehensibility, completeness, balance to name just some. Some minor changes evolved from this step (e.g., shorten long sentences), but the framework in general had not to be changed. The so-evaluated framework has already been communicated to various stakeholders as the national government, security experts and stakeholders in general.

Table 1. Participants in the evaluation step (5) in the DSR process [7]

Role	Sex	Age	From	Expertise in years
Auditor	Male	20+	Academia	2 years **
Auditor	Female	40+	Business	5 years
Technician	Male	30+	Business	7 years
Technician	Male	30+	Business	7 years
Technician	Male	50+	Academia	15 years
CEO	Male	30+	Academia	3 years *
CEO	Female	30+	Business	2 years
CISO	Male	30+	Academia	7 years
CISO	Male	40+	Business	12 years

* Interview via skype, ** self-reported

4 Results

As one key result of the above described DSR process, the designed and tested framework consists of 15 identified impact areas with potentially medium to severe consequences for critical infrastructure providers (see Table 2 with definitions). For an effective application of the framework and to strengthen its reliability, a common understanding of these impact areas among the stakeholders and security experts in the respective critical infrastructure provider is required. The assessment regarding organizations' cybersecurity status relies on indicators able to reflect an impact area (IA). In the framework, we differentiate between metrics and controls. Metrics are linked to threats and vulnerabilities, thus often defined by a lack of or something missing. Furthermore, it is something that can be measured (quantitatively or qualitatively) by comparing it to a reference point [55]. For example, in impact area 1 'Negligent Use' the slow or non-acceptance of cybersecurity policies by employees [56, 57] is such a metric related to a reference point in time, expressed in a rather qualitative, descriptive way (e.g., immediately, fast, medium-fast, slow, no acceptance). This metric indicates that such behavior makes the company vulnerable. A set of metrics, related to an impact area, can be used to assess the current threat and vulnerability status regarding this area. By contrast, controls are safeguards or countermeasures [58], which should be in place to mitigate risks in each impact area and can also be assessed to judge the preparedness of organizations. Controls are related to risk management covering different types of measures such as policies [58]. To give an example, establishing a process to revoke access rights when the status of an employee requiring access to a system has changed [59, 60] is a control related to impact area 1, as it fights negligent use. We consulted leading industry practice frameworks to support the initial selection of metrics and controls. However, we also added other sources, e.g. from academic literature, where appropriate. Interestingly, some impact areas are completely covered by one or two frameworks, (e.g. IA 3 fully covered by the BSI IT baseline protection framework [36]). The most prominent frameworks are the ISO 2700x family [35, 61, 62], the BSI IT baseline protection [36] and the NIST frameworks [32]. Particularly interesting is IA 11 as it is informed solely by academic literature. Table 2 gives examples of according metrics and controls, and their main sources. In our analysis, we used far more sources, however, due to page restrictions we just provide the most relevant ones. As already described, we processed metrics and control in conjunction with the identified roles (CEO, CISO, Technician, Auditor). The number of indicators (metrics, controls) assigned to impact areas and roles varies, e.g. the CEO, CISO and technician roles were assigned to 5, 11 and again 11 controls for IA 13, respectively. The CISO received the main load with 70 metrics and 97 controls.

5 Discussion

The aim of this study was to develop and test a comprehensive framework that allows critical infrastructure providers to evaluate and report their cybersecurity status in a way that allows governmental agencies to further process results to provide a nationwide assessment. The focus was on identifying the main risk areas and relate these with most common threats and vulnerabilities as well as capturing levels of organizational preparedness. Relying on a DSR approach, we based our framework on academic and non-academic sources (standards, guidelines, regulations), conducted workshops and consulted professionals through an iterative approach, which resulted in a holistic set of 15 risk areas (termed impact areas) with related metrics and controls. As intended, the framework can be used by organizations to assess and monitor their cybersecurity status, and by governments to build a ‘landscape’ of the current cybersecurity situation based on aggregating these organizational applications. It would also allow organizations to cooperate and create benchmarks of their individual performance as compared to other market operators. Thus, our framework serves as an innovative generic design for such evaluations, which is also seen as a pre-condition for DSR studies. The framework was also well-tested and documented thoroughly to allow for such an intended application in the given cybersecurity domain. Our results indicate that the final framework design is sufficiently stable in terms of utility, reliability, validity and efficacy. We, thus, contribute to research and practice, especially to national legislators in terms of obtaining and compiling the relevant data to hold critical infrastructure providers to account for their performance in the context of cybersecurity.

Table 2. Definition of impact areas - * refers to parts not or only partly covered by NIS/NIST

Impact Area (IA)/Definition	Metrics (M)/Controls (C)
IA 1: Negligent use: Lacking or inadequate diligence when using IS (examples: insecure passwords, opening spam emails)	M: the slow or non-acceptance of cybersecurity policies by employees * [36, 57]/C: establishing a process to revoke access rights when employees' status has changed [32, 36, 57, 59–61]
IA 2: Lack of prioritization and focus regarding cybersecurity activities: Lacking awareness (knowledge) of responsible actors regarding what has to be protected or how high the probability of certain threats is as well as ranking risks by their severity, hindering the organization to prioritize cybersecurity activities in a reasonable way for assigning resources and capabilities appropriately	M: a well-defined cybersecurity strategy is missing [32, 35, 61]/C: resources to develop a cybersecurity strategy exist [32, 35, 61, 62]
IA 3: Lacking general cybersecurity awareness: A general lack of awareness and knowledge regarding threats and attack vectors. In addition, the knowledge regarding appropriate and effective handling of such challenges is missing	M: no cybersecurity training specifically designed for the needs of the target group * [36]/C: cybersecurity trainings, specifically designed for the target groups, are conducted on a regular basis * [36]
IA 4: Insufficient awareness and appreciation regarding external cybersecurity situation: Knowledge, information or technical resources, processes and capabilities for developing a clear appreciation regarding the external cybersecurity situation is missing. This hinders the organization from reproducing and assessing the external situation	M: no structured analysis of incidents or attacks, affecting the organization or other organizations in the same industry [32, 35, 61, 62]/C: a defined process for the exchange of knowledge and experience with other experts or computer emergency response teams (CERTs) exists [32, 35, 61]
IA 5: Missing or insufficient Business Continuity Management (BCM): The insufficient preparation to handle possible damaging events, as the goal of BCM of an organization is to be back to normal business conduct as fast as possible (also often referred to the term disaster recovery)	M: defined responsibilities and list of involved parties for business continuity management processes are missing [36] */C: well-defined business continuity management processes and measures exist [32, 63]

(*continued*)

Table 2. (*continued*)

Impact Area (IA)/Definition	Metrics (M)/Controls (C)
IA 6: Insufficient attack recognition: The lack of capabilities to recognize in time attempt or successful malicious activates (i.e., cyberattacks) against the organization to be able to react appropriately with the according countermeasures (often subsumed under the term incident response)	M: last year attempted attacks have been recognized very late [36] */C: network traffic is continuously monitored using a software [36, 61] *
IA 7: Legacy systems: IS, which exist due to historical reasons although they are outdated, deprecated and not further supported by the manufacturer (vulnerable against new threats, as security updates by the manufacturer are not provided)	M: critical business processes depend on legacy systems [35, 61, 64] */C: a list of all legacy systems (incl. possible threats) exists [35, 61, 62, 64]
IA 8: Natural catastrophes: Massive natural catastrophes such as floods, earthquakes or fires threaten the infrastructure of IS	M: no emergency plan in case the infrastructure (in particular the data center) is not available due to a natural catastrophe [57, 65, 66] */C: concepts for backup and restore are constantly adopted in the business impact analysis considering impacts of natural catastrophes on IS [57, 65, 66] *
IA 9: Changes in the ownership structure: Changes in the ownership structure may push cybersecurity activities in the background leading to a decrease of investments and unclear responsibilities	M: changes in the ownership structure may hinder the continuation of cybersecurity processes [67–69]/C: the systems have been prioritized to allow appropriate continuity in case of changes in the ownership structure [67–69]
IA 10: Social engineering: Target towards exploiting interpersonal relationships to evoke a specific behavior, in particular, insecure activities to undermine existing cybersecurity policies and precautionary measures	M: employees are not familiar with the common social engineering techniques and attack vectors * [36]/C: technical measure to prevent social engineering attacks established * [36]
IA 11: Misuse of digital identities: Misusing digital identities (i.e., user accounts) facilitate unauthorized access to IS and malicious activities by using the identity of the betrayed user	M: no processes established to force secure passwords [40, 70] */C: least privileges principle established * [36, 40, 61, 70]
IA 12: Unavailability of systems: Distributed denial of service (DDoS) attacks make service unavailable to regular users or reduce their availability	M: no technologies in place to automatically fight DDoS attacks * [36]/ C: sufficient resources are provided to detect, fight and overcome DDoS attacks * [36, 61]

(*continued*)

Table 2. (*continued*)

Impact Area (IA)/Definition	Metrics (M)/Controls (C)
IA 13: Data theft or data manipulation: Data theft leads to loss of confidentiality whereas data manipulation degrades the integrity of data, hence both compromise two main goals of cybersecurity	M: there were data leaks in the last year [35, 61, 64]/C: there is an insurance covering possible risks evolving from data theft and data manipulation [35, 61, 62, 71]
IA 14: Cyber espionage: Politically or ideologically motivated attacks, technically very mature, aim at eavesdrop or wiretap data with high strategical relevance (e.g., business secrets) to gain strategic advantage	M: there have been watering hole attacks with the goal to steal valuable information in the last year [35, 61] */C: there is a strategy to fight cyber espionage accompanied by appropriate measures [32, 35, 61, 62, 64]
IA 15: Cybercrime: Illicit activities conducted via or on information technology and networks. IS foster as an instrument to conduct illegal activities and increase their distribution as well as elicit exponential material or non-material damage	M: there had been incidents relating into ransomware infection last year [61] */C: trainings on a regular base with all employees to increase awareness regarding cybersecurity issues * [35, 61, 62, 71]

Regarding research, the framework adds to the existing literature by providing a compilation of various sources of knowledge, initially informed by a structured literature review. Although we found overlapping contents between well-known frameworks such as NIST and the German BSI IT baseline, we could identify some relevant aspects that were only covered in the academic body of knowledge. Obviously, the impact areas cover technological and social (or individual) issues, yet social issues seem to dominate over pure technical issues. In almost all impact areas, metrics and controls related to social issues can be found. Especially, metrics regarding the lack of training (IA 3, IA 10), awareness (IA 2, IA 3, IA 15) and knowledge (IA 2, IA 3) are important. On the other hand, controls addressing the individual level (training, awareness, knowledge) characterize many impact areas (IA 2 - IA 5, IA 10, IA 11, IA 15). The framework, thus, is consistent with the notion that the human being is becoming the focus of holistic cybersecurity approaches [72], is equally important, in particular the time needed to comply. This has already been discussed in research and considers factors influencing the adoption process such as clear language, up-to-date policies and access to the documents [57]. Regarding the impact areas, we were surprised to find that some of them were not reflected in the well-known practice frameworks but discussed in the literature, in particular natural catastrophes (IA 8) and change in the ownership structure (IA 9). Both have been suggested by prior work [57, 65–68] with a clear focus on the negative effects they might have on the providers of critical infrastructures. Natural catastrophes threaten the facilities and infrastructure of organizations; thus, they should be a vital part of cybersecurity activities to protect IS.

Regarding contributions to practice, we seek to emphasize two key results. Firstly, the well-established standards used in practice do not cover all our identified impact areas completely. As already discussed above, natural catastrophes and changes in ownership structure are two under-documented examples, which all consulted experts from business and the officials of the national government classified as being especially important although not directly cyber-related. Additionally, other impact areas were mainly covered by metrics and controls from academic literature, for example IA 1 and IA 11. Our framework, thus, integrates knowledge from academic research to help to solve our field problem. Secondly, by assessing the number of metrics and controls and putting them into relation to roles, which strengthens responsibility, it became clear that the CISO occupies a particularly important position in this context. This role which combines managerial and technical tasks contributes to the application of the framework more than the technician. The high number of controls (97) assigned to the CISO reflects the importance of this role for the successful implementation and execution of cybersecurity controls. Thus, the CISO can be seen as mainly responsible for the cybersecurity preparedness of an organization.

Finally, in terms of legislation and policymaking, the framework may serve as a blueprint or starting point for governing cybersecurity assessments across the critical infrastructure sector. It suggests the key impact areas and their assessment mechanisms (metrics and controls) to strengthen cybersecurity and its awareness in a country. While the fifteen impact areas seem to define an adequate scope for developing a landscape of the cybersecurity situation among critical infrastructure providers, they are also generic enough to be of value to other organizations.

6 Conclusion, Limitations and Further Research

From the perspective of design science research (DSR), we designed and tested an innovative and well-documented framework consisting of impact areas and their associated metrics and controls, which can be applied by different types of organizations (and operators of critical infrastructures in particular) to assess their cybersecurity situation. Moreover, it can be used as a guideline by governmental institutions to generate national oversight and allow for comparison of different industries' level of cybersecurity. We thereby provide a design science research proposition covering a field problem (prevention of cybercrime and cyberattacks), a design artifact (the developed framework), expected outcomes (assessed and controlled cybersecurity and risk management), and the material and social mechanisms (implementation of metrics and controls covering social and technical issues, including roles and responsibilities) providing these outcomes in our domain of study.

We developed and tested an artifact to address the need of protection of IS that are threatened by attacks from cyberspace, which provides a generic answer on how to accomplish the comprehensive assessment and ongoing monitoring of cybersecurity and related risk management. The contribution of a generic design can be considered as a key requirement of DSR, which in our case was also a mandatory research condition for this study. We based the development and testing of the framework on the six-step DSR process proposed by Peffers et al. [7]. In particular, we used the relevant bodies of literature and standards provided by academia and practice to provide the foundation of the framework, which we amended and corroborated through fieldwork including two main developments and testing iterations. We thus produced a saturated body of evidence supporting the framework. The included metrics and controls shed insights not only on the material (technical) but also on social mechanisms needed to produce the assessment outcomes. Our work is therefore highly relevant in practical and academic terms. It should be stated that our empirical data is limited to one central European country. Although we do not see any deviating cybersecurity requirements as compared to any other developed country, additional empirical insights at a larger scale might be insightful. We are aware that assessing metrics and controls in binary format (yes or no) hinders a more fine-grained assessment. However, we deliberately refrained from a more sophisticated assessment to increase usability. In terms of future research, it would be interesting investigating the role of company characteristics such as size or age in the context of metrics and controls. We would like to note that our domain of study would require more work which targets the daunting process of knowledge accumulation across perspectives and rests on the pair of shoulders incorporating both, academic research and industry practice.

Acknowledgements. This study was funded by the KIRAS Security Program of the National Austrian Research Promotion Agency (FFG) as part of the project CRISCROSS (No. 10652570).

References

1. Krumay, B., Bernroider, E.W.N., Walser, R.: Evaluation of cybersecurity management controls and metrics of critical infrastructures: a literature review considering the NIST cybersecurity framework. In: Gruschka, N. (ed.) NordSec 2018. LNCS, vol. 11252, pp. 369–384. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-03638-6_23
2. European Political Strategy Centre: Building an Effective European Cyber Shield. p. 16 (2017)
3. The Whitehouse: International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World. The President of the United States Washington, DC (2011)
4. Hall, A.T., Bowen, M.G., Ferris, G.R., Royle, M.T., Fitzgibbons, D.E.: The accountability lens: a new way to view management issues. Bus. Horiz. **50**, 405–413 (2007)
5. European Commission: The Directive on Security of Network and Information Systems (NIS Directive). In: Union, O.J.o.t.E. (ed.), vol. L194, pp. 1–30 (2018)
6. Hevner, A.R.: A three cycle view of design science research. Scand. J. Inf. Syst. **19**, 4 (2007)
7. Peffers, K., Rothenberger, M., Tuunanen, T., Vaezi, R.: Design science research evaluation. In: Peffers, K., Rothenberger, M., Kuechler, B. (eds.) DESRIST 2012. LNCS, vol. 7286, pp. 398–410. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29863-9_29
8. Anderson, R., et al.: Measuring the cost of cybercrime. In: Böhme, R. (ed.) The Economics of Information Security and Privacy, pp. 265–300. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39498-0_12
9. Pfleeger, S.L., Cunningham, R.K.: Why measuring security is hard. IEEE Secur. Priv. **8**, 46–54 (2010)
10. Kraemer-Mbula, E., Tang, P., Rush, H.: The cybercrime ecosystem: online innovation in the shadows? Technol. Forecast. Soc. Chang. **80**, 541–555 (2013)
11. Weber, R.H.: Internet of Things - new security and privacy challenges. Comput. Law Secur. Rev. **26**, 23–30 (2010)
12. Khurana, H., Hadley, M., Lu, N., Frincke, D.A.: Smart-grid security issues. IEEE Secur. Priv. **8**, 81–85 (2010)

13. Kandukuri, B.R., Paturi, R.V., Rakshit, A.: Cloud security issues. In: 2009 IEEE International Conference on Services Computing, pp. 517–520. IEEE (2009)
14. Lewis, J.A.: Assessing the risks of cyber terrorism, cyber war and other cyber threats. Center for Strategic & International Studies Washington, DC (2002)
15. European Commission: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. In: European Commission (ed.) (2013)
16. Chohan, U.W.: The problems of cryptocurrency thefts and exchange shutdowns. Available at SSRN 3131702 (2018)
17. Lau, F., Rubin, S.H., Smith, M.H., Trajkovic, L.: Distributed denial of service attacks. In: 2000 IEEE International Conference on Systems, Man and Cybernetics, pp. 2275–2280. IEEE (2000)
18. Cherdantseva, Y., et al.: A review of cyber security risk assessment methods for SCADA systems. Comput. Secur. **56**, 1–27 (2016)
19. Knowles, W., Prince, D., Hutchison, D., Disso, J.F.P., Jones, K.: A survey of cyber security management in industrial control systems. Int. J. Crit. Infrastruct. Prot. **9**, 52–80 (2015)
20. Humayed, A., Lin, J., Li, F., Luo, B.: Cyber-physical systems security - a survey. IEEE Internet Things J. **4**, 1802–1831 (2017)
21. Cybercrime Magazine. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/. Accessed 15 July 2019
22. Hathaway, O.A., et al.: The law of cyber-attack. Calif. Law Rev. **100**, 817–886 (2012)
23. ISACA: The Risk IT Framework. ISACA (2009)
24. Rostami, M., Koushanfar, F., Karri, R.: A primer on hardware security: models, methods, and metrics. Proc. IEEE **102**, 1283–1295 (2014)
25. Bishop, M.: What is computer security? IEEE Secur. Priv. **1**, 67–69 (2003)
26. Jagatic, T.N., Johnson, N.A., Jakobsson, M., Menczer, F.: Social phishing. Commun. ACM **50**, 94–100 (2007)
27. Krombholz, K., Hobel, H., Huber, M., Weippl, E.: Advanced social engineering attacks. J. Inform. Secur. Appl. **22**, 113–122 (2015)
28. Bauer, S., Bernroider, E.W.: From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization. ACM SIGMIS Database: DATABASE Adv. Inform. Syst. **48**, 44–68 (2017)
29. Tadda, G.P.: Measuring performance of cyber situation awareness systems. Air Force Research Laboratory (2008)
30. von Solms, R., van Niekerk, J.: From information security to cyber security. Comput. Secur. **38**, 97–102 (2013)
31. International Telecommunications Union: Series X: Data networks, Open System Communcations and Security - Telecommunication Security, Overview of Cybersecurity. (2008)
32. NIST CSF National Institute of Standards and Technology: Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. In: Technology; N.N.I.o.S.a. (ed.) (2018)
33. Simmons, C., Ellis, C., Shiva, S., Dasgupta, D., Wu, Q.: AVOIDIT: a cyber attack taxonomy. In: 9th Annual Symposium on Information Assurance (ASIA 2014), pp. 2–12. (2014)
34. Samonas, S., Coss, D.: The CIA strikes back: redefining confidentiality, integrity and availability in security. J. Inform. Syst. Secur. **10**, 21–45 (2014)
35. International Organization for Standardization: ISO/IEC27001:2013. Information technology – Security Techniques – Information Security Management Systems – Requirements. ISO, International Organization for Standardization (2013)
36. Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Katalog. In: BSI, Bundesamt für Sicherheit in der Informationstechnik (ed.) 15. Ergänzungslieferung. BSI, Bundesamt für Sicherheit in der Informationstechnik (2016)
37. Furnell, S.M., Gennatou, M., Haskell-Dowland, P.: A prototype tool for information security awareness and training. Logist. Inf. Manag. **15**, 352–357 (2002)

38. International Organization for Standardization: ISO 31000 - Risk management. International Standardization Organization (2018)
39. Azuwa, M., Ahmad, R., Sahib, S., Shamsuddin, S.: Technical security metrics model in compliance with ISO/IEC 27001 standard. Int. J. Cyber-Secur. Digit. Forensics (IJCSDF) **1**, 280–288 (2012)
40. Jouini, M., Rabai, L.B.A., Aissa, A.B.: Classification of security threats in information systems. Proc. Comput. Sci. **32**, 489–496 (2014)
41. Stoneburner, G., Goguen, A., Feringa, A.: Risk management guide for information technology systems recommendations of the national institute of standards and technology NIST special publication 800-30 In: Computer Security Division (ed.) National Institute of Standards and Technology, Washington (2002)
42. ASME Innovative Technologies Institute: All-hazards Risk and Resilience: Prioritizing Critical Infrastructures Using the RAMCAP Plus Approach. ASME (2009)
43. Gordon, L.A., Loeb, M.P., Sohail, T.: A framework for using insurance for cyber-risk management. Commun. ACM **46**, 81–85 (2003)
44. Bojanc, R., Jerman-Blažič, B.: An economic modelling approach to information security risk management. Int. J. Inf. Manage. **28**, 413–422 (2008)
45. Nagurney, A., Shukla, S.: Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability. Eur. J. Oper. Res. **260**, 588–600 (2017)
46. Electricity Information Sharing and Analysis Center (E-ISAC): Analysis of the cyber attack on the Ukrainian power grid (2016)
47. O'Dowd, A.: Major global cyber-attack hits NHS and delays treatment. BMJ: Br. Med. J. (Online) **357** (2017)
48. Cerrudo, C.: An emerging US (and world) threat: cities wide open to cyber attacks. Securing Smart Cities, vol. 17, pp. 137–151. IOActive (2015)
49. Sridhar, S., Hahn, A., Govindarasu, M.: Framework for improving critical infrastructure cybersecurity, Version 1.1. vol. 100, pp. 210–224, Gaithersburg, MD (2018)
50. Alcaraz, C., Zeadally, S.: Critical infrastructure protection: requirements and challenges for the 21st century. Int. J. Crit. Infrastruct. Prot. **8**, 53–66 (2015)
51. Zio, E., Kroeger, W.: Vulnerability assessment of critical infrastructures. IEEE Reliability Society (2009)
52. Dimensional Research: Trends in Security Framework Adoption. A Survey of IT and Security Professionals (2016)
53. Gregor, S., Hevner, A.R.: Positioning and presenting design science research for maximum impact. MIS Q. **37**, 337–355 (2013)
54. Jääskeläinen, R.: Think-aloud protocol. In: Gambier, Y., van Doorslaer, L. (eds.) Handbook of Translation Studies, vol. 1, pp. 371–374. John Benjamins Publishing Company, Amsterdam/Philadelphia (2010)
55. Melnyk, S.A., Stewart, D.M., Swink, M.: Metrics and performance measurement in operations management: dealing with the metrics maze. J. Oper. Manag. **22**, 209–218 (2004)
56. Zammani, M., Razali, R.: An empirical study of information security management success factors. Int. J. Adv. Sci. Eng. Inform. Technol. **6**, 904–913 (2016)
57. Bernik, I., Prislan, K.: Measuring information security performance with 10 by 10 model for holistic state evaluation. PLoS ONE **11**, 1–33 (2016)
58. ISACA. https://www.isaca.org/Pages/Glossary.aspx. Accessed 01 Apr 2018
59. Andreasson, K.J.: Cybersecurity: Public Sector Threats and Responses. CRC Press, Boca Raton (2011)
60. European Union Agency for Network and Information Security (ENISA): Technical Guideline for Minimum Security Measures, Guidance on the Security Measures in Article 13a. European Union Agency for Network and Information Security, Brussels (2014)

61. International Organization for Standardization: ISO/IEC 27002:2005. Information Technology - Security Techniques - Code of Practice for Information Security Management, vol. 27002:2005. ISO, ISO, International Organization for Standardization (2005)
62. International Organization for Standardization: ISO/IEC 27005:2011 Information technology - Security techniques - Information Security Risk Management. ISO, International Organization for Standardization (2011)
63. Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-4 - Notfallmanagement. In: BSI, B.f.S.i.d.I. (ed.) BSI-Standard 100-4 - Notfallmanagement, (2008)
64. CIS CSC Center for Internet Security: Center for Internet Security Critical Security Controls for Effective Cyber Defense. Center for Internet Security (2015)
65. Baker, G.H.: A vulnerability assessment methodology for critical infrastructure sites. In: DHS Symposium: R and D Partnerships in Homeland Security (2005)
66. Stapelberg, R.F.: Infrastructure systems interdependencies and risk informed decision making (RIDM): impact scenario analysis of infrastructure risks induced by natural, technological and intentional hazards. J. Syst. Cybern. Inform. **6**, 21–27 (2008)
67. Lohrke, F.T., Frownfelter-Lohrke, C., Ketchen, D.J., Jr.: The role of information technology systems in the performance of mergers and acquisitions. Bus. Horiz. **59**, 7–12 (2016)
68. Wijnhoven, F., Spil, T., Stegwee, R., Fa, R.T.A.: Post-merger IT integration strategies: an IT alignment perspective. J. Strategic Inform. Syst. **15**, 5–28 (2006)
69. Robbins, S.S., Stylianou, A.C.: Post-merger systems integration: the impact on IS capabilities. Inform. Manag. **36**, 205–212 (1999)
70. Langweg, H.: Framework for malware resistance metrics. In: Proceedings of the 2nd ACM workshop on Quality of protection, pp. 39–44. ACM (2006)
71. OECD: OECD Risk Checklist. Risk checklist. OECD (2015)
72. Aurigemma, S., Panko, R.: A composite framework for behavioral compliance with information security policies. In: 45th Hawaii International Conference on System Sciences, pp. 3248–3257 (2012)