On the Use of Information Security Management Systems by German Energy Providers

14th IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, Arlington, Virginia, USA – March 17, 2020

Sebastian Pape[1], Christopher Schmitz[1], **Dennis-Kenji Kipker**[2], and André Sekulla[3]

[1]Goethe University Frankfurt, Germany

[2]University of Bremen, Germany

[3]University of Siegen, Germany

Agenda

- **Legal Background**
- **Survey**
  - **Methodology**
  - **Results**
- **Legal Assessment**
  - **State of the Art**
  - **Comparison to National Infrastructure Protection Plan (NIPP)**
- **Summary & Outlook**

Legal Basics

- **Critical infrastructures:** Have particular importance for the functioning of the community and for securing the basic needs of the population
- Increasing reliance on ICT makes regulation necessary:
  - IT-SiG (2015), EU NIS-Directive (2016) and its German Implementation Act (2017)
  - Concretization of the definition of critical infrastructure by BSI-KritisV (KRITIS regulation) of the BMI (two stages: 2016 + 2017)
  - Main focus: Significant changes in the BSIG
- **Relevance for the energy sector :** § 11 para. 1a-1c EnWG – IT-security measures established by the operators of energy supply networks and energy facilities (inserted and amended by the IT-SiG and the Implementation Act of EU NIS-Directive)

Critical Services in the Energy Sector

Power supply	Gas supply	Fuel and heating oil supply	District heating supply
• Centralized/decentralized power generation plant • Transmission and distribution networks	• Gas production • Gas transportation via long-distance transmission networks • Gas distribution to consumers	• Crude oil production and product manufacturing • Oil transportation • Fuel and heating oil distribution	• Generation of district heat • Distribution of district heat

Obligations for Operators of Critical Infrastructures

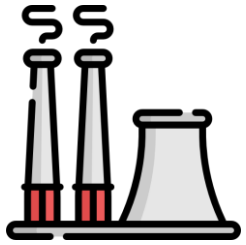
Methodology

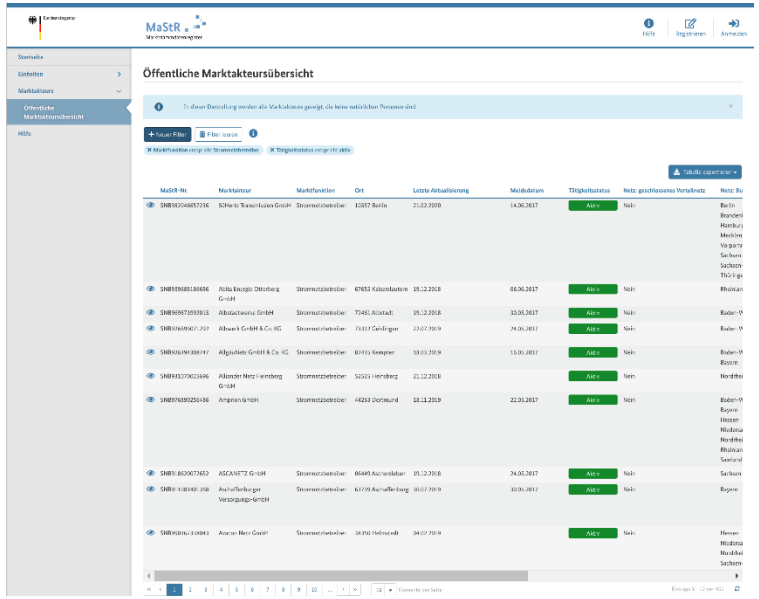
- Pre-tests
  - within the universities' research groups and in the national project on CIP
- 2 surveys in autumn 2016 (2018)


(Snail) mailed to all 881 (890) energy providers in Germany


61 (84) replies -> response rate 6.9% (9.4%)

- Additional information from workshops





Key Aspects of the Survey

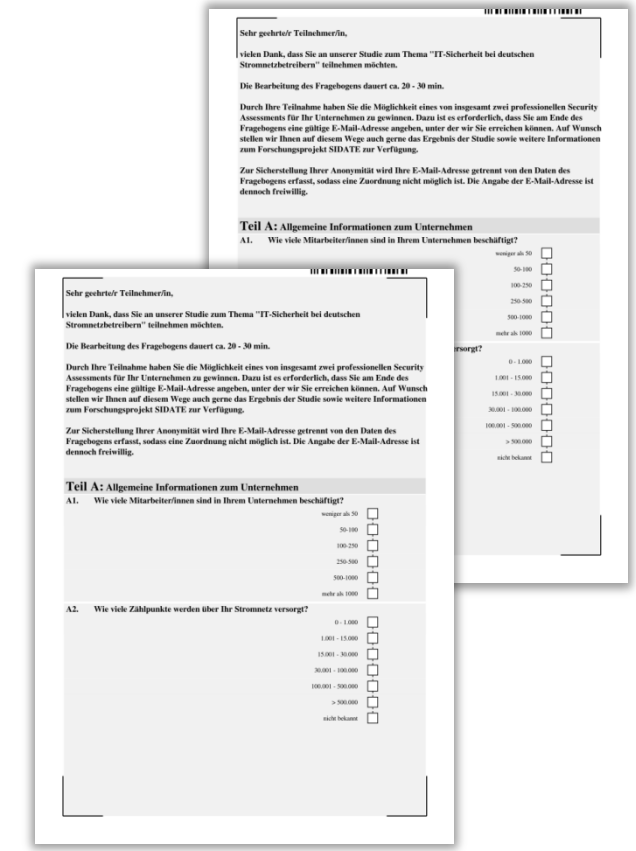
Company information

Organizational aspects

Network structure and security measures

ISMS

- **Motivation** to introduce an ISMS and expected **benefits**
- **Duration** to implement an ISMS
- **Effort** of the ISMS Implementation
- **Planning** of the ISMS (only in 2016)
- **Maintenance** of the ISMS (only in 2018)


Sehr geehrte/r Teilnehmer/in,

vielen Dank, dass Sie an unserer Studie zum Thema "IT-Sicherheit bei deutschen Stromnetzbetreibern" teilnehmen möchten.

Die Bearbeitung des Fragebogens dauert ca. 20 - 30 min.

Durch Ihre Teilnahme haben Sie die Möglichkeit eines von insgesamt zwei professionellen Security Assessments für Ihr Unternehmen zu gewinnen. Dazu ist es erforderlich, dass Sie am Ende des Fragebogens eine gültige E-Mail-Adresse angeben, unter der wir Sie erreichen können. Auf Wunsch stellen wir Ihnen auf diesem Wege auch gerne das Ergebnis der Studie sowie weitere Informationen zum Forschungsprojekt SIDATE zur Verfügung.

Zur Sicherstellung Ihrer Anonymität wird Ihre E-Mail-Adresse getrennt von den Daten des Fragebogens erfasst, sodass eine Zuordnung nicht möglich ist. Die Angabe der E-Mail-Adresse ist dennoch freiwillig.

Teil A: Allgemeine Informationen zum Unternehmen

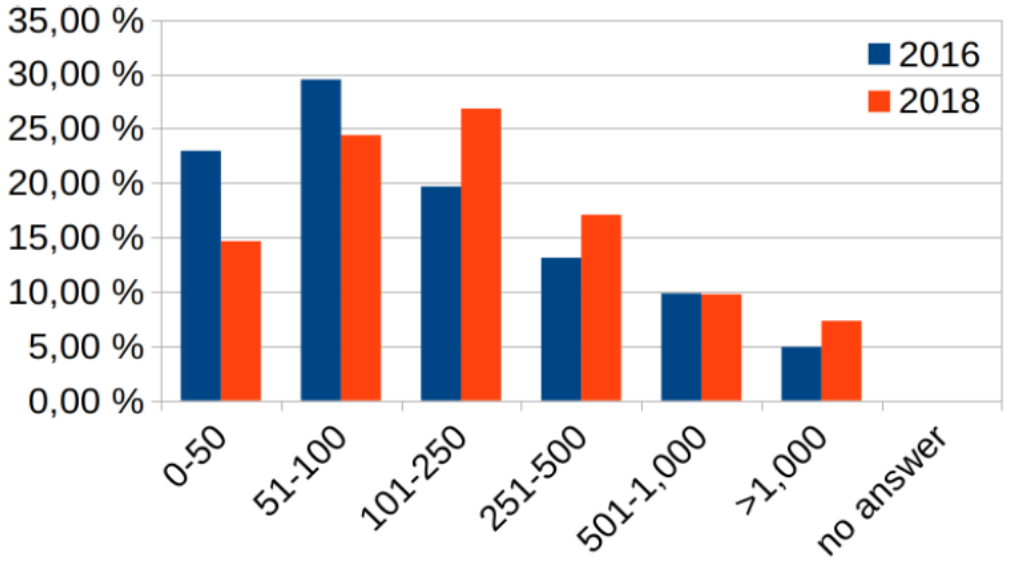
A1. Wie viele Mitarbeiter/innen sind in Ihrem Unternehmen beschäftigt?

- weniger als 50
- 50-100
- 100-250
- 250-500
- 500-1000
- mehr als 1000

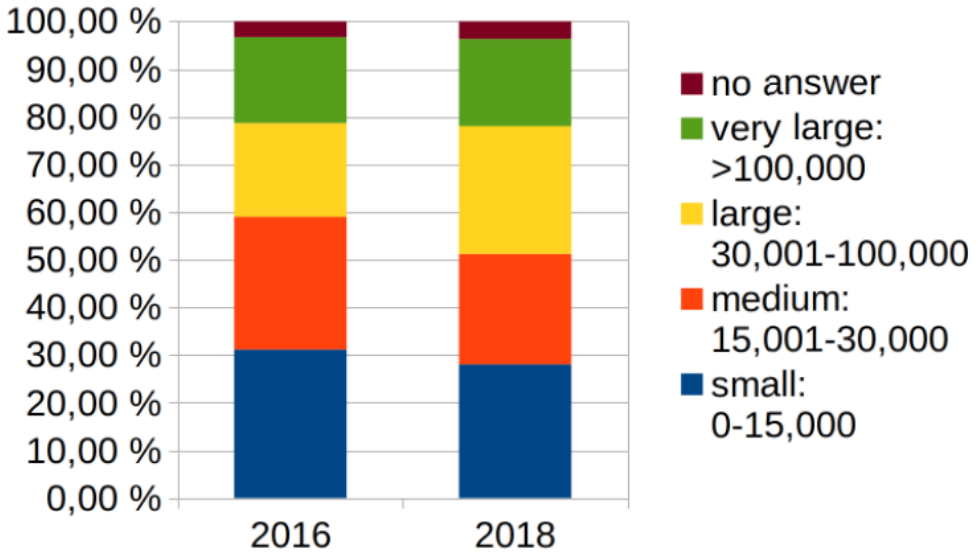
A2. Wie viele Zählpunkte werden über Ihr Stromnetz versorgt?

- 0 - 1.000
- 1.001 - 15.000
- 15.001 - 30.000
- 30.001 - 100.000
- 100.001 - 500.000
- > 500.000
- nicht bekannt

Size of the Participating Energy Providers



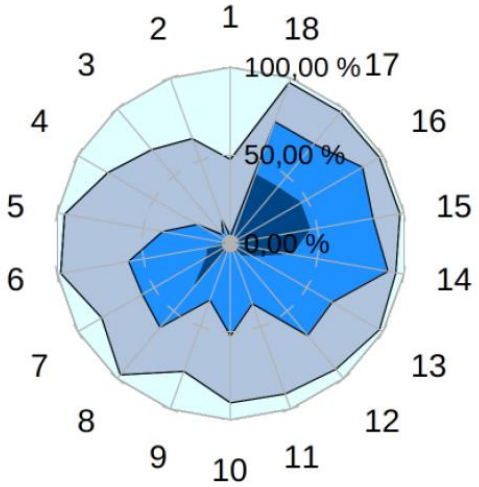
(a) Number of Employees



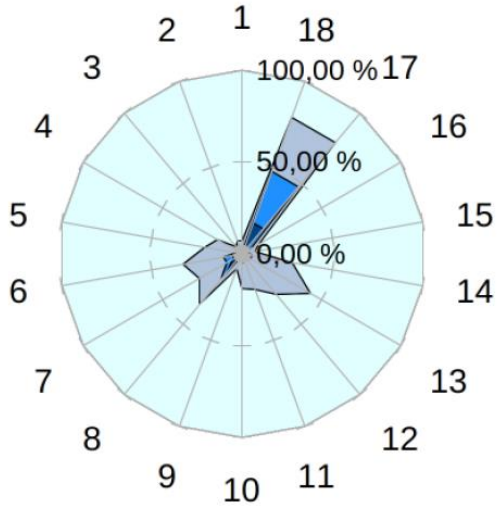
(b) Number of Supply Points

- Spearman's rank correlation between #employees and #supply points (ρ-values of 0.725 and 0.496)
- Two-one-sided t-test (TOST) indicates similarity between 2016 and 2018 (ε = 0.5, p=0.027)

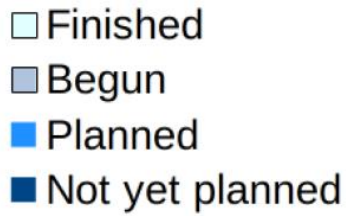
ISMS Implementation Progress



(a) 2016



(b) 2018

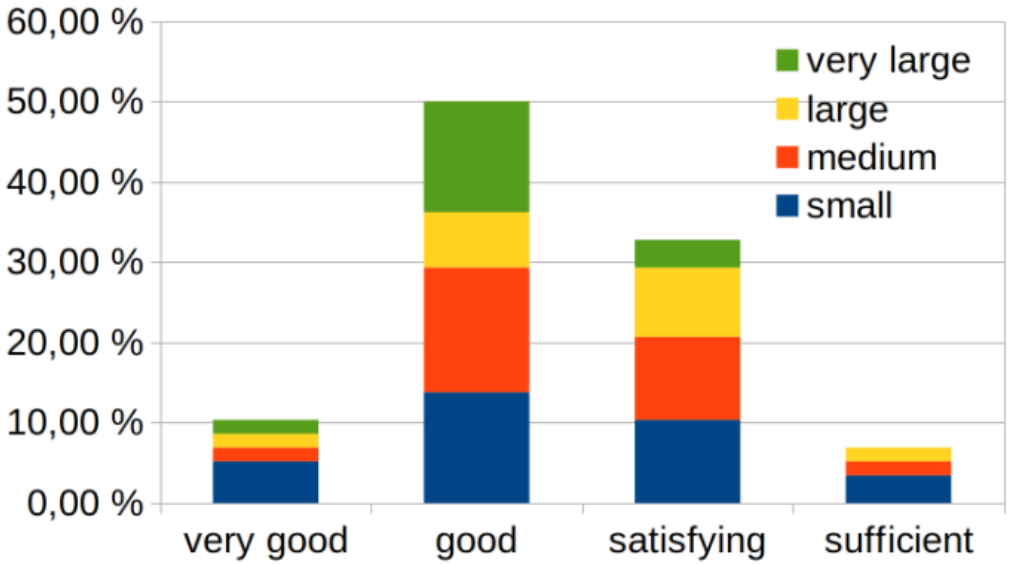


- 18 Incident-Management Support

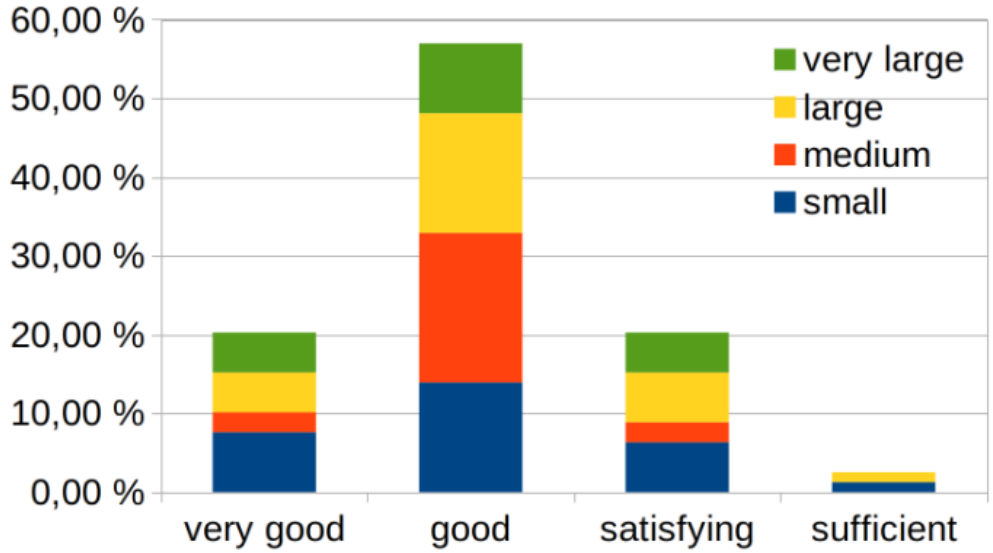
Table 1: Distribution of finished ISMS implementation phases

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

Perceived Security



(a) 2016



(b) 2018

- Independent-samples t-test (t(140)=2.5982, p-value = 0.01):
  increase from 2016 to 2018
- No correlation to size
- Weak correlation to finished ISMS phases (2016+2018)

Costs of the ISMS implementation (2018)

(a) Initial Costs

	Size	mean	sd	IQR	0%	25%	50%	75%	100%	n
Internal	S	56823	75707	50000	3000	10000	30000	60000	300000	17
	M	180275	504143	35525	10080	30000	50000	65525	2000000	15
	L	110000	64142	90000	30000	60000	80000	150000	250000	15
	XL	313500	543240	146500	30000	87500	150000	234000	2000000	12
External	S	54058	50380	60000	4000	20000	40000	80000	200000	17
	M	115891	245959	50000	20000	30000	45000	80000	1000000	15
	L	102058	53620	65000	25000	60000	100000	125000	220000	17
	XL	132769	97367	90000	25000	60000	110000	150000	350000	13

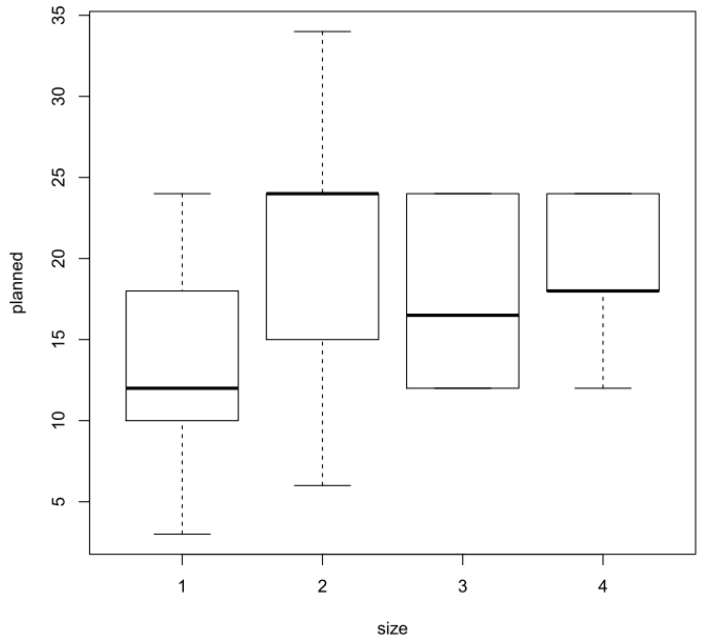
(b) Running Costs

	Size	mean	sd	IQR	0%	25%	50%	75%	100%	n
Internal	S	18529	16789	25000	1000	5000	10000	30000	50000	17
	M	72621	201748	17500	4320	10000	20000	27500	800000	15
	L	33000	23207	25000	10000	20000	25000	45000	100000	15
	XL	101538	126678	70000	10000	30000	80000	100000	500000	13
External	S	10000	12303	7625	1000	2375	6500	10000	50000	16
	M	28125	47314	10000	5000	10000	15000	20000	200000	16
	L	21866	13968	12500	5000	15000	20000	27500	50000	15
	XL	42285	48445	32500	5000	15000	35000	47500	200000	14

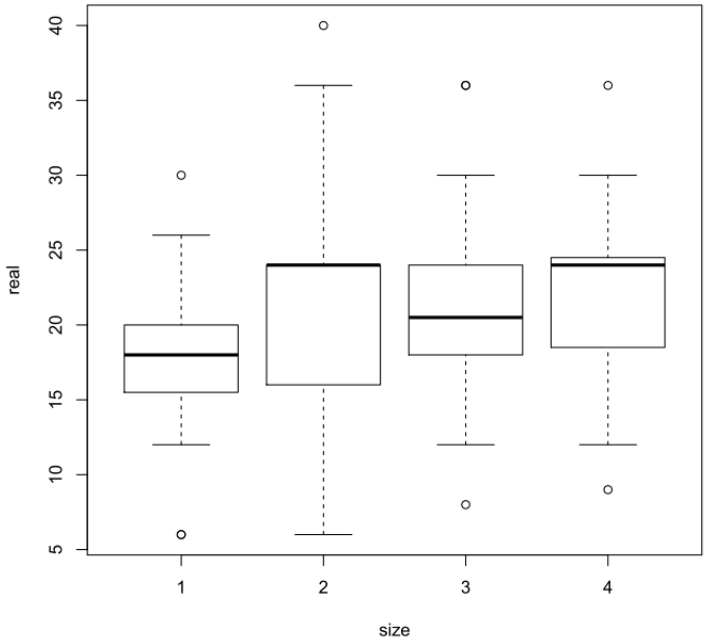
S: small; M: medium; L: large; XL: very large

- Moderate correlation between EP's size & ISMS costs (ρ-values between 0.44 and 0.53)
- 87% and 96% were supported for the implementation of the ISMS
- Only 55% will be supported support for running and improving the ISMS.

Duration to Implement an ISMS (2018)



(a) Planned Duration

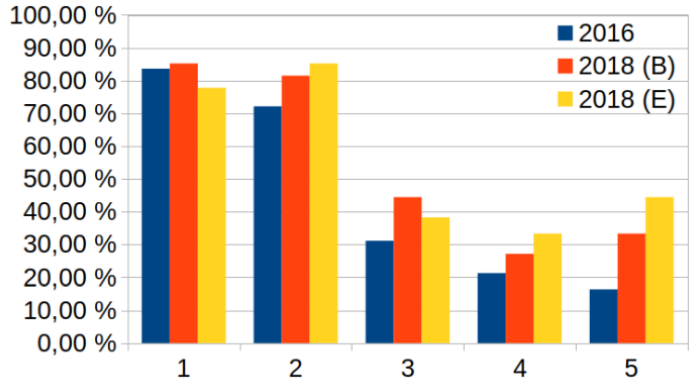


(b) Real Duration

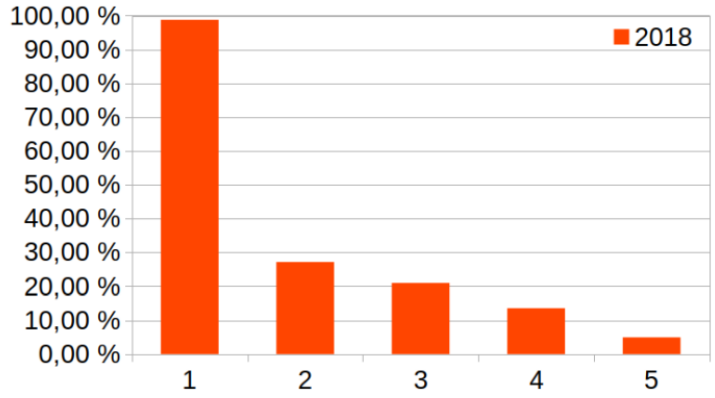
1 – small
2 – medium
3 – large
4 – very large

- Moderate correlation between planned and real duration (ρ-value: 0.61)
- Small correlation between duration and EP's size (ρ-value: 0.27/0.23)
- Real duration ~20% larger than planning (~4 months)

ISMS: Motivation, Benefits and Expectations



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



(b) Top 5 Reasons 2018

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

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

„State of the Art“

- Development status of advanced processes, establishments or operation modes, which make seem the practical suitability of a measure to protect the functionality of IT systems, components or processes against impairments secure
- **→ Undefined legal term, which develops with the dynamical structures of cyber risks**
- → Concretization is possible in particular by industry specific safety standards (B3S)
  - B3S for plants or systems for the control/bundling of electrical power (B3S aggregators)
  - Standard for the distribution of district heating (B3S Vv Fw)
- Documentation by **security and emergency concepts** necessary and appropriate

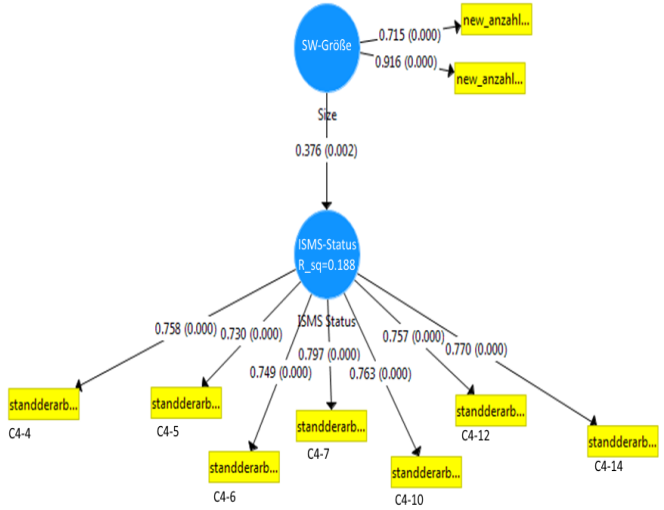
§ 11 EnWG: Special legal Requirements

- **Priority of special legal requirements**: Regulations of the BSIG to TOM are in particular not applicable on operators of energy supply networks or energy facilities in the sense of the EnWG, if they refer to **§ 11 EnWG**
- No obligation to comply with the state of the art, but compliance of the concrete measures named in **security catalogues** :
  - IT-security catalogue for operators of energy networks (BNetzA, 08/2015)
  - IT-security catalogue for operators of energy facilities (BNetzA, 12/2018)
- **Main demand: Establishment of ISMS**
  - Inter alia definition of security categories, measures, risk assessment, contact person for information security
- **Notification obligation in case of IT-security impairment:** For all operators of energy networks and operators of energy facilities, which are a critical infrastructures (§ 11 para. 1c EnWG)

Comparison of European requirements with the U.S. National Infrastructure Protection Plan (NIPP, 2013)

- **Political-strategic document** developed in cooperation between authorities, critical infrastructure operators, companies, scientific institutions, civil society actors
- **Directly comparable with EU cybersecurity objectives:** PPP to achieve a preventive protection, TOM, community building, information exchange
- Risk analysis similar to EU regulation, pandemics included here as well
- **Further sectors beyond EU regulation are defined as critical (or as sub-categories on EU level legislation):**
  - Chemicals (partly addressed by German IT-SiG 2.0 draft)
  - Commercial facilities
  - Critical manufacturing (addressed by German IT-SiG 2.0 draft)
  - Dams
  - Defensive industrial base
  - Government facilities (part of the German political KRITIS strategy)

Limitations



- Small (expected) participation (~10%)
- No linkage between 2016 and 2018

- Space / Time limitations to present results
  - 2016: Estimated time correlates to #employees, but not #supply points
  - 2016: Status in ISMS phases correlated to size (SEM)
  - 2016: Managers estimated significantly less time

  - Many more questions about security measures, ISMS maintenance, etc.

Summary and Outlook

- Most of the energy providers had not started when they were not obliged to do so
- Although they expect the ISMS to increase IT security
- Wish: 1-time black box
- Energy providers benefit from the legislator’s requirements

Future Work

- Remaining questions
- Observe how energy providers run the ISMS

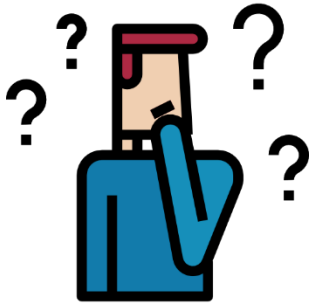
Thank you for your attention!

sebastian.pape@m-chair.de

kipker@uni-bremen.de

Questions?

Status of ISMS Implementation Phases



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 Required 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