Elicitation of Requirements for an inter-organizational Platform to Support Security Management Decisions

J. Dax[2], B. Ley[2], S. Pape[1],C. Schmitz[1], V. Pipek[2] and K. Rannenberg[1]
[1] Goethe University Frankfurt, Chair of Mobile Business & Multilateral Security, Germany
[2] University of Siegen, Institute of Information Systems, Germany
e-mail: {julian.dax; benedikt.ley; volkmar.pipek}@uni-siegen.de
{sebastian.pape; christopher.schmitz; kai.rannenberg}@m-chair.de

Abstract

Due to new regulations in Germany energy providers are required to obtain IT security certificates. Especially small and medium-sized energy providers struggle to fulfill these new requirements. Since most of them are in the same situation, we are dealing with the question on how to support their collaboration using a web-based platform. We elicited criteria from energy providers on how such a platform should be designed to support them. The main contribution is a set of requirements for the collaboration platform along with the implications for its implementation. The focus of this work is not on technical innovation but on how existing technologies and best practices can be adopted for the needs of small and medium-sized energy providers.

Keywords

Usable Security, Security Management, Security Assessment, Security Perception

1. Introduction

The European Program for Critical Infrastructure Protection (EPCIP) was recently implemented in national laws in Germany. The IT security law requires providers of critical infrastructures to get certifications for their security. This especially concerns energy providers as they also have to comply with industry-sector-specific regulations laid out in the Energy Industry Act (EnWG). There is no de minimis rule if the definition for critical infrastructure is fulfilled. As a consequence, in particular small and medium-sized energy providers struggle to fulfill the requirements. Compared to larger providers, they have the handicap that there is a low budget for IT security and that no experts for IT security are employed there. One of their first challenges in order to meet the criteria is to introduce an information security management system (ISMS). Most of the providers mainly do this to comply with the new regulation. When the ISMS is put to work, the energy providers should make use of it to monitor and improve the IT security of their systems.

Most of the energy providers are uncertain how to start and may need to hire external consultants to support them. The aim of the project SIDATE is to support them to continuously improve their security. Since many of the small and medium-sized energy providers face very similar challenges, a natural solution to support them is to stimulate inter-organizational collaboration. This should be done by building an inter-organizational collaboration platform for energy providers. The platform should enable the energy providers to share their knowledge about IT security in a structured way.

In this paper, we describe the requirements elicitation process with the energy providers. We aimed to engage them very early in the design process. It showed that many of the criteria are not domain-specific for energy providers. Therefore, we believe that other domains can profit from those criteria as well. Our contribution is a set of requirements for the collaboration platform along with the implications for its construction.

The remainder of this paper is organized as follows: Section 2 discusses related work. Section 3 describes the used methodology. Section 4 sketches the results of the first workshop with the energy providers. The planned modules for our collaboration platform are shown in Sect. 5. In Sect. 6, we describe the design criteria for the collaboration platform collected from energy providers.

2. Related Work

2.1. Collaboration platforms and expertise sharing

The “endeavor to understand the nature and characteristics of cooperative work with the objective of designing adequate computer-based technologies.“ (Bannon & Schmidt 1989) has always been the aim of Computer Supported Cooperative Work (CSCW). Therefore, collaboration platforms have been a major field of research in CSCW. Inside this field, the aspect of inter-organizational needs for such platforms can be studied. While ‘inter-organizational information systems’ (IOIS) are automated information systems shared by two or more organizations (Cash & Konsynski 1985), CSCW applications provide “capabilities beyond simple information access to facilitate communication and collaboration among partners” (Drury & Scholtz 2005). The term ‘knowledge sharing’ is used for artifact-centered studies, while the communication-centered ‘expertise sharing’ focuses on the actor (Ackerman et al. 2013). Further, expertise sharing focuses on the “self-organized activities of the organization’s members and emphasizes the human aspects” (Ackerman et al. 2013). There have been a number of studies of expertise sharing in CSCW in different fields of application: For example, Doherty et al. (Doherty et al. 2012) studied inter-organizational coordination mechanisms in software development and Hobson et al. (Hobson et al. 2011) studied the information sharing needs and practices in municipal governments. Bharosa et al., (Bharosa et al. 2010) conducted a study on multi-agency disaster response and identified the problem that “actual level of information sharing across different organizations is often limited, although it is being promoted”. For energy providers the German association of municipal corporations "Verband kommunaler Unternehmen" (VKU) offers an efficiency comparison/benchmark, but unfortunately no online platform is offered.

2.2. Shared Risk Analysis, ISMS and Stakeholders' Engagement

Karlsson et al. (Karlsson et al. 2015) regard ISMS to manage information systems in inter-organizational collaborations. The difference to our use-case is, that the energy providers do not collaborate in the sense of sharing business processes. The reason for them to use our collaboration platform would be that they face the same challenges and are able to exchange experiences. Faily (Faily 2014) reports on engaging stakeholders in the design of a secure system. Our platform also aims to engage the stakeholders; not on the system itself but rather on sharing experience and expertise on how to design secure systems.

When it comes to implementing information security policies in organizations, Arif (Arif 2011) studied five factors which determine the willingness to comply with these policies: culture, awareness, training, risk perception and re-enforcement. In his study, the cultural factor was the most impactful. Reichard et al. (Reichard et al. 2011) studied barriers to the successful implementation of such policies and how to overcome them. Like Arif, they stress the importance of a “security culture” in the organization. Moreover, they stress the need for collaborative implementation of such policies. Another related factor in the successful introduction of IT-security policies identified by Reichard et al. is that the principles and benefits of IT-security have to be communicated and “sold” to the organization.

Apart from that, in the US the concept of Information Sharing Analysis Centers (ISACs) can be found. Those non-profit organizations gather and analyze IT security-related information within critical infrastructure sectors (e.g. electricity) and provide analysis results, security strategies and general information to their members. In contrast to that, our approach focuses more on the individual assessing and benchmarking of the energy provider's security level (ISAC Council 2004).

3. Methodology

In order to elicit the target group-specific requirements, three two-hour workshops with different stakeholder groups were conducted. In total, eleven experts from eight energy providers attended the workshops. Most participants were IT security officers or IT managers from energy providers, but also representatives from national interest groups were present.

Seven experts from six different energy providers attended the first workshop. After an introductory talk by the organizer, each of the attendees introduced themselves based on a short questionnaire which addressed, for instance, general characteristics of their company and their experience in IT security. Afterwards, the experts were invited to discuss the platform’s requirements and their expectations in a moderated discussion.

The workshop’s results were subsequently discussed in an additionally internal design workshop, where eight members from the project partners were involved. As a result, several mockups visualizing the platform’s functionalities were sketched.

In another workshop, five experts from six energy providers attended as well as three employees from two interest groups. After the mockups had been presented, the discussion which was moderated by using the card-technique, was opened. The participants were asked to formulate the platform's must-have and nice-to-have requirements on different colored cards. After 10 minutes, the cards were collected and sorted in content-related clusters on a pin board. Then, all cards were discussed in an open discussion.

4. Energy Providers' Needs

Before we started to design our platform, we collected the energy providers' requirements for a collaboration platform. Our assumption was that for the communication between the energy providers, a web-based solution which allows asynchronous communication is most helpful. Mainly, because there is no need to install additional software which lowers the threshold to participate. This was confirmed by the energy providers during the workshop. The following modules were considered helpful by the energy providers: a wiki, a forum, a questions and answers module, a glossary, training modules for further education for security officers and other employees, checklists, a place to exchange documents, benchmarks, security assessment modules and a general module to support the launch of an ISMS.

5. A Platform Supporting Security Management

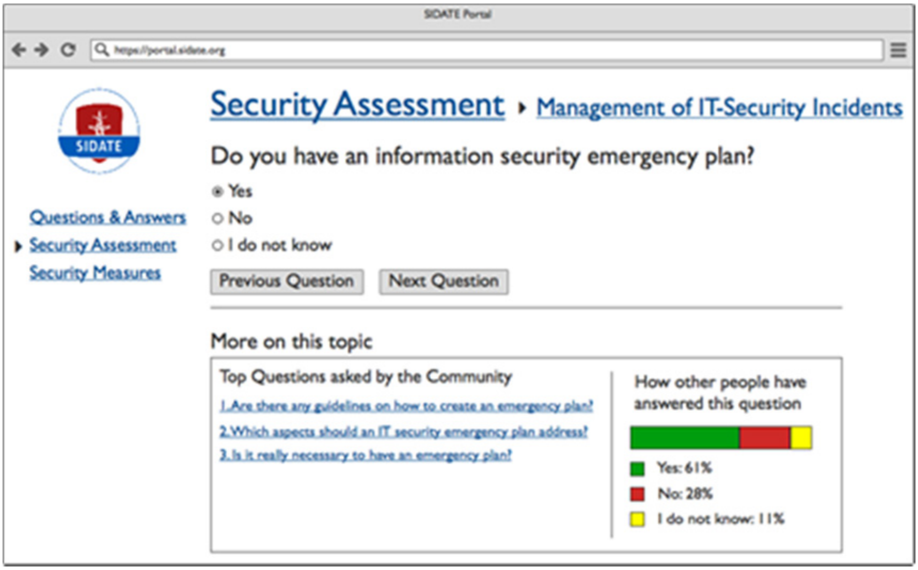
From the results of the first workshop with the energy providers, we inferred that the most relevant modules for the energy providers which should be implemented in the 1st iteration are:

- A security assessment module, which allows the energy providers to get feedback about their security level.
- A security measures module, which provides information and recommendation to energy providers about measures which they can implement in order to strengthen their IT-security.
- A question and answer module.

All modules should allow the energy providers to give feedback and exchange their experiences. We describe them below:

5.1. Security Assessment Module

The security assessment module follows a questionnaire-based quantitative methodology (Frangopoulos et al. 2014). The module allows energy providers to perform a self-assessment in order to assess and to improve their current IT security level. This is done by answering an online questionnaire which is provided on the proposed platform (see figure 1). The answers of other energy providers to these questions are also shown in aggregated form in order to allow the user to compare his/her organization to others. Additionally, the best rated questions asked by other community members related to the current topic are also shown.



SIDATE Portal

https://portal.sidate.org

Security Assessment ▸ Management of IT-Security Incidents

Do you have an information security emergency plan?

● Yes
○ No
○ I do not know

More on this topic

Top Questions asked by the Community

1. Are there any guidelines on how to create an emergency plan?
2. Which aspects should an IT security emergency plan address?
3. Is it really necessary to have an emergency plan?

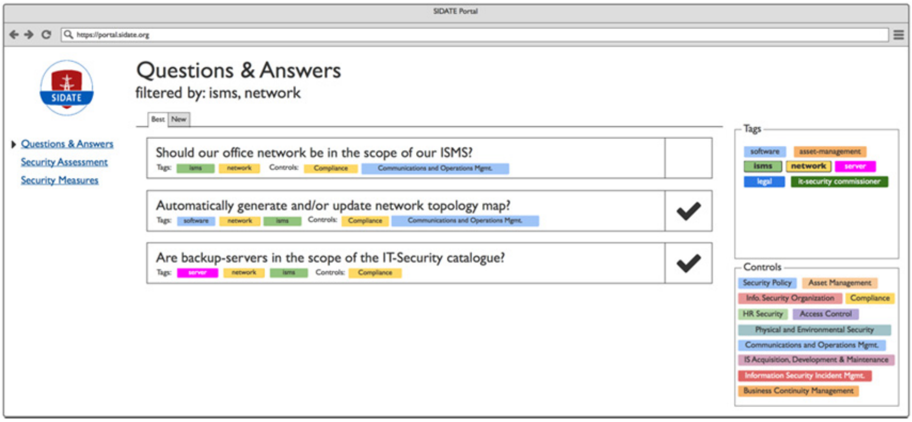
How other people have answered this question

🟩 Yes: 61%
🟥 No: 28%
🟨 I do not know: 11%

Figure 1: Mockup of the Security Assessment Module

5.2. Question and Answer Module

In the questions and answers module registered users can ask questions related to IT-security. These questions can be categorized by tags and be assigned to ISO/IEC 27002 controls.



SIDATE Portal

https://portal.sidate.org

Questions & Answers
filtered by: isms, network

Should our office network be in the scope of our ISMS?
Tags: isms network Controls: Compliance Communications and Operations Mgmt.

Automatically generate and/or update network topology map? ✓
Tags: software network isms Controls: Compliance Communications and Operations Mgmt.

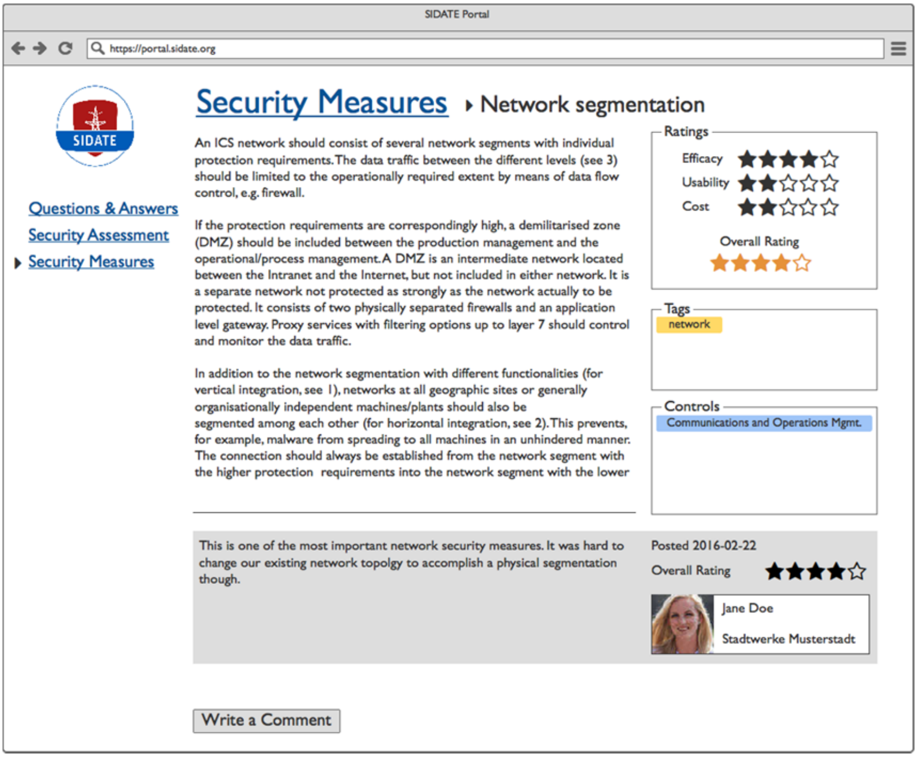
Are backup-servers in the scope of the IT-Security catalogue? ✓
Tags: server network isms Controls: Compliance

Figure 2: Mockup of the Questions and Answers Module

A side bar on the right (see Figure 2) allows users to select these tags and controls to filter the questions. Questions can be answered by other users, and answers can be marked as correct by the user who posted the question. Additionally, questions and answers can be rated and either sorted by rating or creation date.

5.3. Security Measures Module

The security measures module is a catalogue of security measures, which is maintained by security experts. Each security measure is categorized by one or more tags and assigned to one or more specific ISO/IEC 27002 controls. Users can comment on the measures and rate them according to their costs, efficacy and usability.



Security Measures ▸ Network segmentation

An ICS network should consist of several network segments with individual protection requirements. The data traffic between the different levels (see 3) should be limited to the operationally required extent by means of data flow control, e.g. firewall.

If the protection requirements are correspondingly high, a demilitarised zone (DMZ) should be included between the production management and the operational/process management. A DMZ is an intermediate network located between the Intranet and the Internet, but not included in either network. It is a separate network not protected as strongly as the network actually to be protected. It consists of two physically separated firewalls and an application level gateway. Proxy services with filtering options up to layer 7 should control and monitor the data traffic.

In addition to the network segmentation with different functionalities (for vertical integration, see 1), networks at all geographic sites or generally organisationally independent machines/plants should also be segmented among each other (for horizontal integration, see 2). This prevents, for example, malware from spreading to all machines in an unhindered manner. The connection should always be established from the network segment with the higher protection requirements into the network segment with the lower

Ratings
Efficacy ★★★★☆
Usability ★★☆☆☆
Cost ★★☆☆☆
Overall Rating
★★★★☆

Tags
network

Controls
Communications and Operations Mgmt.

This is one of the most important network security measures. It was hard to change our existing network topolgy to accomplish a physical segmentation though.

Posted 2016-02-22
Overall Rating ★★★★☆
Jane Doe
Stadtwerke Musterstadt

Figure 3: Mockup of the Security Measures Module

6. Elicitation of Criteria for the Fundamental Platform Design

In the second workshop with the energy providers, we presented the created mockups to the participants to show the possible functionality of the proposed platform. Then we asked them to write down mandatory and nice-to-have requirements the platform has to fulfil to be usable for them. We got 28 individual answers that we could cluster into four major categories: *(1) platform members, (2)* *confidentially/data privacy, (3) integration into exiting workflows, (4) general usability of the platform*. After we had clustered the participants' answers, we discussed each category to expose the motivations behind the requirements and initial approaches to solution.

6.1. Platform Participants and Data Privacy

The categories *platform members* and *confidentially/data privacy* were discussed together because of several overlaps between both categories. As expected, we could determine that participants had essential concerns about the privacy in respect to sensitive IT-security related data they would share across the platform. However, these concerns basically did not refer to the platform itself or its operator but to other platform members.

While it seems to be acceptable to share information with other energy providers, respectively their employees, participants were worried about the participation of external experts like information security consultants or lawyers. Even if they see an advantage in the qualified and skilled feedback from such persons, we discovered two significant concerns we have to deal with. (1) External experts could misuse the platform for advertising purposes and could flood energy providers with personalized offers based on the platform content. (2) Non-reliable platform members could use the visible content and questions by individual energy providers to identify and make use of possible security flaws.

Based on these initial insights, we developed and discussed several approaches with the workshop participants in order to find possible solutions that protect the energy providers' data and identity on the one hand and make use of the expertise from third parties on the other hand. While some of the approaches that are listed below are mutually exclusive, others complement each other.

- It is necessary that the platform supports **restricted and moderated access** for new members. Individuals or organizations that intend to participate to the platform need to be validated by the platform operator and have to agree to suitable terms of use in order to get access.
- Different UI views based on the user's organization and role could be used to **anonymize individuals and organizations** to external experts. While energy providers are able to see each other's questions, answers and other activities, other participants can only see the content but not the corresponding author. Energy providers should be able to rate the experts' contributions in order to improve their reputation. Instead of getting unwanted advertising, the energy providers can now proactively inquire consultancy service based on the experts' reputation.
- Instead of giving experts access to the platform, energy provides should be able to mark their contribution as *expert approved*. This means that the contribution rests on the result from consultancy service or legal advice the respectively user made use of before. This approach completely excludes

third parties from the platform and only allows the **indirect passing of expert's assessments and opinions** via the energy providers.

- As reliable organizations, the **interest groups for energy providers could undertake the role of experts** on the platform and contribute to energy providers' questions. However, the participating representatives of the interest groups in the workshop made clear that they do not have profound expertise to give sufficient answers to all questions. The only practicable approach is that they inform about legal changes and regulations on information security for energy provider.

6.2. Integration into Existing Workflows

The aim of the platform is to support participating energy providers to improve their information security and fulfill legal regulations. Thus, another important topic we have discussed with the workshop participants was that the effort they have to put into using the platform must not exceed the potential benefit. Several requirements given by the participants dealt with the question on how can the platform and its functionality be integrated into users' existing workflows.

- As a result from the self-assessment module the platform should provide individual **checklists and tools** that help the users' implementing required information security measures. In a first step this should predominantly aim at the fulfillment of statutory provisions (in case of energy providers in Germany the implementation of an ISMS according to ISO/IEC 27001).
- The self-assessment should also contribute to **internal information security audits**, e.g. the regular validation of measures and processes.
- It should be possible to **export results** from self-assessment to reuse them for internal reports (e.g. to be presented to the management) or other processes and workflows like the information security related controlling.

6.3. General Usability of the Platform

The remaining requirements that came up during the workshop focused on the general usability and will only be described briefly here because of their generality. Essentially the participants expect that the content on the platform is well-structured and maintained. There should be a moderator who leads discussions to an outcome, ensures that new topics/questions are created in the right section and prevents duplicates. Also the platform has to be up to date and deprecated content needs to be marked as such.

7. Conclusion and Future Work

Due to new regulatory requirements for critical infrastructures, especially small and medium-sized energy providers struggle to get their IT security certified. Because they face very similar challenges, we proposed a new concept for a collaboration platform in order support them to collaboratively improve their IT security.

To elicit the specific requirements of how such a platform should be designed, we conducted workshops with different stakeholder groups. As a result, we identified a set of functions and requirements which the platform has to fulfill.

There are three elementary modules. A central role plays the security assessment module for assessing and benchmarking the energy provider's security level. The second module is the security measures module which describes the most relevant IT security measures including the practical experiences by other energy providers. Finally, there is the questions and answers module which allows them to share their experiences with both other energy providers as well as with external experts.

Because the platform processes highly sensitive data, aspects in regard to data privacy have a very high priority for the stakeholders. This includes, for instance, having different UI views to anonymize individuals and organizations to external experts, and having a restricted and moderated access for new members. Also the integration into existing workflows plays a central role. For example the self-assessment should provide individual checklists and tools according to the ISO/IEC 27001 and should contribute to the internal information security audit. Besides that, the general usability of the platform was mentioned as essential requirement.

The next step is to implement the proposed concept and to iteratively refine the platform's functions based on user feedback. As future work, it would be interesting to analyse to what extent the platform can be transferred to other domains.

8. Acknowledgement

This research was developed in the context of the project SIDATE which is funded by the German Federal Ministry of Education and Research (BMBF) within its funding priority ”IT Security for Critical Infrastructures". Grant number: 16KIS0239K, 16KIS0240.

9. References

Ackerman, M.S. et al., 2013. Sharing Knowledge and Expertise: The CSCW View of Knowledge Management. *Computer Supported Cooperative Work (CSCW)*, 22(4-6), pp.531–573.

Arif, M., 2011. What Matters Most Among Human Factors to Comply With Organisation's Information Security Policy? In 5th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2011, London, UK, July 7-8, 2011. Proceedings. pp. 35–46.

Bannon, L.J. & Schmidt, K., 1989. CSCW - Four Characters in Search of a Context. *DAIMI Report Series*, 18(289).

Bharosa, N., Lee, J. & Janssen, M., 2010. Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: Propositions from field exercises. *Information Systems Frontiers*, 12(1), pp.49–65.

Cash, J.I. & Konsynski, B.R., 1985. IS Redraws Competitive Boundaries. *Harvard Business Review*, 63, pp.134–142.

Doherty, G., Karamanis, N. & Luz, S., 2012. Collaboration in Translation: The Impact of Increased Reach on Cross-organisational Work. *Computer Supported Cooperative Work (CSCW)*, 21(6), pp.525–554.

Drury, J. & Scholtz, J., Evaluating Inter-Organizational Information Systems. In *Inter-Organizational Information Systems in the Internet Age*. Inter-Organizational Information Systems in the Internet Age, pp. 266–296.

Faily, S., 2014. Engaging Stakeholders in Security Design: An Assumption-Driven Approach. In Eighth International Symposium on Human Aspects of Information Security & Assurance, HAISA 2014 ,Plymouth, UK, July 8-9, 2014. Proceedings. pp. 21–29.

Frangopoulos, E.D., Eloff, M.M. & Venter, L.M., 2014. Human Aspects of Information Assurance: A Questionnaire-based Quantitative Approach to Assessment. In Eighth International Symposium on Human Aspects of Information Security & Assurance, HAISA 2014 ,Plymouth, UK, July 8-9, 2014. Proceedings. pp. 217–229.

Hobson, S.F. et al., 2011. Towards Interoperability in Municipal Government: A Study of Information Sharing Practices. In *Human-Computer Interaction – INTERACT 2011*. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 233–247.

ISAC Council, 2004. *A Functional Model for Critical Infrastructure Information Sharing and Analysis*, White Paper (31 January).

Karlsson, F. et al., 2015. Inter-Organisational Information Sharing - Between a Rock and a Hard Place. *HAISA*, pp.71–81.

Reichard, A., Quirchmayr, G. & Wills, C.C., 2011. Challenges in Implementing Information Security Policies. In 5th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2011, London, UK, July 7-8, 2011. Proceedings. pp. 22–34.