Chapter 1

ON THE USE OF INFORMATION SECURITY MANAGEMENT SYSTEMS BY GERMAN ENERGY PROVIDERS

Sebastian Pape*, Goethe University Frankfurt
Christopher Schmitz, Goethe University Frankfurt
Dennis-Kenji Kipker, University of Bremen
Andre Sekulla, University of Siegen

Abstract Along with other requirements, the German critical infrastructure programme required critical infrastructure providers, i.e. energy providers to implement an ISMS. We used the unique opportunity to observe the implementation and surveyed all German energy providers in autumn 2016 and 2018. Our study shows, that most of the energy providers implemented an ISMS between our surveys and reported a perceived increase in information security suggesting that the critical infrastructure programme fulfilled its purpose.

Keywords: information security management system, isms, energy provider, security

1. Introduction

Critical infrastructures are of vital importance to a nation's society and economy because their failure would result in sustained supply shortages causing a significant disruption of public safety and security. In 2016, malicious software in nuclear power plants was reported[1] followed by further reports[2][3], e.g. warnings about hackers attacking German energy providers in 2018.

With the *European Programme for Critical Infrastructure Protection* (EPCIP) and its counterpart, the German critical infrastructure protection programme KRITIS [0] governments aimed to provide the ground for more

*sebastian.pape@m-chair.de

secure critical infrastructures. The new regulation challenged critical infrastructure providers in many ways. Besides general challenges such as understanding the definitions and requirements (cf. [0, p. 150ff]), and challenges from other areas, i.e. coping with the energy transition, energy providers needed to register a contact point, establish processes to report security incidents, implement security requirements following a security catalogue (§11 Abs. 1a respectively 1b EnWG), and establish and certify an information security management system (ISMS). Our investigation focuses on the introduction of an ISMS by German energy providers. For that purpose, we surveyed German energy providers in autumn 2016 when they had just learned about the requirements and in autumn 2018, roughly half a year after they had to provide the certification of their ISMS. The new regulation offers us the chance to have a closer look at a large amount of energy providers introducing an ISMS to get ready for certification at the same time. We intend to investigate how the introduction of the ISMS went and how the energy providers plan to operate it. Since the real security level can not easily be measured within the survey, we are furthermore looking for evidence if the need to establish an ISMS changed the energy providers' view on security.

The remainder of this paper is as follows. Section 2 discusses the legal background of the European and German infrastructure protection programme and discusses related work. Section 3 introduces the methodology of the study and Section 4 presents the results which are discussed in Section 5. Section 6 concludes our work. Both surveys can be found in last section.

2. Background

In this section, we first sketch the legal background in Europe and especially Germany for critical infrastructure providers in the energy sector. We then compare these regulation with the U.S National Infrastructure Protection Plan. We end this section with related work.

2.1 European and German Political Strategies for Critical Infrastructure Protection

At an early stage, the increasing challenges of information technology protection of critical infrastructures were addressed in terms of legal policy both in the European Union and in Germany. First, in 2006 the European Union adopted the "European Programme for Critical Infrastructure Protection" (EPCIP) - also understood as a blueprint for future legislation in this area[4]. The primary aim is to protect critical infrastructures against terrorist threats. The measures proposed in the

EPCIP are based on the principles of the rule of law and the principle of subsidiarity enshrined in the EU, so that the measures planned by the European Commission relate less to national or regional measures and more to those of pan-European significance. Measures taken to protect critical infrastructures must also be proportionate. This means that risk and threat must be in proportion to each other. EPCIP also describes a sector-specific approach to implementing security measures. Critical infrastructures themselves are not yet defined in EPCIP; the document is rather a catalogue of measures and political guidelines for action. The framework which is proposed by EPCIP consists of several measures:

- A common procedure for the identification and designation of European Critical Infrastructures (ECI) by the way of a European Directive

- Critical Infrastructure Protection (CIP) information exchange: establishment of an EPCIP action plan, a CIP Contact Group as strategic coordinating tool, a Critical Infrastructure Warning Network (CIWIN), the foundation and use of CIP expert groups at EU level, as well as an information sharing process and the identification and analysis of interdependencies

- Contingency planning and external measures/dimensions

Also at the level of the EU Member States, policies specifically for the protection of critical infrastructure have been pursued for several years. For Germany, the "National Strategy for Critical Infrastructure Protection" (KRITIS Strategy) should be mentioned at this point, which was previously supplemented by the "National Plan for the Protection of Information Infrastructures" (NPSI) and is now supplemented by the German cyber security strategies from 2013 and 2016. Based on the KRITIS Strategy, critical infrastructures are organisations and institutions of major importance to the state community, whose failure or impairment would result in lasting supply problems, significant disruptions to public security or other dramatic consequences[5]. In the following, further infrastructures and processing areas are listed that are critical in the aforementioned overall social sense. It should be noted, however, that these classifications are not yet legally binding, as they are only part of a political strategy:

- Basic technical infrastructures: energy supply, information and communication technology, transport and traffic, water supply and sewage disposal

- Socio-economic service infrastructures: health care, nutrition, emergency and rescue services, civil protection, parliament, government, public administration, justice, finance and insurance, media, culture

The KRITIS Strategy divides the risks and threats to such infrastructure into three categories: harmful natural events, technical and human failure, terrorism/crime and war. Based on the above-mentioned hazard situations, the strategic objectives for the protection of critical infrastructures are proposed. The focus of all government measures is on prevention and sustainability, as well as readiness to respond to serious cyber incidents. In order to achieve the objectives , the introduction of business continuity management and cooperation between the state and the private sector in the sense of a public-private partnership are addressed as a priority. In addition, the Federal Government plans to intensify international cooperation on cyber security.

2.2 European and German Legislation on Critical Infrastructure Protection

Based primarily on the European and German political strategies for the protection of critical infrastructures, various laws have been passed in recent years, which also means that there is no uniform law for the implementation of cyber security. This is also a challenge for those companies addressed by the laws. As far as IT security-specific legislation in the EU and in Germany is concerned, the following legal sources can currently be used as key drivers of corporate information security:

- the EU Network and Information Security Directive from 2016 (EU NIS Directive)
- the EU Cybersecurity Regulation from 2019 (EU CSA)
- the German IT Security Act 2015 (IT-SiG) including the BSI Critical Infrastructure Ordinance (BSI-KritisV, published in two stages in 2016 and 2017 respectively)
- the draft version of the 2nd German IT Security Act (IT-SiG 2.0, 2019)

The IT security-specific regulations, which were established by the German IT-SiG, essentially address the operators of critical infrastructures. These are generally legally defined in §2 para. 10 BSIG and are concretized by the numerical specifications of the BSI-KritisV (so-called "threshold values"). The criteria of quality and quantity are decisive. This means that an institution is classified as critical infrastructure within the meaning of the Act if it belongs to the energy, information technology, telecommunications, transport, traffic, health, water, food, finance and insurance sectors - in this respect it is similar to the NPSI, but not congruent. In addition, in the sense of a "fault consequence relevance" as a quantitative criterion, it must be added that the infrastructure is of great importance for the functioning of the community because its failure or impairment would lead to considerable problems in the supply chain or threats to public safety. The measure of the significance of the consequences of such failures is primarily based on the figures/numbers defined in the BSI-KritisV. The German IT-SiG is a so-called "Article Law" and contains a regulatory mandate to the legislator to amend various individual laws. These include the Atomic Energy Act, the Act on the Federal Office for Information Security (BSI), the Energy Industry Act, the Telecommunications Act and the Telemedia Act of Germany. All these regulations contain special requirements for information security, which must be provided by the respective operators. In case of non-compliance, the requirements are subject to sometimes substantial sanctions. The laws themselves do not usually go into the technical-organizational details of the concrete obligations with regard to content. Thus, in most cases only general objectives to be applied to information security are defined, or reference is made to "appropriate" measures that correspond to the "state of the art". This is a so-called "undefined legal term" or a "general clause". From a legal point of view, the "state of the art" is to be classified in the triad of "generally accepted rules of technology" and "state of science and technology", whereby the "state of the art" represents the technical-organisational mean value between these two extremes. Consequently, it depends on what is technically necessary, suitable, appropriate and avoidable in terms of malfunctions and risks at the respective present time. In addition to the technical-organisational IT security obligations in accordance with the "state of the art", critical infrastructures are also subject to a reporting obligation to the BSI. Since the IT Security Act came into force in 2015, there has been considerable speculation and uncertainty on the part of operators of infrastructures affected by the Act regarding the content and scope of the technical and organisational measures to be taken for cyber security. In the meantime, two specific guidelines have been created for the energy sector in particular to define the legal requirements, but these are outside the scope of the law itself:

- Industry-specific safety standards (B3S) Energy, based on §8a para. 2 BSIG: one standard for plants or systems for the control/bundling of electrical power (B3S Aggregators)[6] and one standard for the distribution of district heating (B3S Vv Fw)[7].

- IT security catalogue in accordance with §11 para. 1a EnWG of the supervisory authority Bundesnetzagentur (BNetzA)[8].

Both sources contain detailed specifications for the technical-organizational implementation of cyber security measures by the operators of energy supply networks and energy facilities, which are essentially linked to the introduction of an Information Security Management System (ISMS). The developments around a specifically European and German law of information security are finally supplemented by the EU NIS-RL, the EU CSA as well as by the draft for an IT-SiG 2.0. The NIS Directive contains obligations for so-called "essential services", which for Germany correspond to critical infrastructures. As an EU Directive, it does not have any direct effect in the Member States, but must be incorporated into German law by means of a national implementation law in order to be effective. This has already been done in 2017. In addition, legislators are increasingly creating cross-sectoral IT security-related regulations that go beyond the scope of critical infrastructures - a development that is particularly evident in the CSA and the draft of the IT-SiG 2.0. The CSA is developing a comprehensive, cross-sectoral IT security certification system that is currently still voluntary and theoretically ranges from IoT consumer products to the protection of a critical energy infrastructure. Although IT-SiG 2.0 introduces regulatory proposals aimed at the consumer sector, it also increases the requirements for the operation of a critical infrastructure in Germany. Among other aspects, the draft law requires that manufacturers which install their products in control systems of a critical infrastructure ensure that cyber security is guaranteed for the entire supply chain of their product. The IT-SiG 2.0 is expected to be passed by the German Parliament before the end of 2020.

2.3 Comparison of European and German strategic requirements with the U.S. National Infrastructure Protection Plan (NIPP)

The US NIPP from 2013[9] is also a political-strategic document that was developed in cooperation between authorities, critical infrastructure operators, companies, scientific institutions and civil society actors. The NIPP is also comparable with the European and German objectives in its three-part objectives: In a cooperation between operators and the state, the aim is to achieve a preventive protection of critical infrastructures and to form a community that supports cooperation and the exchange of information. The various national levels and sectors will be equally involved. The NIPP's risk analysis for critical infrastructures addresses similar factors as the EU regulation, but pandemics as a factor for lacking functioning of critical infrastructures are integrated here as well. In addition, further sectors beyond the European and German regulations are defined as critical: Chemicals (in Germany, this is partly addressed by the draft IT-SiG 2.0), commercial facilities, critical manufacturing (also addressed in Germany by the draft IT-SiG 2.0, but not at EU level), dams, defensive industrial base, and government facilities (although part of the German political KRITIS strategy, they are in Germany not part of the binding legal regulations on cyber security). Some of the categories of critical infrastructure that are separately managed in the USA are listed as sub-categories in the EU and in Germany, for example dams or the disposal of radioactive waste for the energy sector. Since the technical measures for IT security are of a global nature, there is also a significant degree of comparability between the EU requirements and those of the NIPP, for example with regard to risk identification, technical-organizational measures in the sense of establishing a PDCA cycle/ISMS or implementing security by design.

2.4 Related Work

Hurst et al. [0] discuss critical infrastructures and the digital threats they face by surveying different infrastructure security strategies. Rehbohm et al. [0] did an interview study among the chief information security officers (CISOs) of the federal states of Germany about current challenges in cybersecurity management. The Federal Office for Information Security[10] (BSI) lists the status of the implementation of cybersecurity in the energy sector in 2015 [0, p. 16ff]. They state that while some of the companies have put IT security measure in place to ensure a high degree of security, other hardly have any measures in place.

Closest to our work is a study from Müller et al. [0] which also investigates ISMS for German energy providers. They called about 200 Chief Information Security Officers (CISOs) from German energy providers and ended up with 42 complete questionnaires.

3. Methodology

We surveyed German energy providers about their information security in 2016 and 2018. Besides the survey, we also got some insights by workshops within the SIDATE project [0] which showed to be useful for the discussion of the results. The SIDATE project aimed to support small and medium energy providers to cope with the security requirements. Personnel from energy providers responsible for IT security participated in the workshops [0, 0].

3.1 Questionnaire

The questionnaire covered sections about general information, organisational aspects, ISMS and ISMS maintanance (only in 2018), the office IT, and networking and organisational aspects about the industrial control system of the energy providers [0, 0],[0, 0]. We did pre-tests within the universities' research groups and in the SIDATE project which included project partners with domain specific knowledge. The two different versions of the questionnaire are shown in the appendix.

3.2 Data Collection

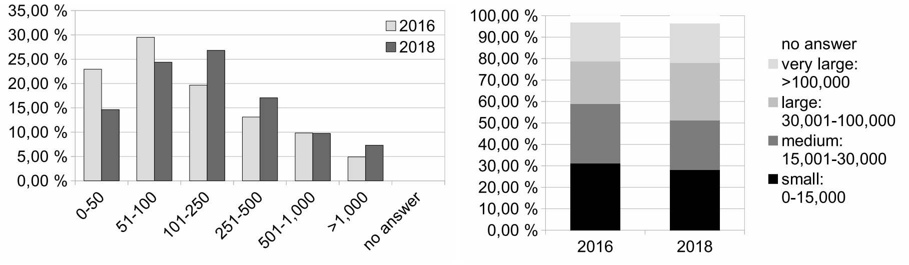
In 2016 (2018), we (physically) mailed to all 881 (890) energy providers listed in August 2016 (September 2018) [0] by the Federal Network Agency (German: Bundesnetzagentur or BNetzA), the German regulatory office for electricity, gas, telecommunications, post and railway markets [0]. We sent them a printed version of the survey and a link to the online survey along with a cover letter referring to the SIDATE project [0] about supporting energy providers with their IT-Security.

The survey lasted from September 1^{st} to October 15^{th}, 2016 (September 10^{th} to October 30^{th} 2018). and received 22 (38) replies online and 39 (46) replies by mail summing up to a total of 61 (84) replies resulting in a response rate of 6.9% (9,4%).

Since two respondents within the 2018 survey claimed that they are not regarded as critical infrastructure and therefore have not implemented an ISMS, we removed their answers.

3.3 Demographics

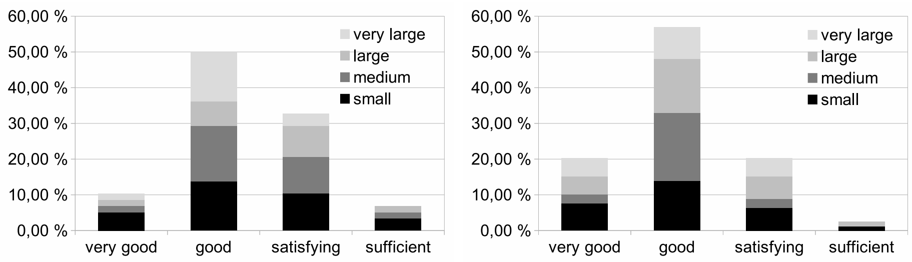
We asked the energy providers about the number of supply points and the number of employees as shown in Fig. 1. In order to refer to the size of the energy providers, we mapped them to the four categories "small, medium, large and very large" according to the number of supply points. In the survey, we had more distinct categories at the border (<1,000 and 100,001 - 500,000), but due to their low population we merged them. We checked with Spearman's rank correlation for similarities with the number of employees and found for 2016 (2018) ρ-values of 0.725 (0.496) with p-values lower than 10^{-5} indicating a strong (moderate) relationship. Therefore, we argue that it is sufficient to consider the number of supply points and refer in the following to the size of an energy provider following the definition above. A comparison with the study from Müller et al. [0] shows that we had more small energy providers than they considering the number of supply points as well as the number of employees.



(a) Number of Employees

(b) Number of Supply Points

Figure 1: Size of the participating energy providers



(a) 2016

(b) 2018

Figure 2: Perceived Security

To test similarity of the data for 2016 and 2018, we conducted a two-one-sided t-test (TOST) [0] for the energy provider's size and since for $\epsilon = 0.5$ the p-value of 0.027 was within the 95% confidence interval, we assume that the participating energy providers are similarly distributed within both surveys.

4. Results

Due to space limitations, we can only present an analysis of selected items of the questionnaire. We asked the participants about their perceived protection of systems and data in their company (cf. Fig. 2.) A Spearman's rank correlation test showed no correlation between size (cf. A2 in questionnaire) and perceived security (cf. B8 in questionnaire), but an independent-samples t-test (t(140)=2.5982, p-value = 0.01) suggests that the perceived security increased significantly[11] from 2016 to 2018.

4.1 ISMS Introduction

Tab. 1 shows that as expected, energy providers were quite active from 2016 to 2018 in implementing an ISMS (cf. C1 in questionnaire). While in 2016 75% of the energy providers only had at most 3 phases finished, in 2018 roughly half of them had 15 or more phases finished. This is also reflected in the mean 2.22 vs. 14.04 with a similar standard deviation (sd) and interquartile range (IQR). The status of the different ISMS implementation phases is shown in Fig. 3 which shows that besides the incident-management support most implementation phases are finished by are large majority.

A Spearman's rank correlation test between the perceived security (cf. B8 in the questionnaire) and the number of finished ISMS phases (cf. C4 in the questionnaire) suggests also a significant small correlation (ρ-value: -0.27, p-value = 0.006). However, since the correlation was not significant when only considering the data from 2016 or 2018, we assume that this effect is merely the result of an increase in perceived security and increase of finished ISMS phases from 2016 to 2018.

Table 1: Distribution of finished ISMS implementation phases

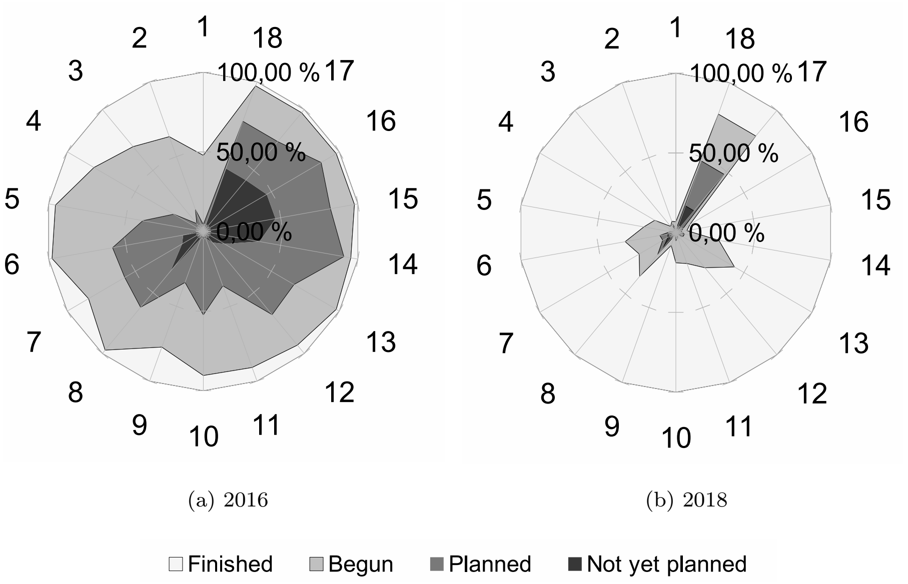
Year	mean	sd	IQR	0%	25%	50%	75%	100%	n	NA
2016	2.22	3.12	3	0	0	1	3	17	46	15
2018	14.04	4.07	4	3	13	15	17	18	57	24

4.2 Motivation and Benefits from the ISMS

Figure 4a shows the energy providers' expectation of the effects of the ISMS's implementation along with the perceived benefits in 2018 (B) and the expected benefits in the future also in 2018 (E). It is visible, that for each of the reasons the energy providers expectations were outperformed. Figure 4b shows the result of the question why the energy providers had introduced an ISMS (in 2018). In both years legal requirements dominate the energy providers' motivation. We also asked in 2018 if the ISMS could improve the information security and 93% confirmed that.

4.3 Effort of the ISMS Implementation

Table 2 shows the costs of the initial implementation of the ISMS (Tab. 2a) and of running the ISMS (Tab. 2b) divided into internal and external costs. Non surprisingly with increasing size, the costs also increase with the exception that the medium sized energy provider seem to have higher costs than large energy provider. The reason is that one



(a) 2016

(b) 2018

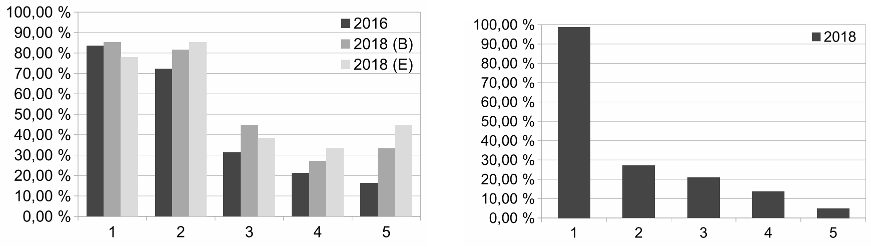
1	Target Setting and Scoping
2	ISMS Policy Development
3	Overview of the existing security architecture
4	Performing Risk Analyses
5	Elaboration of Catalogue of Security Measures
6	Design of the New Security Architecture
7	Description of Quality and Risk Manag. Interf.
8	Development of a Migration Process
9	Elaboration of the Req. Documentation
10	Structure of the Security Organisation
11	Implementation of Management Processes
12	Formulation of Security Architecture (Rules)
13	Measures of Sensitization and Training
14	Implementation of Security Measures
15	Final Project Scope Analysis
16	Preparation for Certification Auditing
17	Execution of Business and Organisational Audits
18	Incident-Management Support

Figure 3: Status of each ISMS implementation phase

medium provider reported very high costs (cf. maximum (100%) column). However, the Spearman's rank correlation test still suggests that there are moderate correlations between size and costs (for all 4 cost types, we found ρ-values between 0.44 and 0.53 with p-values below 10^{-3}). In 2016 (2018) 87% (96%) of the energy providers reported that external consultants were supporting the implementation of the ISMS. However, only 55% reported that they will get external support for running and improving the ISMS.

4.4 Duration

Figure 5 shows the planned duration and the real duration of the ISMS implementation in months. While the duration seems to increase with



1	Fulfilling Legal Requirements
2	Improving Information Security
3	Better Representation of IT Processes (Transparency)
4	Better External Representation of IT Processes
5	(Re-)Structuring of Relevant Business Processes

(a) Top 5 Reasons 2016 + Benefits and Future Expectations 2018

1	Legal Requirements
2	Business Processes are Depending on IT
3	Increased Threats
4	Public Discussion on IT-Security
5	Outsourcing of Services

(b) Top 5 Reasons 2018

Figure 4: Motivation, Benefits and Expectations to Implement an ISMS

Table 2: Costs of the ISMS implementation in thousand Euros (2018)

(a) Initial Costs

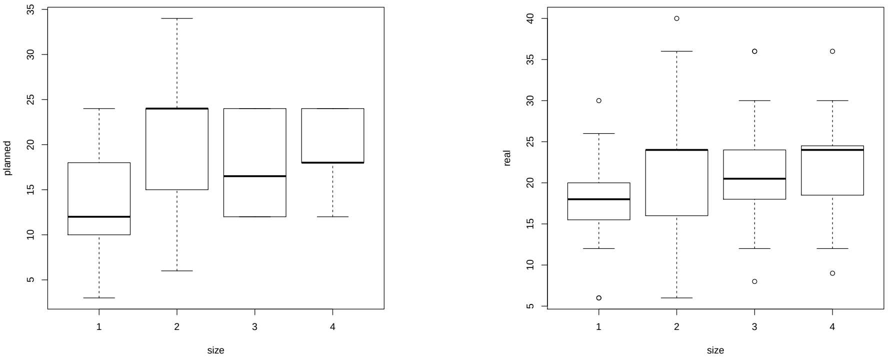
	Size	mean	sd	IQR	0%	25%	50%	75%	100%	n
Internal	S	56.823	75.707	50	3	10	30	60	300	17
	M	180.275	504.143	35.525	10.080	30	50	65.525	2000	15
	L	110.000	64.142	90	30	60	80	150	250	15
	XL	313.500	543.240	146.5	30	87.5	150	234	2000	12
External	S	54.058	50.380	60	4	20	40	80	200	17
	M	115.891	245.959	50	20	30	45	80	1000	15
	L	102.058	53.620	65	25	60	100	125	220	17
	XL	132.769	97.367	90	25	60	110	150	350	13

(b) Running Costs

	Size	mean	sd	IQR	0%	25%	50%	75%	100%	n
Internal	S	18.529	16.789	25	1	5	10	30	50	17
	M	72.621	201.748	17.5	4.320	10	20	27.5	800	15
	L	33.000	23.207	25	10	20	25	45	100	15
	XL	101.538	126.678	70	10	30	80	100	500	13
External	S	10.000	12.303	7.625	1	2.375	6.5	10	50	16
	M	28.125	47.314	10	5	10	15	20	200	16
	L	21.866	13.968	12.5	5	15	20	27.5	50	15
	XL	42.285	48.445	32.5	5	15	35	47.5	200	14

S: small; M: medium; L: large; XL: very large

the size, for medium sized energy providers (size 2), the range seems to be extremely large. We found a medium sized correlation between planned and real duration (0.61 with p-value $< 10^{-8}$), but Spearman's rank correlation suggests only a small correlation between planned (real) duration and energy provider size with ρ-value 0.27 (0.23) and p-value 0.02 (0.04). Overall, the mean real duration (20.7 months) is roughly 20% larger than the mean planned duration (17.0 months).



(a) Planned Duration

(b) Real Duration

Figure 5: Duration to Implement an ISMS in month (2018)

5. Discussion

Results show that the perceived security was increased while in the same time almost all energy providers finished the implementation of their ISMS. This is in line with Müller et al. [0] who reported that 88% of the respondents had already implemented an ISMS. The latter is no surprise, given that the energy providers were legally obliged to do so, although we are aware that some of the small energy providers spent quite some effort to demonstrate that they do not fulfill the definition of a critical infrastructure, and thus do not need to implement an ISMS and get a corresponding certification. This matched the observation that most energy providers' main reason to implement an ISMS were legal requirements, which was also found by Müller et al. [0] (95%). Interestingly, while many were also expecting an increased information security, most of the energy providers had not started to implement an ISMS until they were required by law. On the other hand, more energy providers reported that their information security could benefit from the ISMS than the percentage of providers who expected that before. Again, this is in line with Müller et al. [0] who reported that for 95% the ISMS was beneficial for the energy provider.

Non surprisingly, larger energy providers reported higher costs for implementing and running the ISMS. It would have been interesting to compare that costs not only to the size but to the turnover. However, since many of the energy providers publish their balance sheets, we did not ask for it to ensure their anonymity. Müller et al. [0] reported a lower number of energy providers which received support from external consultants for implementing and running the ISMS than we found, but since they had less smaller energy providers in their sample that most likely explains the difference.

5.1 Limitations

Although we checked for several reliability and validity issues, certain limitations might impact our results. First, the sample size can be considered relatively small for a quantitative study. However, since we checked all results for significance, we argue that our results are still valid, even though, we might have missed results with only a smaller effect size. Furthermore, it is difficult to gather data from energy providers since we could offer them no further incentive than the result of the study and their number is limited (roughly 900).

Our results face also possible self-selection biases since especially in 2018 energy providers who did not manage to implement a reasonable status of their ISMS might not have participated in the study. Additionally, since we decided to do the study anonymously, we could not link the participants from 2016 and 2018. This was an intentional decision, as we noticed that most energy providers were tense. Mainly because in 2016 the energy providers were not sure, what exactly they were required to do and in 2018 because they just had certified their ISMS or were still in the process of doing so.

6. Conclusion and Future Work

Our study suggests that information security of the energy providers benefits from the legislator's decision to require them to implement an ISMS (along with other requirements). Most of the energy providers had not started and only implemented it when they were obliged to do so. The regulation also ensures fairness since all energy providers of a certain size are considered to be critical infrastructure, and thus need to implement it.

It would be interesting in future work to investigate in more detail how the energy providers are coping with new technology such as smart grids and virtual power plants. Furthermore, after the initial implementation, it will be interesting to observe how the energy providers cope with running the ISMS in a useful way.

7. Questionnaires

Question codes

➊: question only appears in the 1st questionnaire
➋: question only appears in the 2nd questionnaire

Answer codes

❖: multiple selection possible;
★: answers: "yes", "no" and "I don't know;
⊙: additional answer: "other";
◘: additional answer: "I don't know".

A: General Company Information

A1 How many employees does your organisation have?

- Less than 50
- 51-100
- 101-250
- 251-500
- 501-1000
- More than 1000

A2 How many meter points are in your network?◘

- 0 - 1,000
- 1,001 - 15,000
- 15,001 - 30,000
- 30,001 - 100,000
- 100,001 - 500,000
- $>$ 500,000

➊**A3** Which unbundling model is implemented in your company?◘⊙

- Small grid
- Major grid
- Lease
- No own grid

B: Organisational Aspects

B1 To which department are you assigned in the company?⊙

- Management IT
- Power system management
- Administration & organization
- Legal department
- Public relations

B2 What is your role in the company?

❶**B3** For how many employees in your company is IT security part of their daily business?

❷**B4** Who in your company is responsible for the operation of the ISMS?

❶**B5** Are there independent service providers in the field of IT security in your company? ★

❶**B6** Who takes on the role of IT security officer in your organization?◻⊙

- I myself
- Other employee
- External service provider(s)
- There is no

❶**B7** To which department is the IT security officer assigned?⊙

- Management IT
- Power system management
- Administration & organization
- Legal department
- Public relations

B8 In your view, how well protected are the systems and data in your company?◻

- Very good
- Good
- Satisfying
- Sufficient

C: ISMS

❶**C1** The introduction of an ISMS is/has ... ◻

- not planned yet
- planned
- already started
- already completed

❶**C2** When should the work on the introduction of an ISMS begin or when did it start?[12]

C3 When was the work on introducing an ISMS completed?[13]

C4 What is the current status of the respective ISMS implementation phases?[14]

❶**C5** By when should the work on introducing an ISMS be completed?[15]

C6 When was the work on introducing an ISMS completed?[16]

C7 How long did you expect the introduction of an ISMS to take at the beginning of the implementation?

C8 How long did it actually take to implement your ISMS?

C9* Have external service providers been or will be consulted when introducing an ISMS?

C10 What were the main reasons for you to introduce an ISMS?❖

- Legal requirements (IT security catalogue, IT security law)
- Increased threat level
- Strong dependence of business operations on IT
- Outsourcing of services to external service providers
- Public discussion on IT security

❷C11 In which areas have you already been able to benefit from the introduction of the ISMS?❖□⊙

- Improvement of information security in the company
- (Re)structuring of the relevant business processes
- Legal compliance
- Better representation of IT processes
- Better external presentation of the IT security processes

C12 What do you hope for or expect from the introduction of an ISMS?❖□⊙

- Improvement of information security in the company
- (Re)structuring of the relevant business processes
- Legal compliance
- Better representation of IT processes
- Better external presentation of the IT security processes

D: ISMS Maintenance

❷D1 In your opinion, could the security level of your company be improved by implementing the ISMS?★

❷D2 How high were your initial costs for the introduction of the ISMS?★

❷D3 Do you have continuous external support for the operation of the ISMS?★

❷D4 What annual costs do you expect for the operation of your ISMS?★

- Internal costs
- External costs

❷D5 In which areas of ISMS operation are the greatest challenges for your company?⊙

- Technical adjustments
- Adaptation of procedures/processes
- Lack of personnel
- Missing hardware
- Process monitoring
- Documentation
- Cooperation with external
- Risk Management
- Implementation of continuous safety improvement

❷D6 Work together with other network operators in the field of ISMS operation or exchange information with from other network operators?★

- Regular cooperation with other network operators
- Regular exchange with other network operators
- Occasional exchange with other network operators
- Little or no exchange with other network operators

❷D7 In your opinion, could cooperation with other network operators contribute to the operation of your ISMS or security level?★

E: Office IT

E1 Are there IT security guidelines for the office IT in your company?★

E2 Are the IT security guidelines updated and, if necessary, adjusted regularly?★

F: Industrial Control System (ICS): network structure

F1 Does your energy control system enable only energy network supervision, or does it also enable to execute switching operations?□

- Supervision only
- Supervision and control

F2 How is the IT network of your energy control system separated from other networks (e. g. IT department, Internet, maintenance companies)?□

- Logical Separation
- Physical Separation
- No Separation

F3 Is the network of your energy control system divided in different security domains (e. g. through different VLANs)?★

❶F4 Which network technologies do you use in your energy control system network?❖□

- Cable connect
- Wireless connect

❶F5 Which communication standards are used in the network of your energy control system?

❶F6 What wireless network technologies do you use?

❶F7 Which communication standards are used in your control system network?❖□⊙

- IP communication
- Serial communication

❶F8 From which producers do you acquire the network administration systems and devices?

F9 Which types of remote access were established for your energy control system?❖□⊙

  - External Access for maintenance and configuration of the control system
  - Employee Access (e. g. for standby or fault clearance service)

F10 How are remote access procedures via external service providers regulated?⊙

  - External service providers can have access to the system and undertake changes only after receiving authorization, but WITHOUT additional surveillance
  - External service providers can have access to the system and undertake changes only after receiving authorization and only under surveillance
  - External service providers can have access to the system and undertake changes independently

G: ICS: Processes and Organisation

G1 Are you/the responsible employees regularly informed about potential hard- /software vulnerabilities?★

G2 How often are the devices and software within your energy control system updated/renewed?[17]

G3 Is there an updated inventory list in which all the software items are documented (e. g. with version numbers, corresponding accounts and IP addresses)?★

G4 Are there documented IT security guidelines for the energy control system in your company?★

G5 Under which security-relevant standards are your IT systems and processes for network administration elaborated?□⊙

  - ISO/IEC 27001
  - BSI Grundschutz
  - None

G6 Do you perform IT risk analyses for the processes and IT systems for network administration?★

G7 How often do you perform such risk analyses?□

  - More than once a year
  - Yearly
  - Every two years
  - More rarely

G8 Do you perform security audits, vulnerability scans, or penetration tests for the administration systems of the network management technology?□

  - Yes; by external service providers
  - Yes; by own employees
  - Yes; by both external providers and employees

- No

G9 How often do you perform such vulnerability scans or penetration tests?□
- More than once a year
- Yearly
- Every two years
- More rarely

G10 Do you have an emergency plan for security incidents of network administration?★

G11 Are security-relevant incidents (e. g. portscans, failed login attempts, unauthorised processes) recorded and evaluated?□
- Yes, only logging
- Yes, logging and evaluation
- No, neither

G12 Which information do you evaluate to identify attacks on the IT systems for network control?❖□⊙
- Firewall logs
- System logs
- Failed logins
- Honeypot logs

G13 Do you use metrics to assess vulnerabilities (e. g. CVSS)?★

G14 Is IT security defined as a requirement for acquiring new hard- and software?★

8. Acknowledgements

This research was supported by the German Federal Ministry of Education within the projects SIDATE (grant numbers: 16KIS0239K, 16KIS0240) and NutriSafe (grant number: 13N15071) and by the European Union within the project CyberSec4Europe (grant number 830929). We especially thank Benedikt Ley, Julian Dax and Frank Terhaag for their contribution to conduct the survey.

Notes

1. German Newspaper: Spiegel Online (2016): „Schadsoftware in bayerischem Atomkraftwerk entdeckt“, `http://www.spiegel.de/netzwelt/web/grundremmingencomputervirus-im-atomkraftwerk-entdeckt-a-1089248.html`
2. German newspaper: Süddeutsche Zeitung (2018): „Warnung vor Hackerangriffen auf deutsche Energieversorger“, `http://www.sueddeutsche.de/digital/itsicherheit-warnung-vor-hackerangriffen-auf-deutsche-energieversorger-1.4015345`
3. German newspaper: Süddeutsche Zeitung (2018): „Hacker haben deutschen Energieversorger angegriffen, `http://www.sueddeutsche.de/digital/enbwtochter-hacker-haben-deutschen-energieversorger-angegriffen-1.3980625`“
4. EPCIP, COM (2006), 786 final, p. 3.
5. Nationale Strategie zum Schutz Kritischer Infrastrukturen, S. 3.

6. `https://www.bdew.de/energie/b3s-aggregatoren/`

7. `https://www.bdew.de/energie/b3s-fernwaermenetze/`

8. `https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_08-2015.pdf`

9. `https://www.dhs.gov/sites/default/files/publications/NIPP\%202013_Partnering\%20for\%20Critical\%20Infrastructure\%20Security\%20and\%20Resilience_508_0.pdf`

10. German: Bundesamt für Sicherheit in der Informationstechnik

11. mean in 2016: 2.41, in 2018: 2.06 with very good as 1 and sufficient as 4

12. Answer options: half years from 2nd 2016 to 2nd 2018, Later and I don't know

13. Answer options: half years from 2nd 2013 to 2nd 2018, Earlier and I don't know

14. It has been asked for the current status (not yet planned, planned, begun, or finished) for the implementation phases described in Fig. 3

15. Answer options: half years from 2nd 2016 to 2nd 2019, Later and I don't know

16. Answer options: half years from 2nd 2013 to 2nd 2016, Earlier and I don't know

17. It has been asked for the update frequency (regularly, for known vulnerabilities, not yet, or I don't know) of: network equipment (e. g. routers, switches), workstation computer/terminal, server, and network control/telecontrol technology

References

[1] D. Kipker: The EU NIS directive compared to the IT security act - Germany is well positioned for the new European cybersecurity space, *ZD aktuell*, vol. 20, 2016.

[2] W. Dolle and J. Hoff, KRITIS-Sektorstudie Energie, Technical report, Revision February 5th 2015, Bundesamt für Sicherheit in der Informationstechnik, Bonn, North Rhine-Westphalia, Germany 2015.

[3] W. Hurst, M. Merabti and P. Fergus, A survey of critical infrastructure security, *International Conference on Critical Infrastructure Protection*, pp. 127–138, 2014.

[4] T. Rehbohm, K. Sandkuhl and T. Kemmerich, On challenges of cyber and information security management in federal structures-the example of German public administration, *Proceedings of the Joint International Conference on Perspectives in Business Informatics Research Workshops and Doctoral Consortium at Centre for New Information Technologies (CNTI)*, pp. 1–13, 2019.

[5] J. Müller, A. Sänn, M.M. Wendt, R.A. Albrecht and P. Langendörfer, Informationssicherheits-Management-Systeme (ISMS) bei Energieversorgern 2018, Betriebswirtschaftliches Forschungszentrum für Fragen der mittelständischen Wirtschaft e. V. an der Universität Bayreuth, Bayreuth, Bavaria, Germany, 2018.

[6] J. Dax, D. Hamburg, S. Pape, V. Pipek, K. Rannenberg, C. Schmitz, A. Sekulla and F. Terhaag, Sichere Informationsnetze bei kleinen und mittleren Energieversorgern (SIDATE), in *State of the Art: IT-Sicherheit für Kritische Infrastrukturen*, S. Rudel and U. Lechner

(Eds.), Universität der Bundeswehr, Neubiberg, Bavaria, Germany, p. 29, 2018.

[7] J. Dax, B. Ley, S. Pape, C. Schmitz, V. Pipek and K. Rannenberg, Elicitation of requirements for an inter-organizational platform to support security management decisions, *Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance*, 2016.

[8] C. Schmitz, A. Sekula, S. Pape, V. Pipek and K. Rannenberg, Easing the burden of security self-assessments, *Proceedings of the Twelfth International Symposium on Human Aspects of Information Security & Assurance*, 2018.

[9] S. Pape, V. Pipek, V., K. Rannenberg, C. Schmitz, A. Sekulla and F. Terhaag, Stand zur IT-Sicherheit deutscher Stromnetzbetreiber, Technical Report, University of Siegen, Siegen, North Rhine-Westphalia, Germany, 2018.

[10] J. Dax, B. Ley, S. Pape, V. Pipek, K. Rannenberg, C. Schmitz and A. Sekulla, Stand der IT-Sicherheit bei deutschen Stromnetzbetreibern, in *State of the Art: IT-Sicherheit für Kritische Infrastrukturen*, S. Rudel and U. Lechner (Eds.), Universität der Bundeswehr, Neubiberg, Bavaria, Germany, p. 69–74, 2018.

[11] J. Dax, A. Ivan, B. Ley, S. Pape, V. Pipek, K. Rannenberg, C. Schmitz and A. Sekulla, Stand zur IT-Sicherheit deutscher Stromnetzbetreiber, Technical Report, University of Siegen, Siegen, North Rhine-Westphalia, Germany, 2016.

[12] J. Dax, A. Ivan, B. Ley, S. Pape, V. Pipek, K. Rannenberg, C. Schmitz and A. Sekulla, Status of German Energy Providers, Technical Report, arXiv 1709.01254, Cornell University, New York, United States, 2016.

[13] Bundesnetzagentur, Listen der Netzbetreiber und Versorgungsunternehmen, Bonn, North Rhine-Westphalia, Germany, December 2019. `https://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/HandelundVertrieb/Lieferantenanzeige/lieferantenanzeige-node.html`

[14] Bundesnetzagentur, About us, Bonn, North Rhine-Westphalia, Germany, September 2013. `https://www.bundesnetzagentur.de/EN/Areas/Energy/AboutUs/aboutus-node.html`

[15] D.J. Schuirmann, A comparison of the two one-sided tests procedure and the power approach for assessing the equivalence of average bioavailability, *Journal of pharmacokinetics and biopharmaceutics*, vol. 15(6), pp. 657–680, 1987.