IT-Security in Critical Infrastructures Experiences, Results and Research Directions

Ulrike Lechner(✉)

Fakultät für Informatik,
Universität der Bundeswehr München, Neubiberg, Germany
Ulrike.Lechner@unibw.de

Abstract. IT security in critical infrastructures is one of the main challenges in informatics today. This contribution shares results and experiences from the research project VeSiKi. The discussion begins with the human factor in cybersecurity, with economic and strategic approaches to cybersecurity and presents selected results form a case study series on Cybersecurity and an eclectic summary of results from a Cybersecurity research program.

Keywords: Critical infrastructures · IT security · Case studies
Serious games · State-of-the-Art · Risk · Risk perception

1 Introduction and Motivation

Security of critical infrastructures, in particular IT security in critical infrastructures is one of today's major challenge in informatics. "Critical infrastructures (CI) are organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences." [1] Critical infrastructure provide the products and services for the modern civilian society as energy, transportation, food, health services, water as well as telecommunication, media and public administration. Availability of products and services is paramount and integrity and confidentiality of information are other concerns in the domain of IT security in critical infrastructures. The increasing use of information and communication technology creates new areas of vulnerability and dependencies and current geopolitical developments add to the levels of risk. Critical infrastructure providers need to increase the level of security and they also need to meet – in our case – requirements from German and European legislation as, e.g., the German IT Security Act [2].

"Today's reality and yesterday's understanding" is according to Loch et al. [3] a seemingly inherent concern in cybersecurity as the white hats, i.e. the "good cybersecurity guys", tends to be a step behind the black hats, the "bad guys". We analyze in this paper in how far strategy and joint societal efforts to increase the level of security change the game to ensure that critical infrastructures are secure and the civil society is safe. We share in this contribution experiences and results from project VeSiKi that coordinated thirteen research projects with over 80 partners in a collaborative research process in IT security in critical infrastructures (cybersecurity). Cybersecurity is a topic

G. Fahrnberger et al. (Eds.): ICDCIT 2019, LNCS 11319, pp. 42–59, 2019.
https://doi.org/10.1007/978-3-030-05366-6_4

that has both regional and global aspects and that is determined by existing structures, the sociomateriality of critical infrastructures and the need to raise the level of security effectively and efficiently. We discuss what it takes to change the black and white hat game in cybersecurity.

The paper is organized as follows. First, we motivate this research and present the context – the research program "IT Sicherheit in Kritischen Infrastrukturen" (IT Security in Critical Infrastructures, itskritis) funded by the German Federal Ministry of Education and Research in Sect. 2. We argue that human perception of risk and economic decision making do not suffice in the domain of IT-Security and also that cybersecurity should not alone be guided by economic methods and tools (Sects. 3 and 4). In Sect. 5, we analyze strategies and cybersecurity as a joint societal challenge. Experiences about successful solutions in practice from the case study series case|kritis and next generation solutions – the state of the art– conclude our analysis (Sects. 6 and 7).

2 The Context – Project VeSiKi and Research Program itskritis

The context of this review of cybersecurity approaches is the research program "IT-Sicherheit in Kritischen Infrastrukturen" (IT Security in Critical Infrastructures, itskritis) and the research project "Vernetzte IT-Sicherheit Kritischer Infrastrukturen" (Networked IT Security for Critical Infrastructures, VeSiKi) funded by the German Ministry of Education and Research (BMBF) from 2014 to 2018.

Fig. 1. Thirteen research projects Aqua-IT-Lab, CyberSafe, INDI, ITS.APT, Mosaik, PortSec, Prevent, RiskViz, SecMaaS, SICIA, Sidate, Surf and VeSiKI with a total of about 80 research partners collaborate in itskritis (www.itskritis.de)

In thirteen projects (Fig. 1), about 80 critical infrastructure operators, technology providers and research institutions collaborate from 2014 to 2018 in research on innovative concepts and technologies for IT security in critical infrastructures. The collaborative research process of the thirteen projects is coordinated by project VeSiKi.

Fig. 2. Monitor, Monitor 2.0, CASE|KRITIS, ITS|KRITIS platform, State of the Art and IT Security Navigator (www.itskritis.de, www.security-standards.de)

Results of VeSiKi and the collaborative research process include the two studies "Monitor" [4] and "Monitor 2.0" [5] with insights on threat level, threat landscape, IT security strategies and perceptions of risk and security. The interpretations of, e.g., the German IT security act [6] or the NIS directive are essential themes in the collaborative research process and the security navigator (www.security-standards.de) provides a collection of German, European, and international norms, standards, and legal acts. The IT security matchplay series with the games Operation Digital Snake, Owl and Chameleon [7] developed as serious games makes awareness training a fun experience. The itskritis "State of the Art" summarizes selected research results of the thirteen research projects. Platform www.itskrits.de supports knowledge transfer among the projects and, furthermore, between the projects and the general public. The paper at hand relies on the research results of VeSiKi and the collaborative research process of itskritis. Particular to the topic of IT security in critical infrastructures is that human factor, organization and technology need to be addressed and the human factor is the aspect with which we start the discussion on IT security of critical infrastructures.

3 The Human Factor in Cybersecurity

Do humans make the right, the future oriented decisions? – is a very relevant question when it comes to cybersecurity, to innovations in cybersecurity and to strategy. The socalled Human Factor -traditionally- is a major concern in the IT security [8]. We asked IT security experts in the two studies Monitor [4] and Monitor 2.0 [5] of IT security in critical infrastructures for an assessment of the threat level of their own organization, of their industrial sector and for the economic region Germany (Fig. 3).

The data analysis distinguishes all participants, KRITIS, i.e., German Critical Infrastructure according to the German IT Security Act and small and medium sized enterprises (SMEs).

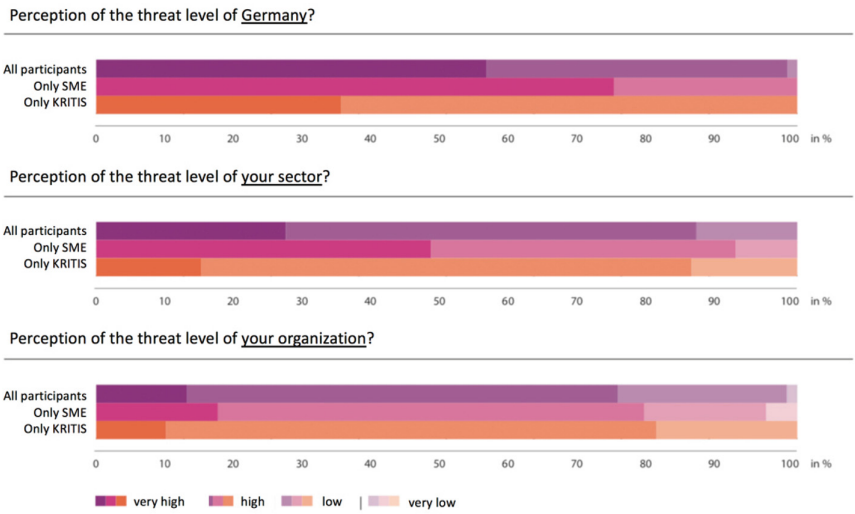

Fig. 3. Threat level perception [5]

There is a distinctive pattern in the data. On average, study participants rate the threat level to their own organization lower than the risk to their sector and this threat level again lower than threat level for Germany (Fig. 3). For the ability to defend against cyberattacks the converse applies: the capabilities of their own organization are rated higher than the capabilities of the sector and these capabilities are again higher than the capabilities of the economic region Germany [4].

This is a known pattern in risk perception: people in general estimate their own risk rather optimistic and are oblivious about this – a phenomenon known as optimism bias [9]. People also tend to overestimate the value of their own work – a phenomenon known as IKEA effect [10] and IT security experts put a lot of effort into the security of their organization. That such perception of individual risks and value of effort is a deeply rooted human trait illustrates the Nobel Memorial Prize in Economic Sciences 2017 that was awarded to Richard Thaler for his work in behavioral economics on risk perception and irrational risk response to abstract risks in the future [9].

A next topic in our studies are the factors that influence the IT security measures in an organization (Fig. 4), i.e. the risk assessment and response on organizational level.

We find that attacks against the organization and regulations have the strongest impact on IT security in an organization. The impact of risk analysis on IT security in an organization seems to be weaker. This is interesting as, e.g. the German IT Security Act as well as international standards and norms require organizations to do risk analysis as part of information security management. We argue, that not only individual

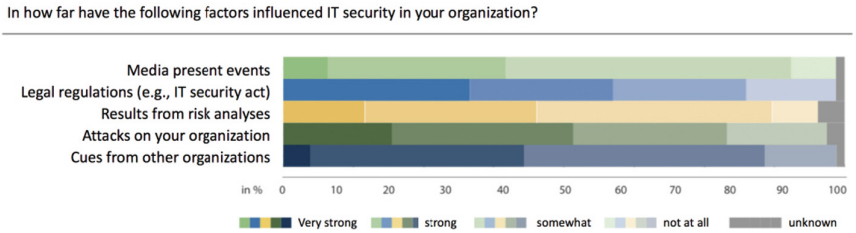

Fig. 4. Impact factors on IT security in an organization [5]

risk perception but also the systematic risk management in organizations seem not to be the driving factor in cybersecurity. Note also that other studies report, that IT security information scouting processes e.g., on novel threats, novel malware or campaigns against the own organization or the sector are typically not well defined, not automated and not systematic. In a study on cybersecurity processes, we find that for many organizations it seems rather unclear on whether IT security related information to the outside contributes to the security within an organization and what the processes eventually look like [11].

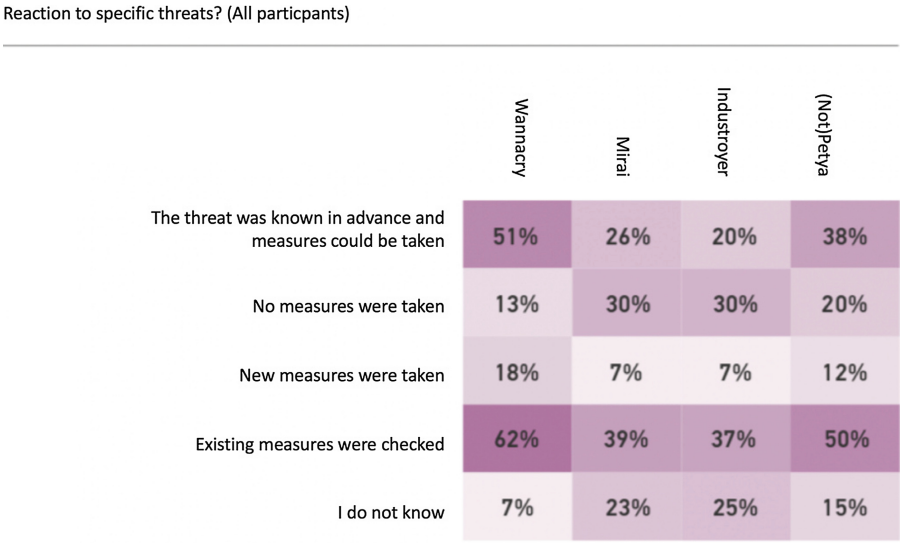

Fig. 5. Reactions of an organization to specific threats [5]

Figure 5 depicts the results on our questions for reaction to news on a Cyberthreat. For a significant percentage of organizations, the threat – in all four cases – was known in advance and measures were already taken in advance, most organizations however reviewed their existing measures, while only a minority took either no action or implemented new IT security measures. One of the IT experts in critical infrastructures

commented on that figure that – "yes, for every new malware we look what that means for our processes". Note that critical infrastructure providers, i.e. that are categorized as KRITIS according to the German IT Security Act are in general more active – they review processes more often and they take more often new measures than providers of (non-critical) infrastructures [5]. This illustrates that critical infrastructure providers take their responsibility seriously and become active whenever there is information on a novel malware. It seems that the confidence in security in their own organization does not prevent the IT security experts to check measures and processes in place. This result seems to contradict – to some extent – the optimistic risk perception and capability perception presented in Fig. 1.

Psychology and marketing literature point out that it is a deeply human trait to be optimistic, to underestimate risks, to respond not rationally to abstract risks in the future. This optimism bias is found in both men and women as well as throughout cultures. Our results from the Monitor studies seem to suggest that the optimism bias applies in cybersecurity and also that the institutionalized systematic risk management as part of the information security management in organizations hardly provide the energy to change the black hat - white hat game in IT security while the critical infrastructure provides need to put effort into their systems with every novel malware and threat.

The Nobel laureate Richard Thaler suggests that such risk response is somewhat inherent for abstract risks in the future: it takes smart decision architectures and a nudge strategy [9] to ensure that humans make the right, the safe and future oriented decisions. "Nudge is a concept in behavioral science, political theory and economics which proposes positive reinforcement and indirect suggestions as ways to influence the behavior and decision making of groups or individuals. Nudging contrasts with other ways to achieve compliance, such as education, legislation or enforcement. A nudge makes it more likely that an individual will make a particular choice, or behave in a particular way, by altering the environment so that automatic cognitive processes are triggered to favour the desired outcome." [9] In subsequent sections, we review whether economic theories and instruments provide guidance in risk response, the global and national approaches to Cybersecurity and technology to enable smart decision architectures and nudges.

4 The Economy of Cybersecurity – a Brief Review

In security of critical infrastructures costs and other burdens of both technological and organizational measures are crucial. Various studies argue that the damage from cybersecurity incidents is on the rise and that this is a global phenomenon (cf. e.g. [12]). Studies suggest that there is a well established yet hidden market for, e.g., zero-day exploits, malware tools, malware-as-a-service as well as for stolen data ranging from credit card data, financial data, employee credentials, compromising pictures or films to Netflix accounts or bonus cards [13].

Determining the necessary investments in IT security measures is far from obvious. The "Calculus of Negligence" suggests $PL > B$ where B is the cost of taking precautions, P is the probability of loss and L is the gravity of the loss. The product

$P * L$ must be a greater amount than B to create a duty of due care. This rule was coined by Judge Learned Hand [14].

The "Return on Security Investments" (ROSI) uses ((ALE*Mitigation ratio – Cost of solution)/Cost of Solution) to determine the return on investments. ALE is the annual loss expectancy [15]. ROSI assumes that investments mitigate risks and potential losses and can be utilized to compare the efficiency for security investments.

The renowned model by Gordon and Loeb allows to reason about the efficiency of security investments: "Our analysis shows that for two broad classes of security breach probability functions, the optimal amount to spend on information security never exceeds 37% of the expected loss resulting from a security breach (and is typically much less that 37%). Hence, the optimal amount to spend on information security would typically be far less than even the expected loss from a security breach." [16, 17].

These three methods for assessing the necessary investments all deal with rather low or unknown likelihoods and potentially huge damage and damages that can hardly be quantified. The question remains whether results of such economic models eventually trigger investments and the right decisions. Yet, there are critical infrastructures to which investments are more of a burden then in others. E.g. the health care sector - at least according to the German health care system - cannot just transfer the costs for IT security to medical bills. The energy sector is less restrained to transfer the costs to protect the infrastructure to its customers. Anyway, customers or end users are reluctant to pay for security and decision makers are equally reluctant to invest in topics that are not honored by the market.

However, discussions on cybersecurity as, e.g., on blackouts or fake news illustrate that cybersecurity has implications to split society. Prof. Dirk Heckmann coined the term "Concordization" for tragedies that – in analogy to the tragic accident of the Concorde that caused to stop not only all flights of the Concorde but defacto all developments of supersonic commercial airplanes – change the trust in technology and developments of technology [18]. Again, this is an argument that investments in cybersecurity should not be measured by economic means alone. Prof. Peter Burgess argued at the first conference of its|kritis in 2015 as keynote speaker for the notion of "social value" of critical infrastructure, i.e., critical infrastructures have the value that society ascribes to them. This underlines the strategic importance of politics and legislation in the domain of critical infrastructures. The subsequent section in this analysis is about society and how legislation addresses the topic of cybersecurity.

5 Strategies in Cybersecurity – Selected Examples

Cybersecurity is a topic of strategic relevance and both a regional and a global phenomenon: The first instances of malware (in the 80s of the past century) spread then globally – according to what was considered global at that time. In the 90s, number and variety of malware increased significantly and infections of mainly personal and desktop computers as Windows PCs, Macintosh, Atari and Amiga desktops spread. Today, the threat landscape of current malware is found to be differentiated with malware that may spread globally or that aims at a particular technology, say of one or

more manufacturers, of a particular system integrator or technology provider, or to target a particular region or nation state, a particular kind of organization or even a single organizations. E.g., Stuxnet as the first prominent malware designed to infect Industrial Control Systems (ICS) was designed to operate and spread in a particular region and address technology from one manufacturer [19]. Social engineering or ransomware that relies on (spear) phishing as primary attack vector relies on knowledge about language and processes as well as of the look-and-feel of forms or emails or a particular exploitation chain to monetarize or make other use of information collected by malware or control gained through malware. This means in practice that technology providers, manufacturers, sectors, region states need to develop capabilities to detect cyberthreats as novel malware or campaigns, to prevent attacks and respond to attacks – as the risk for any of these players could be different and because any of these actors need to provide information to detect and prevent attacks. In our case the strategies of nation states or economic regions are of particular interest as this shapes how authorities and private organizations work together in cybersecurity.

Nation states take different approaches to ensure security of critical infrastructures. This brief review summarizes work x from D. Kipker and Kipker & Müller in project VeSiKi [6, 20, 21]:

Germany implements a rather collaborative public-private partnership approach: the Federal Office for Information Security (cf. bsi.bund.de) is "the national cyber security authority" which "shapes information security in digitization through prevention, detection and reaction for government, business and society" as the central public institution for cybersecurity. "The UP KRITIS National initiative" implements the collaboration of critical infrastructures and public administration. The German IT Security Act [2] articulates the requirements for critical infrastructures: the need to report "critical" cyber incidents to the BSI, certify their measures and establish points of contact for authorities. The CRITIS directive defines thresholds which infrastructure providers are considered to be critical and critical infrastructure providers register themselves as critical infrastructures. These critical infrastructure operators are entitled to information and consultation on security issues. Sectors of critical infrastructures may define sector specific security standards to be approved by the BSI.

Other states employ different approaches. E.g., France uses a more centralized approach: the critical infrastructures are been determined in a process led by public administration. The strategic goal of the French national Digital Security Strategy articulates as the first one is "Fundamental interests, defence and security of State information systems and critical infrastructures, major cybersecurity crisis". (cf. article 22 of the French CIIP law ("Loi de programmation militaire 2014-2019")).[1] Europe's strategy for "An Open, Safe and Secure Cyberspace" represents EU's vision on how best to prevent and respond to cyber disruptions and attacks and articulates priorities[2]. The NIS directive requires the member states to have certain national cybersecurity capability, e.g. a national Computer Security Incident Response Team (CSIRT) and it

[1] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/information-systems-defence-and-security-frances-strategy.

[2] http://europa.eu/rapid/press-release_IP-13-94_en.htm.

requires cross-border collaboration between EU countries, e.g. the operational EU CSIRT network and national supervision of critical sectors.

The US strategy is articulated in the National Security Action Plan (CNAP) and the Executive Order 13636 "Improving Critical Infrastructure Cybersecurity" from 2013 articulates the measures for the protection of critical infrastructures, as e.g. information sharing between public authorities and critical infrastructure operators and facilitates self-regulation. Accordingly, the National Institute of Standards and Technology (NIST) published a "Cybersecurity Framework", with voluntary standards, measures and best practices in cybersecurity. The Cybersecurity Enhancement Act (2014) fosters a voluntary private-public collaboration. Sector specific regulations on federal level are, e.g., the Health Insurance Portability and Accountability Act (HIPAA, 1996) for health related data, the Financial Services Modernization Act (Gramm-Leach-Bliley Act, 1999) for personal financial data or the Federal Information Management Act (FISMA, 2002) for information processing in federal administration and the Cybersecurity Information Sharing Act (CISA, 2015) for sharing IT security relation information between private organization and administration. The Federal Trade Commission (FTC) is the central public authority in the Cyber Security Strategy.

Russia articulated with its second Cyber-Security-Doctrine in 2016 its response to the increasing cyber threat levels. The main focus of this doctrine is not so much on economic aspects but on political and military interests and it is connected with the national security strategy of the Russian Federation and its defense strategy. [6] The "Federal Law on Security of Critical Russian Federation Information Infrastructure" sets not only the frame for security of critical infrastructures, but also lays the foundation for a national IT security system, ranging from detection, prevention to the elimination of the aftereffects of cyber incidents. It defines rights and obligations to service providers as critical service providers take place in an information exchange with authorities and it defines an expansion of official control and instruction rights to review the new legal requirements. Among other, critical infrastructure providers inform public administration on cyber incidents and support public authorities in detection of the state of security, prevention and reaction to Cyber incidents.

In China, the Cybersecurity Law from 2016 and an additional catalogue for operational IT security measure articulate an approach to privacy and information security. Key network technology and services need to be certified in a national security review by the Cybersecurity Review Committee and the Cybersecurity Review Expert Committee in a public-private partnership.

The various cybersecurity strategies differ in scope and focus as well as in the role of public administration and private organizations. Minimum security standards throughout sectors and the preparation for more digitalization with more networked structures for information sharing and common operational pictures is common to all the national cybersecurity initiatives. The German approach relies on collaboration between public authorities and private organizations and therefore it is interesting to see what critical infrastructures do in cybersecurity and what they consider to be successful approaches. It is an open question to be answered in the future which approach will facilitate more innovation and creativity – to get ahead in the game of black hats vs. the white hats.

6 Security in Practice - the Case Study Series CASE|KRITIS Revisited

IT security in critical infrastructures is a complex topic that involves decision making about investments and the right balance in a strategy for human, organizational and technical security measures. This section revisits the CASE|KRITIS case study series [18, 22] to analyze the world of processes in IT security.

Case studies are considered to be a method to study complex, real world phenomena and therefore a suitable method to study IT security measures in critical infrastructures with technology, human factor and organizational processes. Focus of our case studies are business processes and the technology necessary to implement and support them. Our approach is inspired by the eXperience method for case studies [23]. The case studies were conducted from 2015 to 2017 and the cross-case study in 2017 and 2018.

6.1 The Cases of CRITIS

The nine cases with organization, title, case study authors and the case type (successful project, technology or organizational culture) together with a cross case analysis are summarized in Table 1. Note that one case study (Dairy) is anonymized. The cases are presented briefly below.

Table 1. The CASE|KRITIS case studies

	Title (original title)	Authors
Bundeswehr	Working Group IT-SecAsBw – How a working ground fosters IT Security Awareness inland and abroad (*AG IT-SecAwBw – Wie eine Arbeitsgruppe IT-Security Awareness im In- und Ausland fördert*)	A. Rieb, G. Opper
genua gmbh	Remote Maintenance in Critical Infrastructures *(Fernwartung Kritischer Infrastrukturen)*	A. Rieb
itWatch GmbH	A Secure Standard Process for Digital Crime Scene Photography with DeviceWatch (*Ein sicherer Standardprozess für die Digitale Tatortfotografie mit DeviceWatch)*	S. Lücking, S. Dännart
kbo	Balanced Risk Management for Sustainable Security *(Ausgewogenes Risikomanagement für nachhaltige Sicherheit)*	T. Kehr, S. Dännart
Dairy	IT Security in a Dairy: Family Tradition and High Availability (*IT-Sicherheit in der Molkerei: Familientradition und Hochverfügbarkeit*)	S. Dännart
PREVENT	IT Security for Business Processes in the Financial Sector: The Management Solution PREVENT *IT-Sicherheit für Geschäftsprozesse im Finanzsektor: die Managementlösung PREVENT)*	S. Rudel, T. Bollen

(*continued*)

Table 1. (*continued*)

	Title (original title)	Authors
SAP SE	Information Security at SAP SE: The Longest Human Firewall in the World *(Informationssicherheit bei SAP SE: Die längste Human Firewall der Welt)*	U. Lechner, T. Gurschler, A. Rieb
Stadt Gera	Coordination Center East Thuringia: IT-Security in a Coordination Center (*Zentrale Leitstelle Ostthüringen: IT-Sicherheit in einer Leitstelle)*	T. Gurschler, A. Rieb, M. Hofmeier
ugarbe software	Information Security with ClassifyIt: Information Security through Digital Classification of Documents and Emails (*Informationssicherheit durch ClassifyIt: Informationssicherheit durch gestützte Klassifizierung von Dokumenten und E-Mails)*	A. Rieb

The case **"Working Group IT-SecAsBw – How a working ground fosters IT Security Awareness inland and abroad"** is about an IT security awareness campaign: Key visual of the campaign is a power plug with the symbol of a face – a symbol that IT security is both about technology measures and the human factor alike. The PIA campaign exemplifies a collaborative, longitudinal IT security activity with a tradition to engage IT security staff and with a minimum of dedicated resources.

Case **"Remote Maintenance in Critical Infrastructures"** tackles with remote access for maintenance one of the 10 most relevant IT security topics in Critical Infrastructures according to BSI [24]. The remote, secure login for maintenance purposes is the core process considered in the case study. Remote access via a single interface, the functionality to control and monitor "sessions" for remote maintenance increases the security level of critical infrastructures. The single interface for all maintenance service providers and all service operation decreases complexity in securing remote access while the solution is easy to integrate in existing IT landscape in a critical infrastructure.

The case **"A Secure Standard Process for Digital Crime Scene Photography"** presents an innovative secure-by-design solution for crime scene photography and the handling of digital crime scene photos in police work. Police officers may use any digital camera, the photos are watermarked with a signature when transferred in the police information system such that authenticity of pictures is maintained throughout police work. Amortization took only three years and the new process is considered to be modern as well as user friendly as it saves time and resources.

Case **"Balanced Risk Management for Sustainable IT Security"** analyses the reaction to ransomware threats against hospitals. While the first reaction to an imminent ransomware was a complete separation of the hospital from the Internet, the hospital established to a more refined strategy later with a considerable speed up of IT security processes and an increased priority for IT security investments. The novel process of security incident response includes all stakeholders in the hospital as well as external service providers. Joint responsibility for IT security measures as well as a proved and tested communication policy rounds up the process. A few months after the process

was first implemented in the reaction to the ransomware threat: the hospital group was successful in the defense against a considerable threat.

Case **"IT Security in the Food Industry: Tradition and High Availability"** reports on a safety and security culture of a family owned dairy in a rural area. The processing of sensitive primary products as raw milk requires high availability of production lines. The case is about the strategy of the CIO – he integrates traditional organizational and modern IT security measures in a successful digitalization strategy. Cornerstone of his strategy are close relations to IT staff, the integration of IT staff and technicians into one team with uniform IT inspired processes, training of staff and the loyalty of staff over generations to the company as the main employer in town. Employees practice essential IT security routines as e.g., restoring data from backups in their daily work, new IT technology is only implemented when staff feels confident to handle disruptions and IT staff is encouraged to identify and experiment with potentially useful IT innovations. The case explores also IT security measures to ensure high availability as real time backups of the core SAP system or VLan encapsulation of production lines.

The case **"IT Security for Business Processes in the Financial Sector – The Management Solution PREVENT"** demonstrates real-life complexity of a comprehensive enterprise level risk management. In this case study, the business process is the unit of analysis in risk management. The underlying business case is a (fictitious) computing center of a bank that provides business processes as a service to several (fictitious) client banks. The risk management approach comprises a unified way to source all risk relevant data and a collection of tools (simulations, analytic methods) for risk analysis. The case exemplifies the novel risk management approach which an analysis of interdependencies between infrastructure, information system and business process level. The case argues about the advantages such a comprehensive risk management and the business models for which such a comprehensive risk management is a prerequisite.

"Information Security at SAP SE: The Longest Human Firewall in the World" is a case study on the information security campaign at SAP SE. Key visual of the campaign is a chain of SAP employees with a group handshake with crossed arms – a symbol for the joint effort to protect the company. Employees take part in an individual (mandatory) information security training and can then become part of the human firewall with a picture and an individual statement on information security. The case study highlights the pivotal role of employees in information security and that information security eventually benefits from "fun" but also from perseverance.

Case study **"Coordination Center East Thuringia: IT-Security in a Coordination Center"** discusses availability of emergency services: The alarm process from an emergency call to alerting the emergency services need to be available despite outage of IT components. The case study presents fallbacks and redundancies as well as IT security concepts to ensure highest availability of the emergency number 112 with emergency services. It addresses questions in the further development of information and communication technologies in a coordination center of emergency services. Success factors are the volition of staff not only to use but to understand the infrastructure with its technologies and to get to the bottom of any problem to solve it.

Case **"Information Security by Digital Classification of Documents and E-Mails"** is about a tool to ensure confidentiality of information. ClassifyIt is a PlugIn for Microsoft Office that support users in the classification of documents and emails. Together with a firewall it ensures that only documents and emails with adequate classification can leave the organization and that encryption that is adequate for the document is used for sending it via email. The software is distributed via standard software distribution tools, and it can be customized individually, interfaces for users and administrators are perceived to be user friendly and it needs no Internet connection.

The nine cases illustrate strategic decisions made by critical infrastructure providers and operators. They illustrate that the field of IT security provides a plethora of challenges for novel technical or organizational measures and that technologies, processes, leadership and strategy matter in the domain of Cybersecurity. What distinguishes these projects that can be considered good or best practices? This question is to be answered in a cross-case analysis in the subsequent section.

6.2 Success Factors for IT Security in Critical Infrastructures

This section presents selected topics from the cross-case analysis to identify success factors beyond the apparent contribution to IT security. For the paper at hand we selected codes and arguments from the full cross case analysis presented in [18] and focus on the topics of risk response and the human factor (cf. Sect. 3).

The first analysis perspective is the one on risk perception (cf. Sect. 3). We have looked for information in how far IT security is being measured and what we can learn from the cases on risk management. This perspective is captured in the code "**Measurement of IT Security".** To be able to measure or assess the level of IT security is an important capability – critical infrastructure operators as well as public institutions look actively for methods and tools to "measure security".

The cross-case analysis identifies various perspectives: The case on the "Management Solution PREVENT" exemplifies the complexity of a comprehensive risk assessment. The SAP case illustrates that measurements of the level of IT security can be relatively simple (SAP uses only a couple of questions) – what matters is perseverance over several years to see how the level of security changes over time. However, measuring security to increase the level of security seems not to be the main driver in the cases: It is a qualitative assessment of vulnerabilities and the need to address them that is the dominant pattern throughout the cases.

The economic perspective is captured in code "**Cost efficiency of IT security measures"**. Cost efficiency of IT security measures is an important factor in particular for the small and medium sized critical infrastructure operators. The cases offer different perspectives on cost efficiency and investments: The case on the Secure Standard Process for Digital Crime Scene Photography by itWatch is on a secure-by-design solution and this case study is the only one that reports on return of investment: the new process is more efficient than the "old, analogous" way of handling photographs. The case study on the Toolbox for an awareness campaign argues first, that such a toolbox is more cost efficient than individual campaigns developed from scratch and costs for running the working group and providing awareness campaign material are reasonable. The cases on IT security products (Remote Maintenance, ClassifyIt by ugarbe.de

software) argue with limited costs for trainings and –qualitatively– that well designed solutions, solutions with little integration and training efforts and with standard processes have economic advantages in the long run.

A second code that captures the economic perspective is "**Simplicity of IT security measures".** No one wants "over-complex" security projects – this is common sense – and ideally, successful IT security projects should be simple, in particular as small and medium-sized critical infrastructure operators are reluctant to adopt seemingly "complex" measures. The code "simplicity of measure" in the cross case analysis captures the resources necessary to implement and operate IT security measures. The coding and the inductive analysis process identify three criteria as the ones that are used in practice to capture "simplicity": (1) user friendliness (2) implementation effort and (3) training effort for end users, IT staff as system administrators. These three criteria are the ones of which our interview partners are proud of as technology providers or as security experts and which they consider to be success factors in cybersecurity.

Other codes analyze interdependencies between security solutions and other information systems and their processes and the analysis identifies little interdependency as a success factor as well as the prerequisites, i.e., the "homework that needs to be done" to make a solution effective. The trade-off between availability and IT security of the IT landscape is a core topic in case "Stadt Gera" and availability is also the driver in the design of the whole security organization in case "Dairy". The cases Dairy and SAP and the case of the research project PREVENT illustrate the size and complexity of IT security solutions: the leadership necessary to take a family owned business into the digital age with the necessary level of security, the fun and effort to raise awareness in a global organization and the complexity of collecting and analyzing data for risk management at business process level in the research of project event. This leads us to the next section of future security, i.e. on research projects in the domain of cybersecurity.

7 The State of the Art in Cybersecurity – Selected Results and Experiences from Research in itskritis

The cases focus on successful projects and the case analysis identifies simplicity and costs as important factor – the projects of the research program have been selected for research on systemic approaches to IT security. The State-of-the-Art [25] summarizes selected results from the research program itskritis with its thirteen projects (cf. Sect. 2). In this brief and eclectic review we emphasize again the topics risk perception and response.

The IT security topics particular to the domain of Cybersecurity with its industrial control systems and its particular focus on availability of products and services is addresses by several projects: PortSec develops methods to analyze and increase dependability of the software hubs in ports that process incoming and outgoing messages. These pieces of software are to some extent legacy, heterogenous and with software architectures from times, in which dependability and security were less of importance. Furthermore, they operate in an open setting with connections to other hubs and technology. Methods to analyze and retrofit such complex software projects

are crucial not only in the port use case. Project INDI develops methods and tools to monitor networks with protocols from the pre-Internet era to analyze whether communication is compliant with the protocols. Project SURF uses trusted elements to harden devices and develop an holistic approach to increase the level of security as well as an holistic information security approach.

The risk perception, risk assessment and the risk response are the core research results of several research projects. Project SecMaaS goes beyond technology and develops concepts and tools for security services in the domain of public administration. Tools that allow risk assessment to provide services are a essential contribution by SecMaaS. Mosaic does the risk analysis at architecture level and provides respective methods and tools. The solutions of project Aqua-IT-Lab include a method and tool for self-assessment of the level of security that provides recommendations for methods necessary to reach the sector specific state of the art in IT security. This research by project Aqua-IT-Lab is done in particular for the sector water with the many small and medium sized water suppliers in Germany in mind. Project SICIA assess the level of risk from components, relates these risks via connectedness graphs and allows a comparative and time series analysis. This research was done with the complexity of energy plants and energy sector in mind. The approach of project ITS.APT addresses the risks of end users and employees in the open setting of hospitals and provides an innovative concept and solution for testing awareness of users: software that emulates attacks as phishing is being deployed and users experience attacks and typical malware behavior and the test allow to analyze the cybersecurity awareness of users, i.e., will they identify malware, abnormal behavior of their computer and report to the service desk for security incident response. The method of project RiskViz relies on a search engine to identify devices on the Internet or Intranet and relate this information to vulnerabilities databases and other information sources, as well as methods from the risk assessment in insurance industry that allows to determine the level of risk for critical infrastructures. Project Sidate provides a networking platform for small and medium sized critical infrastructure providers and tools to assess the level of security and provide recommendations. The systemic projects of itskritis facilitate a risk assessment and relate the abstract risks to concrete IT security measurements or measures.

A brief presentation of one of VeSiKi's research results, the IT security game series "IT-Matchplays" with the games Operation Digital Chameleon, Operation Digital Owl and Operation Digital Snake concludes the review of research results. Red and blue teams develop attack chains and IT security measures. Figure 6 depicts the game board with typical IT components of a critical infrastructure.

The red team's task is to develop an attack against the critical infrastructure protected by the blue team. Team red chooses a threat actor as a role and they declare a goal related to their role. In addition to that, red teams are instructed to justify their attack before designing their attack chain and before deciding on a goal. I.e. red teams have to think about motivation and technique of neutralization of the threat actor that they enact. The blue team knows which kind of actor is going to attack. The development of attack chains and defense strategies is followed by a presentation and the decision about which team(s) win(s). Red teams present goal, technique of neutralization and attack chain. Results of teams red and blue are assessed in a group

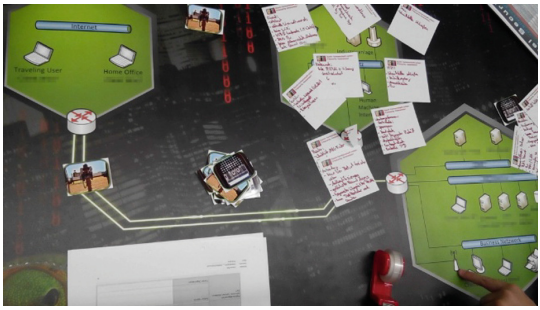

Fig. 6. The board of "Operation Digital Chameleon"

discussion led by the game master regarding plausibility of the concepts with the chosen threat actor and feasibility. The gaming phase is followed by a debriefing which aims to solicit emotions, proposals on improvements of the gaming experience, and a self-assessment of IT security awareness levels. A discussion of the threat actor including their attacks and team blue's defense strategies is part of the debriefing. For more details regarding the model of the game, see [26]. This game allows to analyze the level of awareness and to raise awareness about concerns of IT security specialists about current tools and procedures. Furthermore, it allows to make intangible, weak signals about forthcoming topics tangible and a look ahead – by thinking out of the box in a creative format. We argue that the technology implements smart decision architectures and give impulses to assess risk and react in a future oriented way.

8 Summary

IT security for critical infrastructures is an enticing field – the level of security needs to be increased and we argue that this is a societal challenge. Risk perception and risk response are considered to be inherently difficult – they can be considered human factors for the domain of critical infrastructures. The article briefly reviews selected economic models which seem to fall short in supporting adequate decision making and risk response. The various strategies of regions and state take different society approaches to cybersecurity and it remains open, which strategy eventually fosters innovation and creativity beyond networking and information sharing. The results from the case study series illustrate experiences from practice in Cybersecurity projects while the results of the project illustrates the future dimension of systemic approaches to cybersecurity. Risk reaction and risk response are the focus in this brief and very subjective review. The security of critical infrastructures currently is a relevant topic, yet novel approaches and more research is needed for creativity to change the white hat vs. black hat games and to develop a better understanding for today's challenges.

Acknowledgements. This research is funded by the German Federal Ministry of Education and Research under Grant Number FKZ: 16KIS0213K.

I would like to thank all case study partners and interviewees for the insights as well as our project partners from VeSiKi and our fellow projects from ITS|KRITIS for their engagement in the collaborative research process of itskritis. I am indebted to the VeSiKi Team and in particular Steffi Rudel as well as Sebastian Dännart, Andreas Rieb, Thomas Diefenbach, Tamara Gurschler, Manfred Hofmeier, and Tim Reimers as well as Kathrin Möslein, Albrecht Fritzsche, Max Jalowski, Matthias Raß, Benedikt Buchner and Andreas Harner for their work on the research results of VeSiKi and itskritis. Dennis Kipker and Sven Müller contributed with their work on norms, standards and Cybersecurity law in VeSiKi to this article.

References

1. BSI - Critical Infrastructure Protection in Germany. https://www.bsi.bund.de/EN/Topics/Criticalinfrastructures/criticalinfrastructures_node.html
2. Bundesgesetzblatt: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz, Bundesgesetzblatt Jahrgang 2015 Teil I Nr. 31) (2015)
3. Loch, K.D., Carr, H.H., Warketin, M.E.: Threats to information systems: today's reality, yesterday's understanding evolution of computer security. MISQ. **16**, 173–187 (1992)
4. VeSiKi: Monitor IT-Sicherheit Kritischer Infrastrukturen. Universität der Bundeswehr München, Neubiberg (2017)
5. Lechner, U.: Monitor 2.0 IT-Sicherheit Kritischer Infrastrukturen (2018)
6. Kipker, D.-K., Müller, S.: Internationale Cybersecurity-Regulierung (2018)
7. Rieb, A., Gurschler, T., Lechner, U.: A gamified approach to explore techniques of neutralization of threat actors in cybercrime. In: Schweighofer, E., Leitold, A., Mitrakas, A., Rannenberg, K. (eds.) APF 2017, vol. 10518, pp. 87–103. Springer, Heidelberg (2017). https://doi.org/10.1007/978-3-319-67280-9_5
8. Badke-Schaub, P., Hofinger, G., Lauche, K.: Human Factors - Psychologie sicheren Handels in Risikobranchen. Springer, Heidelberg (2012)
9. Thaler, R.H., Sunstein, C.R.: Nudge: Improving Decisions About Health, Wealth, and Happiness. Yale University Press, New Haeven (2008)
10. Norton, M., Mochon, D., Ariely, D.: The "IKEA Effect": When Labor Leads to Love (2011)
11. Bhanu, Y., et al.: A cyberthreat search process and service. In: Proceedings of the 2nd International Conference on Information Systems Security and Privacy, ICISSP 2016 (2016)
12. Ponemon Institute and Accenture: 2017 Cost of Cyber Crime Study, p. 56 (2017)
13. McFarland, C., Paget, F., Samani, R.: The hidden data economy - the marketplace for stolen digital information (2015)
14. Brown, J.P.: Toward an economic theory of liability. J. Legal Stud. **2**, 323–349 (1973)
15. Enisa: Introduction to Return on Security Investment, p. 18 (2012)
16. Gordon, L.A., Loeb, M.P.: The economics of information security investment. ACM Trans. Inf. Syst. Secur. **5**, 438–457 (2002)
17. Gordon, L.A., Loeb, M.P., Zhou, L.: Investing in cybersecurity: insights from the Gordon-Loeb model. J. Inf. Secur. **07**, 49–59 (2016)
18. Lechner, U., Dännart, S., Rieb, A., Rudel, S.: IT-Sicherheit in Kritischen Infrastrukturen: Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen. Logos Verlag, Berlin (2018)
19. Zetter, K.: Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Broadway Books, Portland (2015)
20. Kipker, D.-K.: VPN-Tunnelabschaltung und „ Chinese Cybersecurity Law " – wohl mehr Mythos als Realität. DuD - Datenschutz und Datensicherheit **42**(9), 574–575 (2018)

21. Kipker, D.-K.: Pläne für ein Datenschutzgesetz in Indien: Untersuchung des White Paper des Expertenkomitees (2018, to appear)
22. Dännart, S., Diefenbach, T., Hofmeier, M., Rieb, A., Lechner, U.: IT-Sicherheit in Kritischen Infrastrukturen – eine Fallstudien-basierte Analyse von Praxisbeispielen. In: Drews, P., Burkhardt, F., Niemeyer, P., Xie, L. (eds.) Konferenzband Multikonferenz Wirtschaftsinformatik 2018: Data driven X - Turning Data into Value. Leuphana Universität Lüneburg, Lüneburg (2018)
23. Schubert, P., Wölfle, R.: The experience methodology for writing IS case studies. In: Americas Conference on Information Systems, pp. 19–30 (2006)
24. BSI: Industrial Control System Security: Top 10 Bedrohungen und Gegenmaßnahmen 2016 (2016)
25. Lechner, U., Rudel, S.: IT-Sicherheit für Kritische Infrastrukturen. Ergebnisse des Förderschwerpunkts IT-Sicherheit für Kritische Infrastrukturen ITS|KRITIS des BMBF. VeSiKi - Vernetzte IT-Sicherheit Kritischer Infrastrukturen (2018)
26. Rieb, A., Lechner, U.: Operation digital chameleon – towards an open cybersecurity method. In: Proceedings of the 12th International Symposium on Open Collaboration (OpenSym 2016), Berlin, pp. 1–10 (2016)