A Cyberthreat Search Process and Service

Yogesh Bhanu[1], Sebastian Dännart[2], Henning von Kielpinski[1], Alexander Laux[2], Ulrike Lechner[2], Tobias Lehmann[3], Andreas Rieb[2], Martin Riedl[2] and Florian Wolf[4]
[1]*Consol, München, Germany*
[2]*Fakultät für Informatik, Universität der Bundeswehr München, Neubiberg, Germany*
[3]*Inopus GmbH, Neubiberg, Germany*
[4]*Mergeflow AG, München, Germany*

Keywords: IT-Security Management, Search Process, Technology Scouting.

Abstract: Searching for IT-Security related information should be a standardized and/or partially automated process. This position paper presents a literature review that depicts a reference process design and the design of a tool to support search and analysis of IT-security related information.

1 INTRODUCTION

Searching for cybersecurity information should be a standardized process, implemented with adequate IT-support, effectiveness as well as efficiency in mind. Moreover, the landscape of IT-security topics relevant to an organization should be available as a service. These two ideas for a reference process and a service for the search of IT-security related information formed the basis of our research project. The position paper at hand discusses empirical findings on the design of a search processes and a service.

Today, majority of search done for cyber threats or other IT-security related information is not done in a systematic way and it is hardly automated and are barely supported by tools. Herein, literature and our empirical findings (cf. Sect. 2 and 3) arrive at the same conclusion. Our research attempts to make a contribution to IT-security management in theory and practice.

We describe our approach with two scenarios. First scenario: IT-security professionals meet and share information about what could be the next "big attack". Assuming, Stuxnet has been relevant and so is the less famous Gauss. The IT-professionals share rumours. Next day, back in the office they do research. There is no acronym, no CVE-number to begin with and no newsfeed of IT-security specialists has information to offer.

The term "Gauss" provides a clue and this leads to a tedious search, as the search term "Gauss" is overloaded with the mathematician Carl-Friedrich Gauss, the mathematical programming kit Gauss, the metrical unit Gauss. Information about the Advance Persistent Threat (APT) Gauss is somewhat lost among all what the main search engines have to offer (tested in an online search in October 2015) and the search for a "Gauss-related", unnamed upcoming IT-threat is a bit like searching for a needle in a haystack. This highlights the need to have a database with cybersecurity related information which will make the process of searching for IT-Security related information less cumbersome or a specialized search application tool that caters to cybersecurity information and can analyse data points according to the relevant concepts.

Second scenario: A hosted service provider that has to make sure that all the hosted applications as well as the hosting technology are safe. Such a service provider would be interested in all upcoming IT-security topics as well as politically or economically motivated threats to the clients, e.g. by hacktivists. Is there a need to reconsider a configuration, or is there a need to patch systems or to warn a client from hacktivists ?

The search for IT-security related information in our second scenario is tedious as there are hundreds of technologies and applications at play for which

Bhanu, Y., Dännart, S., Kielpinski, H., Laux, A., Lechner, U., Lehmann, T., Rieb, A., Riedl, M. and Wolf, F.
A Cyberthreat Search Process and Service.
DOI: 10.5220/0005806605280535
In *Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016)*, pages 528-535
ISBN: 978-989-758-167-0
Copyright © 2016 by SCITEPRESS – Science and Technology Publications, Lda. All rights reserved

security needs have to be monitored. This monitoring needs to happen frequently. This leads to further questions e.g. When should the search process be stopped? Which sources of information need to be considered? Does an average IT-professional need to take not only the open information sources into account, but also the "dark corners" or the darknet itself into consideration? What level of quality in terms of data collection and data analysis needs to be undertaken in order to document the effort, to do the job well or to avoid negligence lawsuits?

Technically speaking the two scenarios are about the search for weak signals with the aim to stay ahead of the game. In reality, the search involves browsing through search engine results and other information sources: Twitter accounts of leading professionals, news ticker or newsfeeds from companies or from public institutions, forums, communities or pastebin services, etc.

Scenarios as the ones above motivated our joint research project and our research interest in

- search strategies and search processes,
- quality and IT-support of search processes.

There is one particularly vexing question: How exhaustive should be the search? We suggest that scope and strategy need to be defined for a search.

2 LITERATURE AND STATE OF THE ART REVIEW

The first, well known genre of IT-security related information are interactive maps with information about volumes, kind, source and target (cf. https://cybermap.kaspersky.com. The second well established genre are analysis reports (cf. (Anon 2012; Bundesamt für Sicherheit in der Informationstechnik 2015) with analyses of APTs, IT-security trends and forecasts. There are some novel technology as dedicated (semantic) search or intelligence technologies (e.g. (Awad et al. 2015)) or for sharing IT-security related information (e.g. (Ward et al. 2014).

As there is hardly any literature on search and analysis of IT-security information and since this search is interested in "novel technologies" we reverted to the scholarly methods "literature review" and to "technology scouting" as the domains from which we take terminology and concepts for the design of our search process and tool support.

Structured literature review is a method to cover an extant body of (scholarly) literature. The definition of the scope of a literature review, the methods used to analyze identified literature and the structure of the findings are key elements of the method literature review. (Boote & Beile 2005; Randolph 2009; Webster & Watson 2002). The literature on the method literature review as a scholarly method illustrates that a search and analysis process needs to be defined with care and the aim in mind.

Technology scouting for information on upcoming technology is considered a structured process in technology or innovation management. Wolff describes that „In the 1980s, as U.S. companies came to recognize they could no longer meet all of their technology needs internally, more and more companies began scouting for overseas technology in a formal, organized way." (Wolff 1992). He describes that leveraging information, such that an organization eventually would adopt technology identified in scouting, is a major challenge. He refers to interviews on the reality of technology scouts describing, "you have to understand the corporate strategy, the divisional strategy, and the personality and goals of the decision maker. Technology scouting requires a much more thorough understanding of these factors than competitive intelligence does." (Wolff 1992). Wolff argues: „Viewed positively, any technology adoption that does occur is serendipitous; viewed negatively, it's a haphazard process. ".

Rohrbeck describes in his case study of the technology scouting process in Deutsche Telekom that technology scouting is a process of technology intelligence to "identify opportunities and threats arising from advances in technology" with the goal to maintain competitive advantage (Rohrbeck, 2010). Sarpong et al. argue that strategic foresight is crucial to organizational success in rapidly changing environments with complexity and genuine uncertainty where interventions cannot be prescribed in advance. Foresight is described as "refined sensitivity for detecting and disclosing invisible, inarticulate or unconscious societal motives, aspirations, and preferences and of articulating them in such a way to create novel opportunities hitherto unthought-of and hence unavailable to a society or organization". Sarpong et al. capture the delineation of foresight as "[a] process that attempts to broaden the boundaries of perceptions in four ways: by assessing the implications of present actions, decisions, etc. (consequent assessment); by detecting and avoiding problems before they occur (early warning and guidance); by considering the present implications of possible future events (proactive

future formulation); [and] by envisioning aspects of desired futures (normative scenarios)". The process perspective, therefore, is grounded in the widespread recognition that foresight is not a positive science but rather a contextual process of "way-finding" driven by anticipation, imagination, continuous probing, and the enactment of the future (Sarpong et al. 2013). So, technology scouting is by no means a trivial process - it is contextual, difficult to formalize and support and leveraging information to adequate action is a major challenge.

Rohrbeck defines technology scouting and the evolution of the related concepts of technology intelligence, future studies, foresight and forecasting (Rohrbeck 2010) and distinguishes

- Technology monitoring, i.e. the search of specified topics and scope,
- Technology scanning, i.e. the search of "white spaces", i.e. on topics and a scope not covered in the technological scope of an organization.
- Technology scouting, i.e. the search process to facilitate the sourcing of technology.
- Technology intelligence, i.e. the process concerned with identification, assessment and usage of information on technological developments (Rohrbeck 2010).

Technology scouting needs to address white spaces (Rohrbeck 2010) or the unknown unknowns, i.e. the information whose nature scouts, experts and managers not even suspect (Oertl et al. 2014).

ICT will revolutionize foresight studies: future studies will be a practice, the demand for future studies will increase, quality of data will improve and the reliance on group wisdom will increase while the reliance in individual experts will decrease (Keller & von der Gracht 2014).

There are several models and concepts for technology scouting processes: (1) Early identification of technologies, trends and shocks, (2) Raising the attention for threats and opportunities of technological development, (3) Stimulation of innovation by combining the technology reports with business potential assessment, and (4) Facilitation of the sourcing of external technologies by reaching through the network of technology scouts to their sources of information (Rohrbeck et al. 2013). The process has four phases: (1) Identification, (2) Selection, (3) Assessment, and (4) Dissemination to produce information relevant for the innovation strategy, CTOs and CMOs, R&D and Product Managers. More design and organizational implementation of technology scouting can be found in (van der Duin et al. 2014), (Vishnevskiy et al. 2014), (Oertl et al. 2014), and (Battistella & De Toni 2011).

Scouting processes have decreasing returns over search time and search costs with most of the results identified early in the process (Oertl et al. 2014). Most of the technology findings come from internal or external full-time scouts whereas internal and external part-time scouts contribute less (Rohrbeck 2010).

This first part of the review illustrates that the design of search processes is a challenge. Little is known about the search for IT-security information.

One main strategy in IT-security is to identify threats as early as possible: IT-Security however seems to be about today's reality and yesterday's understanding (Loch et al. 1992) and seemingly too little has changed in understanding the IT-security landscape - calling for black and white hat research and illustrating the need to get closer to the "black hats" and their activities (Mahmood et al. 2010). This need to get close to the sources motivates the use of technology scouting as analogous domain.

IT-security information plays a crucial role in IT-security management. There is empirical evidence on the relevance of IT-security information for compliance of users with IT-security policies and adoption of IT-security technology (cf. e.g., (Blugurcu et al. 2010), (Roberts et al. 2013), (Siponen & Vance 2010), (Johnston & Warkentin 2010), (Spears & Barki 2010)).

In general, the gap between information and adequate action is imminent in the IT-security domain. Harten et al. (Harten et al. 2014) refer to studies suggesting that while 80 percent of companies think of cybercrime as a high risk to the economy, less than one third of companies perceived the threat to their company as high (Geschonneck et al. 2013). Optimism bias describes the disparity between perceived general and perceived individual risk (Pfleeger & Caputo 2012). Individuals who have been attacked in the past assess their risk higher than the ones who have not been attacked and the likelihood of detected attacks is related to with the ability to uncover cybercrimes (Harten et al. 2014). This adds to our argument that information about IT-security is a crucial element in the IT-security management of any organization.

3 THE SEARCH PROCESS

The empirical basis of the study of search processes and the design of a reference process are ten expert interviews with IT-security experts from various

organizations connected to the IT-security cluster Munich. The interviews were semi-structured, done from December 2014 to April 2015 and lasted between 44 and 98 minutes. The interviews were recorded and transcribed or (alternatively) minutes were taken during the interview. The processes were reconstructed in a qualitative analysis and structured according to a reference structure, which is based on common features of the inquired processes.

3.1 The Reference Structure

The reference structure for the search of IT-security information with the five main processes is depicted in Fig. 1.

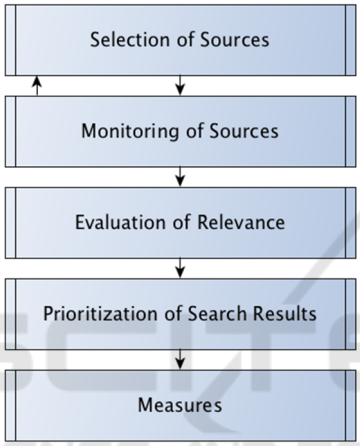

Figure 1: Reference structure for the search for IT-security information.

The reference structure consists of selection of sources, monitoring of sources, evaluation of relevance of the search results of monitoring (relevant or of interest only), prioritization of search results, and measures.

None of the organizations had a process for the search for IT-security information formally defined and established. In eight (out of ten) cases a process could be identified.

All interview partners are confident about the quality of their level of information about IT-security. E.g., one of our interview partners suggests that his organization never missed an exploit in the past („Also ich glaube, wir haben noch nie eine Sicherheitslücke verpasst“). None of the organizations had a dedicated tool support to search, structure and organization of this information to a cybersecurity operational picture of the current IT-security status of the organization. None of the organizations had a clear overview of the costs of search for IT-security information and in some cases is was common practice for the employees to search for IT-security related information in their leisure time and from their private devices at home. Furthermore, the interview partners referred to past experiences, individual judgments “gut feelings” as their way on how they select sources and do the analysis.

3.2 An Example: The Search Process of an IT-Service Provider

Fig. 2 depicts, the reconstruction of the search process of an IT-service provider. This process is considered as one of the best structured processes in our empirical sample.

This IT-service provider needs to consider the IT-security of the technology for hosting as well as the security of the hosted IT-services. We found that the search process for cybersecurity information is not formalized – there is however an established, structured method for this search.

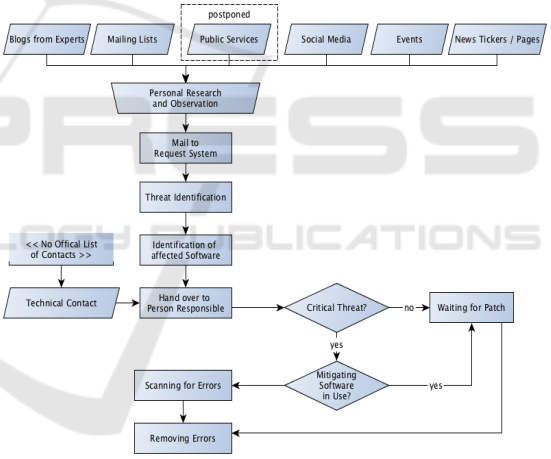

Figure 2: Search process of an IT-service provider.

Our interview partners referenced six different kinds of sources: (1) Blogs from experts, (2) Mailing lists, (3) Public services, (4) Social Media, (5) Events as, e.g., conferences and fairs, and (6) News tickers and news pages. The interview partner distinguishes between closed (available to a closed group) and open (available to the general public) mailing lists and considers quality and relevance of closed lists higher than quality of open mailing lists.

In Monitoring, the interview partners suggest that employees monitor their preferred sources as part of their job as well as in their leisure time. Information on threats or relevant information is sent as a ticket to a request system.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

Evaluation of relevance is done by experts. The decision who evaluates the relevance of a ticket is ad hoc, based on individual experiences of the expert handling the security ticket.

To prioritize, the expert handling the ticket determines the level of criticality and organizes adequate IT-security measures.

An IT-security vulnerability that is classified as critical until a patch is available. If no countermeasure is available for a critical software, a "deep inspection", i.e. a process of searching and eliminating vulnerabilities begins.

3.3 The Reference Process

This reference process is based on the result of reference modeling which in turn is based on the results of expert interviews, literature study (with analogies to technology scouting and scholarly literature review) and our domain knowledge of IT-security and search processes is depicted in Fig. 3. The reference structure (cf. Fig. 1) forms the basis this model.

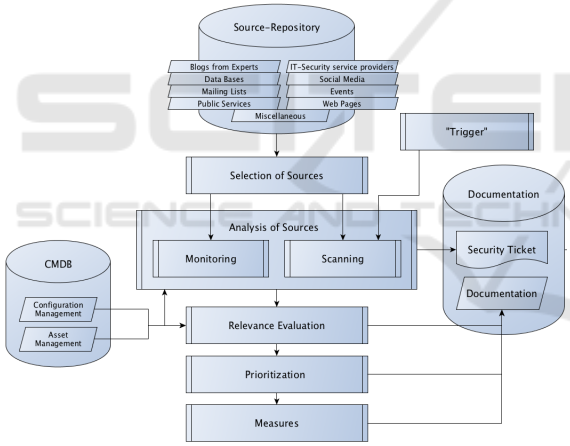

Figure 3: The Reference Process.

The first step of the process is the selection of sources. These sources are maintained in a source-repository. We distinguish a collection of classes of sources: Blogs / Experts, Databases, Mailing lists, Public institutions and their services, IT-security service providers, Social Media, Events (Fairs, Conferences), Webpages, and Miscellaneous.

Process step "Analysis of sources" distinguishes two search strategies: (1) Monitoring is a process that evaluates predefined sources according to predefined criteria on a regular basis. Monitoring is concerned with IT-security information and threats that can be captured according to predefined criteria in the analysis of sources. (2) Scanning is typically an interactive process done by experts that deals with "blank areas" on the threat landscape and with the unknown unknowns, i.e. threats that go beyond established attack vectors and concepts. Scanning could also be done as a reaction to some cause of concern. Note that we follow here the terminology and concepts of technology scouting (cf. Sect. 2) as well as the wording that the IT-security experts used in the interviews.

In "Analysis of Sources" a security ticket is created that documents the results of the analysis. Note that this result may be "negative" as well. Note furthermore that the recommendation to the use of a ticket system was our observed during the interviews. The interview partners referred only to positive results to result in a security ticket. In order to document the search and analysis efforts as well as to facilitate the analysis of key performance indicators, we recommend to document all results. Note that this step also gets input from the documentation of the search process.

The "Analysis of Sources" is followed by step "Relevance Evaluation". This process step evaluates IT-security information according to its relevance for a particular organization and it distinguishes "merely interesting" from "actually relevant" information. This step gets information about relevant technologies, configurations and assets, from the asset or configuration management (and its databases).

Step "Prioritization" then classifies and ranks the relevant information to trigger adequate measures. Again, this step gets input from configuration or asset management.

A more detailed description of the selection of sources as well as the quality management of the whole process is provided in (Dännart et al. 2016). Note that e.g. a predefined set of sources implies that one knows the sources that need to be considered and also when to stop searching, in case the search yields no result. The Mergeflow search application offers IT-support for the search for and analysis of IT-security related information.

4 THE MERGEFLOW APPLICATION

Part of the research was the development of a tool to support the search for IT-security information and the analysis of this information.

The Mergeflow application supports the creation of a repository for sources, a configurable spidering

application for collecting data from a configurable variety of sources. Fig 4. depicts the results for the search for “Stuxnet” with a number of search results and keywords associated with this search.

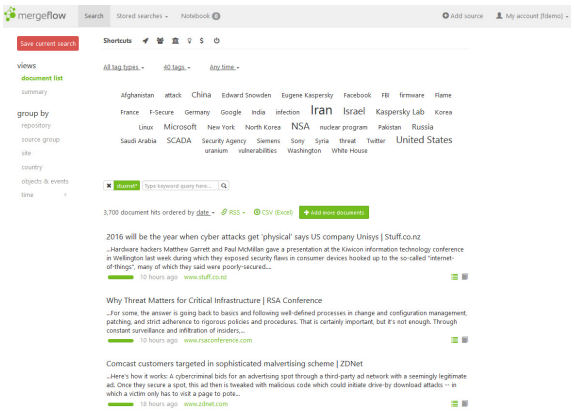

Figure 4: Search results in the Mergeflow application.

The application supports an interactive search process through clustering functionalities. Clustering can be done according to “technology”, “person” (persons involved), “company”, or “vulnerability”. The analysis is done by a text mining specialized for the domain IT-security.

Fig. 5 depicts the results of representation as a graph. This graph can be manipulated to support the search for relations between concepts. Concepts are, e.g. CVS number, persons, country. Edges represent documents that contain a relation between the concepts. These documents can be inspected to learn more about the nature of the connection between the concepts and they can refer to the original source or the internal database of spidered or otherwise collected documents. Fig. 6 presents a different structure for the information. Here the organizations, the threats and the development over time are presented.

The application also supports workflows and allows schedule routine queries (for the search strategy monitoring) and results, e.g. for handing search results over in a structured search process. The application supports an analysis for changes in the graphs to identify new topics that gain momentum – the weak signals of upcoming topics or threats.

Note that this application goes beyond what has been formulated in the search process in terms of analysing and structuring functionalities. It can support the operational IT-security level that is interested in information about current threats and current IT-security information. It can also support more tactical analysis, e.g. for compiling an operational IT-security picture.

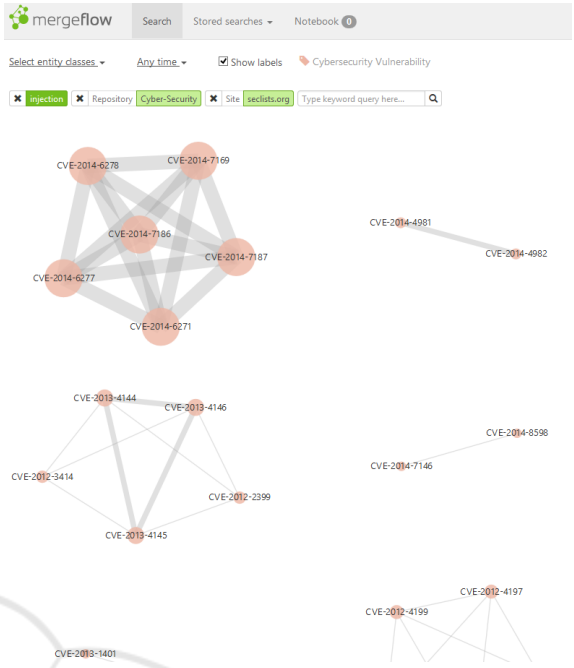

Figure 5: Graph with CVS number relations.

Figure 6: Relation organizations and IT-security threats over time.

5 CONCLUDING REMARKS

Our research interests are

- search strategies and search processes

- quality and IT-support of search processes

of IT-security related information. This position paper presents a literature review, the design of a reference process for search and the Mergeflow application to support the search of IT-security information, to analyse this information and to develop an operational common picture or a more strategic operational picture.

While seeking data as well as during designing the process and the tool some of the initial assumptions of what eventually would be useful for IT-security professionals had to be turned on its head. First, we assumed that search of IT-security information is about detecting weak signals as all IT-professionals will attempt to stay ahead of the game. This is what IS and IT-security literature suggest and what an IT-professional would think as to be cool (cf. Stuxnet). Our analysis suggests that most IT-professionals would benefit from being provided support when monitoring professional sources and structuring this information.

IT-management would benefit from search of IT-security information as a standard process with a scope and quality criteria. We suggest that it should be implemented as a dedicated role within the organization (instead of a joint effort of employees done partly in the leisure time). Our reference process suggests scope and criteria (cf. also (Dännart et al. 2016) for such a search.

The Mergeflow application itself however would need customization as well as integration, in particular consulting effort as very little is known about the relevance of search of IT-security of an organization and the needs to get this information search and analysis structured. It is still an open question what a useful operational cybersecurity picture should look like. Consequently, more research needs to be done here.

ACKNOWLEDGEMENTS

We would like to acknowledge the funding from IUK Bayern for project “Laufend aktuelles Cybersecurity Lagebild“ (FKZ:IUK-1304-0011// IUK427-004). We are grateful to our interview partners for their valuable input.

REFERENCES

Anon, 2012. *IT-Sicherheitsniveau in kleinen und mittleren Unternehmen. Studie im Auftrag des Bundesministerium für Wirtschaft und Technologie*, Available at: www.bmwi.de/DE/Mediathek/publikationen,did=525400.html.

Awad, W. S., El-Alfy, E. S. M. & Al-Bastaki, Y., 2015. *Improving Information Security Practices through Computational Intelligence*, IGI-Global.

Battistella, C. & De Toni, A. F., 2011. A methodology of technological foresight: A proposal and field study. *Technological Forecasting and Social Change*, 78(6), pp.1029–1048.

Blugurcu, B., Cavusoglu, H. & Benbasat, I., 2010. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MISQ*, 34(3), pp.523–548.

Boote, D. N. & Beile, P., 2005. Scholars Before Researchers: On the Centrality of the Dissertation Literature Review in Research Preparation. *Educational Researcher*, 34(6), pp.3–15.

Bundesamt für Sicherheit in der Informationstechnik, 2015. Die Lage der IT-Sicherheit in Deutschland 2015. *Informationstechnik*.

Dännart, S., Laux, A., Lechner, U. & Riedl, M., 2016. Suche nach IT-Sicherheitsinformationen – Ein Referenzmodell. In *Konferenzband Multikonferenz Wirtschaftsinformatik 2016 (To appear)*. Ilmenau.

van der Duin, P., Heger, T. & Schlesinger, M. D., 2014. Toward networked foresight? Exploring the use of futures research in innovation networks. *Futures*, 59, pp.62–78.

Geschonneck, A., Fritzsche, T. & Weiand, D.K., 2013. *e-Crime - Computerkriminalität in der deutschen Wirtschaft mit Kennzahlen für Österreich und Schweiz*, Available at: www.tnsemnid.com/politik_und_sozialforschung/pdf/Studie_e-Crime-2012.pdf.

Harten, C. et al., 2014. Towards an Awareness Gap on Cybercrime – an Empirical Analysis of the Perceived Threat Level and Implemented IT Security Measures in Companies. In D. Kundisch, L. Suhl, & L. Beckmann, eds. *MKWI 2014 Multikonferenz Wirtschaftsinformatik*. pp. 533–546.

Johnston, A. C. & Warkentin, M., 2010. Fear Appeals and information Security Behaviors: An Empirical Study. *MISQ*, 34(3), pp.549–566.

Keller, J. & von der Gracht, H. a., 2014. The influence of information and communication technology (ICT) on future foresight processes — Results from a Delphi survey. *Technological Forecasting and Social Change*, 85, pp.81–92.

Loch, K. D., Carr, H. H. & Warketing, M. E., 1992. Threats to Information Systems : Today’s Reality, Yesterday's Understanding Evolution of Computer Security. *MISQ*, (June), pp.173–187.

Mahmood, M. A. et al., 2010. Moving toward Black Hat Research in Information Systems Security: An Editorial Introduction to the special issue. *MISQ*, 34(3), pp.431–433.

Oertl, A., Heiss, M. & Homma, C., 2014. The Iterative Involvement of internal Experts into the Technology Scouting Process a Siemens case study. pp.1–6.

Pfleeger, S. L. & Caputo, D. D., 2012. Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, 31(4), pp.597–611.

Randolph, J. J., 2009. A Guide to Writing the Dissertation Literature Review. *Practical Assessment, Research & Evaluation*, 14(13).

Roberts, T. L. et al., 2013. Insiders´ Protection of Organizational Information Assets: Development of a Systematcs-Based Taxonomy and Theory of Diversity for Protection Motivated Behaviors. *MISQ*, 37(4), pp.1189–1210.

Rohrbeck, R., 2010. Harnessing a network of experts for competitive advantage: technology scouting in the ICT industry. *R&D Management*, 40(2), pp.169–180.

Rohrbeck, R., Thom, N. & Arnold, H., 2013. Technological Forecasting & Social Change IT tools for foresight : The integrated insight and response system of Deutsche Telekom Innovation Laboratories. *Technological Forecasting & Social Change*.

Sarpong, D., Maclean, M. & Davies, C., 2013. A matter of foresight: How practices enable (or impede) organizational foresightfulness. *European Management Journal*, 31(6), pp.613–625.

Siponen, M. & Vance, A., 2010. Neutralization: New Insights into the problem of employee information systems security policy violations. *MISQ*, 34(3), pp.487–502.

Spears, J. L. & Barki, H., 2010. User Participation in Information Security Risk Management. *MISQ*, 34(3), pp.503–522.

Vishnevskiy, K., Karasev, O. & Meissner, D., 2014. Integrated roadmaps and corporate Foresight as tools of innovation management: The case of Russian companies. *Technological Forecasting and Social Change*.

Ward, D. et al., 2014. Trust building and the European research network for critical infrastructure protection community. *International Journal of Critical Infrastructure Protection*.

Webster, J. & Watson, R.T., 2002. Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MISQ*, 26(2), pp.13–23. A.

Wolff, M. F., 1992. Scouting for Technology. *Research-Technology Management*, 35(2), p.10.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS