Integrating Shared Cyber Security Information into Information Security Risk Management

Clemens Sauerwein

Department of Computer Science
University of Innsbruck
Innsbruck, Austria
Email: Clemens.Sauerwein@uibk.ac.at

Supervisor: Ruth Breu

Abstract. In the last couples of years, the complexity and interconnectedness of Information Systems (IS), and security related incidents increased significantly. In order to guarantee confidentiality, integrity, and availability of these IS an appropriate information security risk management (ISRM) must be in place. Reliable ISRM represents a challenge for organizations, since they take security related decisions based on outdated data, overlook vulnerabilities, threats or common incidents. To overcome these issues the acquisition of shared cyber security information at the right time supports ISRM to reduce risks, identify attacks, and enhance resilience of an IS. However, the exchange and acquisition of shared cyber security information represents a major challenge in ISRM. In the proposed PhD thesis we focus on this challenge by developing a framework that automatically combines and integrates shared cyber security information into ISRM processes. In doing so, we develop quality criteria, measures, and metrics to evaluate and filter shared cyber security information.

Keywords: Information Security Risk Management, Shared Cyber Security Information, Information Integration, Information Quality

1 Motivation

The increasing complexity and heterogeneity of Information Systems (IS) combined with more sophisticated cyber-attacks manifest serious threats harming an IS's security. Recent prominent information security incidents have shown that attacks can lead to business-critical loss of intellectual property, productivity, money, and reputation [1–3]. In order to counteract these threats, and to guarantee confidentiality, integrity, and availability, an organisation needs to put an information security risk management (ISRM) in place [4]. ISRM includes processes to identify, assess, treat, accept, communicate and monitor information security related risks [5]. It employs information derived from a multitude of internal information sources, like monitoring tools, enterprise architecture artifacts, and stakeholder's knowledge.

Reliable ISRM represents a major challenge for organizations, since they fail to predict risks [6], due to decisions based on outdated data [7], or deficiencies in the timely reaction to occurring threats [8]. To tackle these issues and improve ISRM the acquisition of shared cyber security information and knowledge has been frequently stated as desirable [6]. In the last couples of years a multitude of shared cyber security information sources were created, ranging from public available information sources (e.g. National Vulnerability Database[1], Exploit Database[2], Vendor-specific Advisories,. . .) to threat intelligence sharing communities that exchange threat intelligence among each other [9].

In recent years, research and practice introduced several technologies, data formats, messaging protocols, and frameworks that enable the exchange of cyber security information [10–13]. However, cyber security information sharing in the field of ISRM is hardly present, and depicts one of the core challenges [6]. Thereby, the right selection of information for ISRM plays an important role since inaccurate data could affect the ISRM and can result in undesired effects [14, 15], or uncertainty [16].

In the PhD thesis we want to answer the following overarching research question:

How can shared cyber security information be integrated into information security risk management?

The main objective of the PhD thesis is the development of a framework to combine and integrate shared cyber security information into ISRM, thereby we want to focus primarily on security information shared between organisations. In this context, the development of criteria (e.g. timeliness, completeness, reliability, provenance of information) and methods to evaluate data quality, and filter relevant information for ISRM plays an important role.

Our contribution is threefold: At first we characterize the landscape of relevant and valuable shared cyber security information for ISRM. Secondly, we develop a taxonomy to evaluate the quality of shared cyber security information and provide rules to filter it. Finally, we implement a framework which bases upon the developed taxonomy, provides methods to automatically evaluate the data quality and filter relevant shared cyber security information, and combines and integrates the collected information into ISRM.

2 State of the Art

Cyber Security information sharing is a contemporary topic in information security communities. In recent years several standardization efforts have addressed the challenge of representing cyber security information in a standardized manner [17]. As a result a number of protocols, data formats and frame-

[1] https://nvd.nist.gov/ Accessed: March, 2016

[2] https://www.exploit-db.com/ Accessed: March, 2016

works have been introduced, e.g. Common Vulnerability Exposure (CVE), Structured Threat Information Expression (STIXX), Trusted Automated eXchange of Indicator Information (TAXII), Common Configuration Enumeration (CCE), Common Attack Pattern Enumeration and Classification (CAPEC), and the Open Vulnerability and Assessment Language (OVAL), among others [11, 10, 13]. In [12], a taxonomy is introduced to classify cyber security information sharing technologies, identify gaps, and explain the differences between them from a scientific perspective.

While there are a number of ad-hoc solutions for cyber security information sharing, like email exchange, phone calls, shared databases or data feeds, there is a tendency to establish systems for automated data exchange, and form communities for cyber security information sharing [17]. For example, in the Netherlands the government together with companies has introduced the National Detection Network(NDN) [9]. In this context, there is a need for an effective cyber security information sharing platform, the challenges, requirements and expectations are discussed by [17, 16].

To benefit from information, a persistent theme in research is the assessment of information quality. Therefore, several data quality metrics, measures and frameworks focusing on information quality exist [18–21]. In ISRM only a few researches dealt with the aspect of information quality, e.g. investigations regarding quality deficiencies in the documentation of business security requirements [22], or how to improve quality assessment in ISRM processes through stakeholder knowledge [23].

To the best of our knowledge no prior research has been conducted that examines how shared cyber security information with respect to quality criteria can be integrated into ISRM. In doing so, research and practice lacks metrics, measures and methods for quality assessment of shared cyber security information.

3 Research Questions & Expected Contributions

In Section 1 we introduced our overarching research questions which we divide in the following three research questions: (a) *What are potential shared cyber security information sources for ISRM?*, (b) *What are quality requirements for shared cyber security information for ISRM?*, and (c) *How can ISRM processes be supplied with shared cyber security information?* In the following we explain these research questions and outline the expected contributions.

3.1 RQ1: What are potential shared cyber security information sources for ISRM?

As described in Section 2, several standards for describing and exchanging of shared cyber security information exist. At first we provide a comprehensive overview of the state of the art of standards in the field. Based on these investigations we conduct a study with the goal of identifying potential shared cyber security information sources applied in practice. In this context, our primary focus is on security information which is shared between organisation. In addition to them, we analyse information which is available from public security databases. Finally, the contribution of this research step includes a classification of the landscape of valuable shared cyber security information sources, underlying standards, and their relevance for practice.

3.2 RQ2: What are quality requirements for shared cyber security information for ISRM?

Based on the identified landscape of shared cyber security information for ISRM we develop criteria, metrics and measures to evaluate the data quality. For example, they take in account criteria, like timeliness, provenance, reliability, or completeness of shared information. For this purpose, we analyze the adoption possibilities of existing quality models from information science [18–20, 24, 25], and other fields of ISRM, e.g. [23]. In doing so, we want to analyse if it is possible to adopt or extend existing approaches to evaluate the quality of shared cyber security information. Our main goal is the development of criteria to assure quality of shared cyber security information and provide criteria to filter information in order to reduce the information overhead and facilitate the integration of information into ISRM. Finally, our contribution includes a comprehensive taxonomy containing quality criteria, metrics, and measures to evaluate the quality of shared cyber security information.

3.3 RQ3: How can ISRM processes be supplied with shared cyber security information?

As depicted in Figure 1, based on the identified landscape of shared cyber security information and the taxonomy for quality assurance we develop a framework that automatically collects, combines, and integrates shared cyber security information to ISRM processes. Thereby, we are following three goals: (a) To integrate a multitude of shared cyber security information into ISRM processes, (b) assure the quality of integrated information, and (c) reduce the implicated overhead of useless information. The developed framework should be capable of being integrated into information security management systems implementing ISRM processes.

4 Research Plan

As depicted in Figure 2 our research plan can be divided into the following three steps considering the design science principles [26]: (a) *Identifying the landscape of shared cyber security information*, (b) *development of the taxonomy for information quality assurance*, (c) *development and evaluation of the framework*. In our research we collaborate with a number of organizations, like the OWASP[3]

[3] https://www.owasp.org (Accessed: March, 2016)

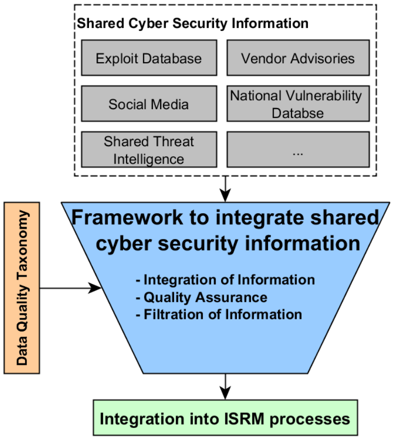
Shared Cyber Security Information
Exploit Database
Vendor Advisories
Social Media
National Vulnerability Databse
Shared Threat Intelligence
...
Data Quality Taxonomy
Framework to integrate shared cyber security information
- Integration of Information
- Quality Assurance
- Filtration of Information
Integration into ISRM processes

Fig. 1. Overview of the framework to integrate shared cyber security information into ISRM processes

community, TÜV Austria[4], Security Interest Group Switzerland[5], our research partners in Europe, and industry partners in the DACH region.

4.1 Identifying the landscape of shared cyber security information

At first, we conduct empirical studies with the goal of identifying the landscape of shared cyber security information. Therefore, we carry out qualitative expert interviews with experts in the field. The interviewees include security experts from our industry and academic partners. Based on the results of the interviews we carry out a quantitative survey addressing the same issue. In doing so, our main goal is the validation of the results of the expert interviews, and subsequently provide of a comprehensive picture of relevant shared cyber security information for ISRM in practice.

4.2 Development of the taxonomy for information quality assessment

Secondly, we identify and develop quality criteria with corresponding quality metrics to assess the quality for shared cyber security information. Therefore, we conduct a systematic literature study on existing data quality criteria and metrics in different applications areas of information science. Based on qualitative expert interviews we evaluate the applicability of the identified quality criteria and metrics to shared cyber security information. Thereby, it might be necessary to adopt or add one or another quality metric. The main result of

[4] https://www.tuv.at/ (Accessed: March, 2016)
[5] https://www.sig-switzerland.ch/de/ (Accessed: March, 2016)

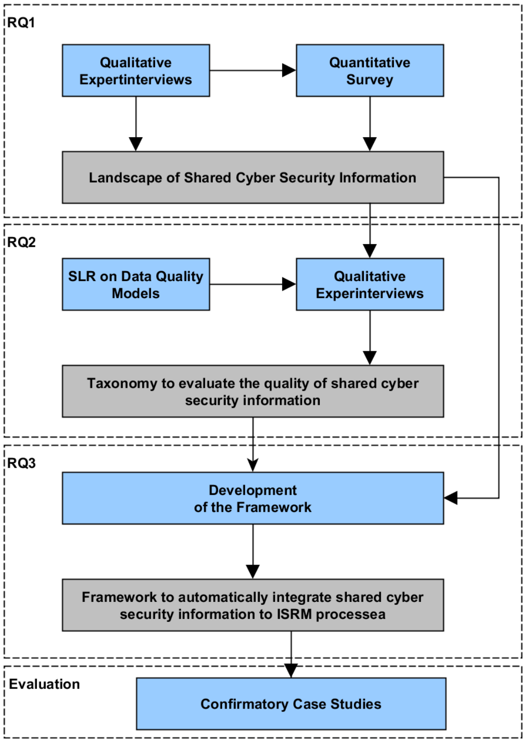
RQ1
Qualitative Expertinterviews
Quantitative Survey
Landscape of Shared Cyber Security Information
RQ2
SLR on Data Quality Models
Qualitative Experinterviews
Taxonomy to evaluate the quality of shared cyber security information
RQ3
Development of the Framework
Framework to automatically integrate shared cyber security information to ISRM processea
Evaluation
Confirmatory Case Studies

Fig. 2. Research plan depicting the different steps with corresponding research questions

the the systematic literature study and the expert interviews is a comprehensive taxonomy to evaluate the quality of shared cyber security information.

4.3 Development and evaluation of the framework

Thirdly, we develop a framework to supply shared cyber security information for ISRM processes. As mentioned in Section 3 the framework should be capable of being integrated into information security management systems (ISMS) implementing ISRM processes. In order to demonstrate the integration capabilities we integrate it into the tool-supported ISMS framework ADAMANT [27] which is part of one of our ongoing research projects. Finally, we evaluate our framework through confirmatory case studies with our research and industry partners.

5 Conclusion

The main goal of our research, and the proposed PhD thesis is the development of a framework that integrates shared cyber security information into ISRM processes. In doing so, the framework combines information originating from different sources, ensures a certain degree of information quality, and filters information in order to counteract useless information overflow. Thereby our research contributions are threefold: (a) Identifying the landscape of shared cyber security information, (b) providing a taxonomy to evaluate the quality of shared cyber security information, and (c) developing the described framework. This paper provides an overview of the addressed research questions, expected contributions and applied research methodology. At the time of writing this paper we were analysing the results of the survey and expert study for identifying valuable shared cyber security information for ISRM, described in section 4.1.

References

1. P. Wood, B. Nahorney, K. Chandrasekar, S. Wallace, and K. Haley. Symantec internet security threat report 2015. Technical report, Symantec Corporation, 2015.
2. Louis Marinos and Andreas Sfakianakis. Enisa threat landscape-responding to the evolving threat environment. *ENISA (The European Network and Information Security Agency)(September 2012)*, 2012.
3. Andrew Miller, Richard Horne, and Chris Porter. 2015 information security breaches survey. Technical report, PWC, 2015.
4. ISO/IEC. ISO/IEC 27001:2013: Information technology - security techniques - information security management systems - requirements. 2013.
5. ISO/IEC. ISO/IEC 27005:2011: Information technology - security techniques - information security risk management. 2011.
6. Stefan Fenz, Johannes Heurix, Thomas Neubauer, and Fabian Pechstein. Current challenges in information security risk management. *Information Management & Computer Security*, 22(5):410–430, 2014.
7. Matthias Farwick, Berthold Agreiter, Ruth Breu, Steffen Ryll, Karsten Voges, and Inge Hanschke. Requirements for automated enterprise architecture model maintenance. In *13th International Conference on Enterprise Information Systems (ICEIS), Beijing*, 2011.
8. Daniel Bachlechner, Ronald Maier, Frank Innerhofer-Oberperfler, and Lukas Demetz. Understanding the management of information security controls in practice. 2011.
9. F. Fransen, A. Smulders, and R. Kerkdijk. Cyber security information exchange to gain insight into the effects of cyber threats and incidents. *e & i Elektrotechnik und Informationstechnik*, 132(2):106–112, 2015.
10. Jessica Steinberger, Anna Sperotto, Mario Golling, and Harald Baier. How to exchange security events? overview and evaluation of formats and protocols. In *Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on*, pages 261–269. IEEE, 2015.
11. Panos Kampanakis. Security automation and threat information-sharing options. *Security & Privacy, IEEE*, 12(5):42–51, 2014.
12. Eric W Burger, Michael D Goodman, Panos Kampanakis, and Kevin A Zhu. Taxonomy model for cyber threat intelligence information exchange technologies. In *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*, pages 51–60. ACM, 2014.

13. Robert Martin et al. Making security measurable and manageable. In *Military Communications Conference, 2008. MILCOM 2008. IEEE*, pages 1–9. IEEE, 2008.
14. Luc Dandurand and Oscar Serrano Serrano. Towards improved cyber security information sharing. In *Cyber Conflict (CyCon), 2013 5th International Conference on*, pages 1–16. IEEE, 2013.
15. Mari Kert, Javier Lopez, Markatos Evangelos, and Bart Preneel. State-of-the-art of secure ict landscape. Technical report, ENISA - NIS Platform - Working Group 3, 2014.
16. Oscar Serrano, Luc Dandurand, and Sarah Brown. On the design of a cyber security data sharing system. In *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*, pages 61–69. ACM, 2014.
17. Sarah Brown, Joep Gommers, and Oscar Serrano. From cyber security information sharing to threat management. In *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, pages 43–49. ACM, 2015.
18. Carlo Batini, Cinzia Cappiello, Chiara Francalanci, and Andrea Maurino. Methodologies for data quality assessment and improvement. *ACM computing surveys (CSUR)*, 41(3):16, 2009.
19. Laura Sebastian-Coleman. *Measuring data quality for ongoing improvement: A data quality assessment framework*. Newnes, 2012.
20. Laure Berti-Equille, Isabelle Comyn-Wattiau, Mireille Cosquer, Zoubida Kedad, Sylvaine Nugier, Verónika Peralta, Samira Si-Said Cherfi, and Virginie Thion-Goasdoué. Assessment and analysis of information quality: a multidimensional model and case studies. *International Journal of Information Quality*, 2(4):300–323, 2011.
21. Peter van Nederpelt and Piet Daas. 49 factors that influence the quality of secondary data sources. 2012.
22. Christian Sillaber and Ruth Breu. Quality matters: Systematizing quality deficiencies in the documentation of business security requirements. In *Availability, Reliability and Security (ARES), 2014 Ninth International Conference on*, pages 251–258. IEEE, 2014.
23. Christian Sillaber and Ruth Breu. Using stakeholder knowledge for data quality assessment in is security risk management processes. In *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*, pages 153–159. ACM, 2015.
24. Fatimah Sidi, PH Shariat Panahy, Lilly Suriani Affendey, Marzanah A Jabar, Haidi Ibrahim, and Aouache Mustapha. Data quality: A survey of data quality dimensions. In *Information Retrieval & Knowledge Management (CAMP), 2012 International Conference on*, pages 300–304. IEEE, 2012.
25. Amrapali Zaveri, Anisa Rula, Andrea Maurino, Ricardo Pietrobon, Jens Lehmann, Sören Auer, and Pascal Hitzler. Quality assessment methodologies for linked open data. *Submitted to Semantic Web Journal*, 2013.
26. R Hevner von Alan, Salvatore T March, Jinsoo Park, and Sudha Ram. Design science in information systems research. *MIS quarterly*, 28(1):75–105, 2004.
27. Michael Brunner and Ruth Breu. It compliance mit kontextuellen sicherheitsanforderungen. *DA CH Security*, pages 136–147, 2014.