






# Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework

Barbara Krumay<sup>1</sup>(✉) , Edward W. N. Bernroider<sup>2</sup> ,  
and Roman Walser<sup>2</sup> 

<sup>1</sup> Johannes Kepler University Linz, Linz, Austria  
barbara.krumay@jku.at

<sup>2</sup> WU Vienna University of Economics and Business, Vienna, Austria  
{edward.bernroider, roman.walser}@wu.ac.at

**Abstract.** In recent years, cybersecurity management has gained considerable attention due to a rising number and also increasing severity of cyberattacks in particular targeted at critical infrastructures of countries. Especially rapid digitization holds many vulnerabilities that can be easily exploited if not managed appropriately. Consequently, the European Union (EU) has enacted its first directive on cybersecurity. It is based on the Cybersecurity Framework by the US National Institute of Standards and Technology (NIST) and requires critical infrastructure organizations to regularly monitor and report their cybersecurity efforts. We investigated whether the academic body of knowledge in the area of cybersecurity metrics and controls has covered the constituent NIST functions, and also whether NIST shows any noticeable gaps in relation to literature. Our analysis revealed interesting results in both directions, pointing to imbalances in the academic discourse and underrepresented areas in the NIST framework. In terms of the former, we argue that future research should engage more into detecting, responding and recovering from incidents. Regarding the latter, NIST could also benefit from extending into a number of identified topic areas, for example, natural disasters, monetary aspects, and organizational climate.

**Keywords:** Cybersecurity metrics · Cybersecurity controls  
Critical infrastructures · Literature review

## 1 Introduction

Disruptions of the power supply happen occasionally and are most often caused by *force majeure* such as heavy storms. In December 2015, approximately 230,000 people in Ukraine were left without power for up to six hours. Remarkably, this outage was not caused by heavy weather but due to the first successful cyberattack against a nation's power grid [1]. Not only energy suppliers, but also organizations in many other industries are confronted with an increasing number of cyberattacks: financial

services, health care or IT service providers – just to name a few. The new digital world with its strong interconnectedness creates new business opportunities, but with its increasing number of attack vectors also bears considerable risk. Until recently, cyberattacks mainly targeted individuals or specific organizations at a micro level. Today, more and more attacks are carried out at the macro level, trying to negatively affect entire critical infrastructures (e.g. communication networks, household appliances).

Consequently, over the last years governments around the globe have been intensifying their efforts to better protect their national cyberspaces. Also, the Parliament of the European Union (EU), one of the world's largest politic economies, in 2016 has adopted a Directive on cybersecurity to be transposed into national laws by the Member States by May 2018 [2]. The new EU NIS Directive will require operators of essential services to continuously monitor their cyberspace, integrate and consider potential risk for own information systems and take appropriate technical and organizational security measures. Thus, organizations throughout the EU will have to find and implement a well-defined set of metrics to successfully monitor and evaluate their current cybersecurity status. Moreover, organizations operating critical infrastructures in the EU will be required to evaluate and report any incidents to the relevant national authority.

As with any statutory change, there is major uncertainty among all involved parties (including legislators of the EU Member States). This uncertainty is also reflected by the fact that as of July 2018, 17 out of 28 Member States were in delay and received a letter of formal notice to fully transpose into national laws the first piece of EU-wide legislation on cybersecurity [3]. Most large organizations already have internal control systems in place, which could serve as a basis for the determination of suitable security metrics. Those internal control systems are mainly based on leading frameworks such as the Cybersecurity Framework by the US National Institute of Standards and Technology (NIST). However, many organizations across the EU might be obliged to implement additional measures to monitor their cyberenvironment for fully complying with new legal regulations. So far, it is unclear whether the current reliance on established frameworks will be sufficient for organizations to adequately monitor and assess their cybersecurity situation. Also, it remains unclear whether existing literature covers all relevant aspects for measuring an organization's cybersecurity.

In this paper we will therefore review literature on controls and metrics for measuring cybersecurity. Our aim is to contrast the results with the contents of the NIST framework to show how well the NIST framework is covered by academic literature. This allows us to pinpoint areas where additional research is needed. Additionally, we aim to illuminate any potential blind spots which might occur when organizations adopt the NIST framework unchallenged for measuring cybersecurity. Moreover, our findings could either confirm or challenge the popular NIST framework and propose some room for necessary extensions. In practice, our work might help operators of critical infrastructure to better measure their cybersecurity status and thus help to comply with the new EU NIS directive [2].

The remainder of this paper is organized as follows. First, we will give some theoretical background and information about the context to ensure a common understanding of the relevant terms and concepts. In a subsequent chapter, we will

explain the methodological approach we followed for conducting our literature review. In chapter four, we will present the results of our literature review and discuss them in chapter five together with contributions and limitations. The last chapter will conclude our work.

## 2 Conceptual Background and Context

Cyberattacks can be 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” [4]. Basically, cyberattacks occur since the existence of information systems. With organizations’ increasing reliance on computer systems, also their dependence on the correct functioning of the adopted technology became greater. The success of whole industries is mainly dependent on the unobstructed operation of organizations’ technical infrastructures. Consequently, organizations make investments to obtain a reasonable level of cybersecurity through software, hardware, education and effective personnel [5].

However, recent studies show that both the number and severity of cyberattacks is dramatically on the rise (e.g., [6, 7]). One explanation is that the opportunities to perform attacks have grown. For example, the recent technological development towards larger and more interconnected infrastructures (often referred to as Internet of Things; in short IoT) make cyberattacks potentially even more harmful than before. An array of devices such as Smart TVs with internet access might be integrated in a botnet to bundle computational power for performing more powerful attacks against a given target system (e.g., DDoS attacks). Also, the growing number of devices and inter-connection led to more attack vectors and vulnerabilities which can be exploited. Because attacks might also be exercised politically motivated, governments have started legal initiatives to increase the level of cybersecurity among all relevant parties.

Usually, a set of controls is implemented to build an internal control system and obtain a reasonable level of cybersecurity. According to the COBIT-Glossary a control is “the means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, technical, management, or legal nature” [8]. In addition, the COBIT website remarks that controls are “also used as a synonym for a safeguard or countermeasure” [8]. Since a single, well-established definition for controls does not exist, for the purpose of this research, we define controls as safeguards or measures on the operational, administrative and strategic levels to manage cybersecurity risks. By contrast, a metric has been defined as “a verifiable measure, stated in either quantitative or qualitative terms and defined with respect to a reference point” [9]. We refer to metrics as possibilities for measuring the quality of cybersecurity management efforts, which allow for comparison with specific cybersecurity goals and evaluations from former periods or across organizations.

### 2.1 Measuring Cybersecurity

Measuring an organization’s cybersecurity status has become an important but challenging task for today’s Chief Information Officers (CIOs) and Chief Information

Security Officers (CISOs). To accurately determine the cybersecurity investment needs, a precise assessment of the current status is indispensable. Various factors make the measurement of security hard: a lack of possibilities to test security requirements, the interconnectedness of systems and exaggerated optimism of the management – just to name a few [10]. One common approach for determining suitable metrics is reliance on a set of metrics from a cybersecurity framework. Key Performance Indicators (KPIs) and/or Key Risk Indicators (KRIs) can be deducted from the risks and controls proposed. To give an example, subcategory PR.DS-7 from the NIST cybersecurity framework (v1.1) states: “The development and testing environment(s) are separate from the production environment” [11]. In the former environments, systems are less reliable, e.g. due to unknown bugs or less strict privileges. Production systems need stable environments to ensure continuous business operations. The degree to which the production environment is separated from development or testing could be determined as one of many metrics to estimate the current level of cybersecurity. Organizations may rely on a mix of frameworks and only adapt the parts perceived as relevant [12].

## 2.2 NIST Cybersecurity Framework

The originators of the NIST define their cybersecurity framework as “a voluntary risk management framework consisting of standards, guidelines, and best practices to manage cybersecurity-related risk” [11]. The first version of the publicly accessible framework was released in 2014 and updated to version 1.1 in April 2018. Although it was originally intended as a framework for operators of critical infrastructures, its contents were also considered by various other businesses over the last years. A cyber exposure company’s survey among more than 300 US IT and security professionals has shown that approximately 70 percent of the survey respondents see the NIST cybersecurity framework as a best practice [13]. It can thus be seen as a *de facto* standard among CISOs, which is widely adopted globally. NIST built their framework based on internal knowledge and contents of the following institutions: Center for Internet Security (CIS) Controls V7, Control Objectives for Information Related Technology (COBIT) V5, International Society of Automation (ISA) standards, International Organization for Standardization (ISO) 27001.

The NIST cybersecurity framework consists of five different so-called functions, which contain an overall number of 23 categories and 108 subcategories. Table 1 provides an overview of the framework’s contents. The originators point out that this framework is not exhaustive but extensible and the order of the elements should not be understood as any prioritization.

**Table 1.** NIST functions (summary based on [11])

Function	Function contents
Identify (ID)	Identification and management of assets (incl. business environment), governance of policies, procedures and processes to inform management of cybersecurity risk, risk assessment, determination of risk appetite, development of a risk management strategy (incl. IT of suppliers)
Protect (PR)	Identity management, logical and physical access protection to assets and network (incl. remote access). Regular review of permissions and authorizations, assurance of authentication (e.g. multi-factor authentication), training of users (awareness, roles, responsibilities), adequate data protection, security policies for protecting information, maintenance and repairs of components, log recording and regular audits
Detect (DE)	Continuous monitoring of systems and assets, detection and impact estimation of anomalous activities and, appropriate communication of detection information, continuous improvement of detection processes
Respond (RS)	Development of incident response plans and trainings based on predefined criteria, clear roles and responsibilities, coordination and information exchange with stakeholders, mitigation of incidents, documentation of lessons learned and updating of response strategies
Recover (RC)	Training and execution of recovery processes and procedures as required, coordination of restoration activities with internal and external parties, management of public relations and reparation of reputation after an incident

### 2.3 EU NIS Directive

Over the last year, governments around the world have started to increasingly recognize the importance of assuring a reasonable level of cybersecurity. This awareness might be the result of recent attacks on operators of critical infrastructures such as the previously mentioned attack on the Ukrainian power grid. It is arguable that the number of (also politically motivated) cyberattacks will further increase.

Consequently, in July 2016, the EU Parliament adopted the Directive on security of network and information systems (Directive (EU) 2016/1148). In short, the directive is often referred to as NIS Directive. In the European Union, it was the first legislation with the aim to boost the overall level of cybersecurity in the EU. The Directive was intended to be transposed into national law in all of the 28 Member States by May 2018. The NIS Directive mainly addresses operators of so-called essential services, whose definition might vary slightly from country to country. Providers of essential services will usually have access to or operate critical infrastructures. A fact sheet, which was published in May 2018 substantiated the industries and infrastructures which are covered by the following essential services [14]:

- Energy (electricity, oil and gas)
- Transport (air, rail, water and road)
- Banking (credit institutions)
- Financial market infrastructures (trading venues, central counterparties)
- Health (healthcare settings)
- Water (drinking water supply and distribution)
- Digital infrastructure (internet exch. points, DNS operators, TLD name registries)

Operators of essential services should be identified by the governments until November 2018. The NIS Directive aims to improve the level of cybersecurity through three different means: (1) increased cooperation at EU-level, (2) improved cybersecurity capabilities at the national level, and (3) risk management and incident reporting obligations for operators of critical infrastructures at the organization level.

Consequently, the national governments of the EU Member States have initiated project with the aim of improving the national cybersecurity capabilities. Asking organizations to objectively assess their cybersecurity status at an individual level is already a challenging task. For instance, employees accountable for the company's information systems might tend to report positively biased information. In addition, the selection of suitable metrics (which are available within the companies) is crucial to get a good estimation. Even more challenging, those individual cybersecurity evaluations must be aggregated and compared to get a picture of the national situation. Although the leading cybersecurity frameworks are proven to a certain degree, there might be some important aspects missing to assess an organization's cybersecurity status. On the other side, also solely relying on scientific papers might neglect some important areas. By conducting a more holistic review of literature on cybersecurity metrics, we aim to illuminate any potential blind spots both in specific framework such as NIST but also in existing literature on measuring cybersecurity.

### 3 Methodological Approach

Based on a systematic literature review, we investigated the body of knowledge and existing results in the area of cybersecurity metrics and controls. In general, we follow the process as described by Levy [15], consisting of input, processing and output. For the input, we first selected - with the help of six experts in the area of cybersecurity and critical infrastructures - search terms related to security in the cyberspace (i.e., cybersecurity, information security, IT security, data security) and related to metrics and controls (i.e., metrics, indicators, controls, measures, risks, management). In the actual search procedure, we applied Boolean search mechanisms (e.g., "metrics" AND "cybersecurity" AND "critical infrastructure" leading to approx. 3,500 results) for combining the search terms.

Although starting with high-level journals and scientific databases is recommended [15, 16], for our study it is important to use a wide variety of sources. Therefore - and to gain a more holistic view - we used Google Scholar as our primary search engine, using its mechanisms for excluding patents and cited sources. The search process (12/2017–02/2018) resulted in more than 9,000 pre-selected articles, excluding double matches, articles in foreign languages and results with dead links. In a next step, we excluded all non-peer-reviewed articles (i.e., journals purely from practice, textbooks, theses) resulting in approximately 7,500 articles. For further investigation, we selected all papers, directly addressing controls or metrics of cybersecurity (respectively IS/IT security) in the context of critical infrastructures as their main focus of research. As a result, we were able to identify 320 peer-reviewed papers fitting the requirements. Finally, we excluded all papers, which address more or less the same controls or metrics (e.g., further developments of existing papers, papers related to the NIST

guideline), resulting in 56 papers. From these papers, we extracted 1,378 units (metrics and controls) for further investigation.

Our level of analysis consists of the NIST guideline’s 23 categories. In case of any doubts, we use the subcategories of the guideline as a reference. For this purpose, we developed seven simple coding principles (see Table 2) for mapping the units extracted from literature to the NIST framework (i.e. to its 23 categories). Rule R1, for example, means that the unit “Sum of critical assets” [17] is a metric (M). Applying rule R2 implies that units (e.g., “% of securized areas”, “% of critical equipment with adequate physical protection”, “% of secured configurations” [17]) are covered by the term “IS security architecture” [17]. Therefore, we excluded the higher-level term “IS security architecture” and used the underlying metrics as units of analysis. Regarding rule R3 and R4, the unit “Sum of critical assets” [17] has been directly mapped to the function ‘Identify’, based on the description of the NIST subcategory “Asset Management (ID. AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy” [11]. According to R5, we marked the unit “Degree of organizational climate satisfaction” [18] as ‘uncovered’. Regarding Rule R6 (and in the same way R7), the unit “Change management - analyses of impacts that technology changes have on existing systems” [18] is directly mapped to “Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information” [11], yet indirectly mapped to other functions such as ‘Identify’.

**Table 2.** Coding principles (pre-set)

R1	Based on the working definition of this paper, units are either controls (C) or metrics (M)
R2	To avoid duplication of meaning, units on different levels (e.g., metrics which are aggregated into one combined metric) from the same source, the highest level is excluded from further investigation (E)
R3	General rule: every non-excluded unit must have one direct mapping (D) and may or may not have one or more indirect (I) mappings to the NIST framework
R4	Every unit is directly (D) mapped to only one function of the NIST guideline (exclusive mapping). Direct mapping means that this unit fits best into this one function (based on categories of NIST)
R5	If a unit does not fit directly into one function, it is marked as ‘uncovered’ (U)
R6	Every unit may be mapped indirectly (I) to other functions of the NIST guideline, if it holds aspects of these functions
R7	Every unit may be mapped indirectly to functions ‘uncovered - indirect’ (UI), if it holds aspects not covered by NIST

Two researchers were trained on the coding procedure. To test intercoder reliability, we used a simple percentage agreement method [19], assessing the agreement between the coders from 0 (no agreement) to 1 (perfect agreement). Both coders were coding the same 50 units and the results were compared. The agreement between the two coders was about 0.91. In addition, we calculated intracoder reliability, also using 50 units for coding, which have been coded by the same coder two times, three days after the first coding round. The intracoder reliability 0.96 and 0.97 for the two coders. The coding itself was done in July 2018 by both coders. After this first round, we cross-checked the NIST functions and categories against the units to make sure that gaps are not resulting from the coding rules. This led to changes in only a minority of the mappings (less than 2%) allowing us to assume that bias from the coding principles and coders is negligible. Units which have been marked as ‘uncovered’ were further analyzed. In this stage we applied coding techniques, which are often applied in Grounded Theory approaches [20]. In particular, we applied a form of open coding and categorizing based on the meaning of the ‘uncovered’ units.

## 4 Results

The results of the literature review are presented in three different ways. First, we describe the sample, i.e. papers in the samples and units of investigation. Next, we show in how far NIST framework functions are represented in the literature. Finally, we present topics which are discussed in the literature but hardly covered by NIST guideline.

### 4.1 Sample Description

As already described above, the sample consisted of 56 articles. The articles in the sample are mainly published in academic journals (38) and conference proceedings (16), only two were book sections from scholarly collections. All articles were published between 2003 and 2017 with no clear peak on any year. Eleven of the articles were published in eight journals with a 5-year impact factor above 3.5, mostly related to the Information System (IS) and Computer Science (CS) community, (i.e. Decision Support Systems [21], Expert Systems with Applications [22, 23], Reliability Engineering & System Safety [24, 25], IEEE Transactions on Smart Grid [26, 27], Information Sciences [28], Information Systems Journal [29], International Journal of Information Management [30]). The highest impact factor in our sample, however, is related to a journal with no clear relationship with IS nor with CS research (Renewable & Sustainability Energy Reviews, IF 9.184, [31]). Thirteen of the papers in our sample were cited more than 100 times; the oldest one in our sample [32] even about 1,000 times (according to Google Scholar).

Regarding the units of analysis, we excluded 325 units based on coding rule R2, resulting in 1,053 units of analysis, 443 of which are metrics and 610 are controls (coding rule R1). Regarding direct mapping, 918 units have been directly mapped to NIST functions [11], leaving 135 which are not directly covered by NIST and additional 122 have aspects, which are not covered by NIST.



## 4.2 Mapped Metrics and Controls

Mapping the units to the NIST functions [11] revealed a rather clear, yet surprising picture. Most of the units, which we were able to map directly, are related to the functions ‘Identify’ (41.94%) and ‘Protect’ (44.88%). Interestingly, these two functions are mainly covered by controls (about 2/3 per function). In comparison, the functions ‘Detect’ (8.06%), ‘Respond’ (4.03%) and ‘Recover’ (1.09%) were hardly covered by the literature (see Table 3). By contrast, these functions are mainly covered by metrics.

**Table 3.** Mapping of metrics and controls to NIST guideline [11]; D = direct mapping; I = indirect mapping

Function/Category	D (%)	I (%)
<i>Identify (ID)</i>	41.94	41.11
Asset management (ID.AM)	10.35	9.91
Business Environment (ID.BE)	5.77	8.03
Governance (ID.GV)	9.69	9.23
Risk Assessment (ID.RA)	13.94	8.21
Risk Management Strategy (ID.RM)	1.09	4.70
Supply Chain Risk Management (ID.SC)	1.09	1.03
<i>Protect (PR)</i>	44.88	31.54
Identity Management and Access Control (PR.AC)	7.52	2.31
Awareness and Training (PR.AT)	6.32	3.59
Data Security (PR.DS)	11.44	5.21
Information Protection Processes and Procedures (PR.IP)	8.50	14.36
Maintenance (PR.MT)	1.42	0.43
Protective Technology (PR.PT)	9.69	5.64
<i>Detect (DE)</i>	8.06	12.05
Anomalies and Events (DE.AE)	0.65	3.33
Security Continuous Monitoring (DE.CM)	3.81	5.30
Detection Processes (DE.DP)	3.59	3.42
<i>Respond (RS)</i>	4.03	11.88
Response Planning (RS.RP)	0.87	3.93
Communications (RS.CO)	0.00	0.77
Analysis (RS.AN)	2.18	3.59
Mitigation (RS.MI)	0.54	2.74
Improvements (RS.IM)	0.44	0.85
<i>Recover (RC)</i>	1.09	3.42
Recovery Planning (RC.RP)	1.09	1.79
Improvements (RC.IM)	0.00	1.03
Communications (RC.CO)	0.00	0.60

When looking at indirectly mapped units, the disproportional research focus softens. While ‘Identify’ (41.11%) and ‘Protect’ (31.54%) remain to be covered by the vast majority of units, the rates related to ‘Detect’ (12.05%), ‘Respond’ (11.88%) and ‘Recover’ (3.42%) increased. Due to multiple mapping, metrics and controls indirectly mapped are hard to compare. However, it can be said, that controls do more often have indirect mappings, whereas 66% of all metrics were mapped within only one function from the NIST guideline, 40% were even mapped directly to one category without any further indirect mapping to other categories.

### 4.3 Uncovered Topic Areas

In our analysis, some units were marked as ‘uncovered’ (257 of which are 159 controls and 98 metrics). We used these units for identifying ‘uncovered topic areas’ by coding and categorizing them based on the underlying meaning or purposes of controls and metrics. A brief overview presenting all uncovered topic areas is shown in Table 4. The table provides metrics (M) and controls (C) (where applicable) which have been assigned to these topic areas. These topic areas do not seem to directly align with the NIST functions.

**Table 4.** Uncovered topic areas with examples (U = Number of Units, M = Number of Metrics, C = Number of Controls)

Topic areas	Representative examples	U	M	C
Organizational climate	M: “Degree of organizational climate satisfaction” [17] C: “Enhance individual/group pride in the organization” [29]	65	13	52
Monetary aspects	M: “Cost of image rebuilt after information security accidents” [33] C: “Security budget segregation” [17]	59	41	18
Executive involvement	M: “Leaderships’ involvement in information security planning” [18] C: “Develop a management team that leads by example” [29]	25	5	20
Ethics	C: “Create an organizational code of ethics” [29]	23	0	23
General management	M: “documents scheduled for that month must be received within five business days of due date” [34] C: “Ensure a right balance between centralization and decentralization” [29]	23	12	11
IT Service Levels	M: “Customer Satisfaction” [33] C: “SLA covers all the aspects of security when there is a third party providing other services” [35]	22	11	11
Cognitive response	C: “Instill a fear of consequences” [29]	18	0	18
Procurement	M: “Testing ICT before acquisition” [18] C: “Procure IT Resources” [36]	14	4	10
Business value	C: “Contribution to the overall business” [32]	10	0	10
Natural disasters	M: “Intensity of the extreme weather event” [37] C: “Fire, voltage and flood protection of buildings and premises” [18]	10	3	7

We will further elaborate on five uncovered topic areas, which are either prevailing the analysis (i.e., organizational climate, monetary aspects, executive involvement, ethics) or highly important in the context of critical infrastructure cybersecurity (i.e., natural disasters). In terms of organizational climate, 65 units (13 metrics, 52 controls) have been assigned which relate to organizational climate in a company, such as motivation and employee satisfaction (e.g. in [29, 32, 38]). Interestingly, aspects of organizational climate, influencing overall cybersecurity are not directly listed in NIST. They could be assumed as underlying ideas in categories where responsibilities and communication are claimed (e.g. in Respond – Communication [11]), yet an immediate mapping was not possible. Related in NIST is ID.AM-5 where ‘personnel’ is addressed as a resource, but not further discussed. Development of skills, e.g., awareness, is addressed in the category “Awareness and Training (PR.AT)” [11], as well as in “PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)” [11].

Regarding monetary aspects, we found 59 units (41 metrics, 18 controls), addressing revenues or costs (see for example [29, 36, 39, 40]). Although in the description of the NIST guideline monetary aspects are discussed in terms of “cybersecurity risks ... can drive up costs and affect revenue” [11], in the NIST functions, costs are hardly covered. The sub-category “ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value” [11] refers to resources in general, but not explicitly to monetary resources.

The picture is similar for executive involvement (25 units: 5 metrics, 20 controls), which is discussed widely in the literature (e.g., [18, 29]), but rarely addressed in the NIST guidelines. We found evidence for executive involvement in two sub-categories (“PR.AT-4: Senior executives understand their roles and responsibilities”, “RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams”) and the category “Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets” [11]. However, the literature discussed these issues in more depth, e.g. “Top management’s engagement” [41], “Top Management: Leadership” [38] or “Management Support (MS): Management involvement” [42].

Interestingly, ethics appears in the literature (23 controls, no metrics), yet is elided by NIST. For example, Bernik and Prislán (2016) address “Ethical, socially responsible and transparent security management” [18], Dhillon and Torkzadeh (2006) discuss “value-based work ethics” [29] as a factor in cybersecurity management and van Eeten and Bauer (2008) name “Ethics” [43] among the controls required in this area.

Finally, we found metrics (3) and controls (7), which relate to threats evolving from natural disasters, such as “Exposure: natural hazards or change impacts that will affect the system” [44] or “Fire, voltage and flood protection of buildings and premises” [18]. Especially in the context of critical infrastructures, we would have expected this topic covered in the NIST guidelines. This topic could be in parts assigned to other functions, such as ‘Asset Management’ or ‘Supply Chain Risk Management’ in the ‘Identify’-function of the NIST guideline. Consequently, we marked these metrics and controls only as ‘indirectly uncovered’.

## 5 Discussion, Contributions and Limitations

Critical infrastructures are the backbones of developed societies. Information systems have become a vital part for managing them, thus, securing information systems directly influences safety of critical infrastructures. Standards and guidelines support providers of critical infrastructures in their cybersecurity management efforts. The NIST cybersecurity framework [11] is most arguably one of the most important risk management framework in this regard. It recently gained in influence since it is used to guide contemporary legislation on cybersecurity [2]. For this reason, we conducted a comprehensive literature review to firstly provide insights on how well the NIST cybersecurity framework (version 1.1., 2018) is covered by academic literature. Based on a content analysis guided by pre-set coding principles, we extracted 1,053 units (metrics and controls) from the found academic articles and matched these against 23 categories (functions) of the NIST guideline. By doing so, we were able to show that academic research most distinctively investigates the NIST functions “identification” and “protection” from cybersecurity threats in terms of investigating metrics (possibility to measure and compare) and also controls (ability to manage). By contrast, “detecting”, “responding to” and “recovering” from cybersecurity incidents are areas that receive relatively scarce attention, especially when it comes to controls. It seems that these dimensions, which are usually important components of a more comprehensive layered or in-depth security strategy, are often overlooked by academic studies. NIST, however, explicitly states that a no function is more important than another and calls for a balance over functions. This balance is certainly not evident in prior academic work. When looking at indirect inclusion, we noted slight reductions of the detected imbalances. It seems that future research should pay more attention to directly investigating how to manage and assess these important areas, which reflect the soundness of cybersecurity management after a breach has happened.

Next, our study indicates ‘blind spots’ in the NIST framework as contributions to practice, in particular to support the tasks of critical infrastructure providers. By describing such ‘blind spots’, we suggest to practice to go beyond mere compliance with the new EU NIS directive, and suggest that organizations pursue a cybersecurity strategy which acknowledges additions to the framework depending on given needs. Our analysis has revealed a number of potential gaps, which we called ‘uncovered topic areas’ of the NIST framework. The detected underrepresentation of organizational climate and social aspects is surprising. Academic literature has long established that in particular social norms and organizational climate affect behavior and are influential in achieving compliance [45]. Most importantly, the monetary aspects of cybersecurity management are hardly covered in NIST, but well mentioned in academic literature (e.g., [29, 36, 39, 40]). Despite the importance of safeguarding against cyberattacks directed at critical infrastructure, the economic consequences for the involved organizations deserve greater attention. It is well accepted that any compliance initiative is costly, and that many organizations struggle to meet time and cost objectives of related control activities and audits, e.g. [46]. Additionally, we highlighted that executive involvement (e.g. as role models), ethical aspects linking into organizational culture and climate, and threats evolving from natural hazards also deserve clearer NIST

placements. Since the latter is also well considered in the wider IS security literature (e.g. [47, 48]), it is surprising that NIST only rather unspecifically lists that response and recovery plans related to disasters should be in place. Our analysis covering a recourse of research concerned with critical infrastructure and natural disasters also establishes the importance of natural hazards, which can be exploited by attackers, and even offer metrics and controls to assure information system security and critical infrastructure safety, e.g. “Probability of failure/inundation due to natural hazard”, [49], “List of hazard initiating events” [50] or “Wind storm occurrence” [51]. It seems that organizations would benefit from not only consulting NIST, but also these and other studies to support cybersecurity management practice in their continuous assessment duties.

In terms of limitations, we need to note the interdisciplinary characteristic of our research topic around metrics and controls, and the ambiguities of these terms, which together make any consolidation initiative more difficult. It is advised that many different research fields need to be consulted. While we accounted for papers in our sample also outside the fields of information systems and computer science, it is likely that we have missed papers using different terms. In our paper, we offered working definitions of controls and metrics, which helped in terms of interpreting our findings. For example, we noted that controls are often covering more than one function and category, whereas the majority of metrics refer to one function or category only. This may owe to the fact that metrics usually have a specific anchor point and measure one particular phenomenon, whereas controls are broader and may cover multiple situations.

## 6 Conclusion

Since the EU NIS directive mandates providers of essential services to improve cybersecurity capabilities guided by risk management and incident reporting obligations, many organizations from the sectors energy, transport, banking, health, water, and digital and financial market infrastructures need to consider the NIST cybersecurity framework in order to assure a reasonable level of cybersecurity. This explicitly includes assessing controls and applying metrics to report their security status and maturity. Our study among the first to match the current version (1.1) of the NIST framework issued in April 2018 and related academic bodies of knowledge to assist in the evaluation of cybersecurity management. In doing so, we showed the coverage of the NIST framework by research in terms of metrics and controls, and suggested areas deserving more attention in future research. Additionally, we also suggested a number of topic areas that seem missing or underrepresented in the NIST framework. Thus, our study offers important insights for both research and practice for evaluating the management of cybersecurity-related risk, which is becoming a new regulatory requirement for providers of critical infrastructures.

**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. European Political Strategy Centre: Building an Effective European Cyber Shield, p. 16 (2017)
2. 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)
3. European Commission: July Infringements Package: Key Decisions. July Infringements Package: Key Decisions, (2018)
4. Hathaway, O.A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., Spiegel, J.: The law of cyber-attack. *Calif. Law Rev.* **100**, 817–886 (2012)
5. Nagurney, A., Shukla, S.: Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability. *European Journal of Operational Research* **260**, 588–600 (2017)
6. Accenture: Cyberthreat Scape Report (2017)
7. EY: Cybersecurity Regained: Preparing to Face Cyber Attacks (2017)
8. ISACA (2018). <https://www.isaca.org/Pages/Glossary.aspx>
9. 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)
10. Pfleeger, S.L., Cunningham, R.K.: Why measuring security is hard. *IEEE Secur. Priv. Mag.* **8**, 46–54 (2010)
11. Sridhar, S., Hahn, A., Govindarasu, M.: Framework for improving critical infrastructure cybersecurity, Version 1.1, Gaithersburg, MD, vol. 100, pp. 210–224 (2018)
12. Nicho, M., Muamaar, S.: Towards a taxonomy of challenges in an integrated IT governance framework implementation. *J. Int. Technol. Inf. Manag.* **25**, 2 (2016)
13. Dimensional Research: Trends in Security Framework Adoption (2016)
14. European Commission: Fact Sheet - Directive on Security of Network and Information Systems, the First EU-wide Legislation on Cybersecurity, vol. 2020, pp. 7–10 (2018)
15. Levy, Y., Ellis, T.J.: A systems approach to conduct an effective literature review in support of information systems research. *Informing Sci.* **9** (2006)
16. Webster, J., Watson, R.T.: Analyzing the past to prepare for the future: writing a literature review. *MIS Quarterly* xiii-xxiii (2002)
17. Torres, J.M., Sarriegi, J.M., Santos, J., Serrano, N.: Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness. In: International Conference on Information Security, pp. 530–545. LNCS, (2006)
18. Bernik, I., Prislán, K.: Measuring information security performance with 10 by 10 model for holistic state evaluation. *PLoS ONE* **11**, 1–33 (2016)
19. Lombard, M., Snyder-Duch, J., Bracken, C.C.: Content analysis in mass communication: Assessment and reporting of intercoder reliability. *Hum. Commun. Res.* **28**, 587–604 (2002)
20. Strauss, A., Corbin, J.M.: Basics of Qualitative Research: Grounded Theory Procedures and Techniques. Sage Publications, Inc. (1990)
21. Chu, A.M., Chau, P.Y.: Development and validation of instruments of information security deviant behavior. *Decis. Support Syst.* **66**, 93–101 (2014)
22. Sohn, M.H., You, T., Lee, S.-L., Lee, H.: Corporate strategies, environmental forces, and performance measures: a weighting decision support system using the k-nearest neighbor technique. *Expert Syst. Appl.* **25**, 279–292 (2003)
23. Asosheh, A., Nalchigar, S., Jamporzmay, M.: Information technology project evaluation: an integrated data envelopment analysis and balanced scorecard approach. *Expert Syst. Appl.* **37**, 5931–5938 (2010)

24. 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)
25. Francis, R., Bekera, B.: A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliab. Eng. Syst. Saf.* **121**, 90–103 (2014)
26. Hahn, A., Govindarasu, M.: Cyber attack exposure evaluation framework for the smart grid. *IEEE Trans. Smart Grid* **2**, 835–843 (2011)
27. Hahn, A., Ashok, A., Sridhar, S., Govindarasu, M.: Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. *IEEE Trans. Smart Grid* **4**, 847–855 (2013)
28. Feng, N., Wang, H.J., Li, M.: A Security risk analysis model for information systems: causal relationships of risk factors and vulnerability propagation analysis. *Inf. Sci.* **256**, 57–73 (2014)
29. Dhillon, G., Torkzadeh, G.: Value-focused assessment of information system security in organizations. *Inf. Syst. J.* **16**, 293–314 (2006)
30. Bojanc, R., Jerman-Blažič, B.: An economic modelling approach to information security risk management. *Int. J. Inf. Manage.* **28**, 413–422 (2008)
31. Arghandeh, R., von Meier, A., Mehrmanesh, L., Mili, L.: On the definition of cyber-physical resilience in power systems. *Renew. Sustain. Energy Rev.* **58**, 1060–1069 (2016)
32. Ittner, C.D., Larcker, D.F., Meyer, M.W.: Subjectivity and the weighting of performance measures: evidence from a balanced scorecard. *Account. Rev.* **78**, 725–758 (2003)
33. Huang, S.-M., Lee, C.-L., Kao, A.-C.: Balancing performance measures for information security management: A balanced scorecard framework. *Ind. Manag. Data Syst.* **106**, 242–255 (2006)
34. Potter, J.G., Hsiung, H.: Service-level agreements: aligning performance and expectations. *IT Prof.* **10**, 41–47 (2008)
35. Abuhussein, A., Bedi, H., Shiva, S.: Evaluating security and privacy in cloud computing services: a stakeholder's perspective. In: *International Conference for Internet Technology And Secured Transactions 2012*, pp. 388–395. IEEE (2012)
36. Sahibudin, S., Sharifi, M., Ayat, M.: Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. In: *Second Asia International Conference on Modeling and Simulation, AICMS*, pp. 749–753 (2008)
37. Jufri, F.H., Kim, J.-S., Jung, J.: Analysis of determinants of the impact and the grid capability to evaluate and improve grid resilience from extreme weather event. *Energies* **10**, 1–7 (2017)
38. Zammani, M., Razali, R.: An empirical study of information security management success factors. *Int. J. Adv. Sci., Eng. Inf. Technol.* **6**, 904–913 (2016)
39. Ben-Aissa, A., Abercrombie, R.K., Sheldon, F.T., Mili, A.: Defining and computing a value based cyber-security measure. *Inf. Syst. E-Bus. Manag.* **10**, 433–453 (2012)
40. Rabai, L.B.A., Jouini, M., Aissa, A.B., Mili, A.: A cybersecurity model in cloud computing environments. *J. King Saud Univ. Comput. Inf. Sci.* **25**, 63–75 (2013)
41. Merete, H.J., Albrechtsen, E., Hovden, J.: Implementation and effectiveness of organizational information security measures. *Inf. Manag. Comput. Secur.* **16**, 377–397 (2008)
42. Flowerday, S.V., Tuyikeze, T.: Information security policy development and implementation: the what, how and who. *Comput. Secur.* **61**, 169–183 (2016)
43. van Eeten, M.J., Bauer, J.M.: *Economics of Malware: Security Cessions, Incentives and Externalities*. OECD Science, Technology and Industry Working Papers 2008, pp. 1–68 (2008)
44. 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)

45. 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. Inf. Syst.* **48**, 44–68 (2017)
46. Fogel, K., El-Khatib, R., Feng, N.C., Torres-Spelliscy, C.: Compliance costs and disclosure requirement mandates: some evidence. *Res. Account. Regul.* **27**, 83–87 (2015)
47. Zimmerman, R., Restrepo, C.E.: The next step: quantifying infrastructure interdependencies to improve security. *Int. J. Crit. Infrastruct.* **2**, 215–230 (2006)
48. Jouini, M., Rabai, L.B.A., Aissa, A.B.: Classification of security threats in information systems. *Procedia Comput. Sci.* **32**, 489–496 (2014)
49. Oh, E.H., Deshmukh, A., Hastak, M.: Vulnerability assessment of critical infrastructure, associated industries, and communities during extreme events. In: *Construction Research Congress 2010: Innovation for Reshaping Construction Practice*, pp. 449–469 (2010)
50. Chen, Y.-R., Chen, S.-J., Hsiung, P.-A., Chou, I.-H.: Unified security and safety risk assessment - a case study on nuclear power plant. In: *2014 International Conference on Trustworthy Systems and their Applications (TSA)*, pp. 22–28. IEEE (2014)
51. Li, G., et al.: Risk analysis for distribution systems in the northeast US under wind storms. *IEEE Trans. Power Syst.* **29**, 889–898 (2014)