Tailoring policies and involving users in constructing security policies – A mapping study

Elham Rostami

CERIS - Informatics department, Örebro University, Örebro, Sweden
Elham.rostami@oru.se

Abstract

The purpose of this study is to survey existing information security policy (ISP) construction research to understand to what extent the concept of tailored ISP and user involvement have been considered by researchers. The results are based on a literature mapping study of ISP construction between 1990 and 2017 in Scopus and Web of Science databases. The findings show that researchers have not given tailoring of ISPs any attention and there are only a few researchers that paid attention to involving users in constructing ISPs. This research has implications for both researchers and practitioners and shows the way for the future researches by focusing on the concept of tailored policy and how it can be achieved as well as involving users in such tailoring.

Keywords

Information security policy, Policy construction, Tailored policy, User involvement, Mapping study

1 Introduction

Information security policies (ISPs) as one of the most important controls to reduce security breaches in organizations have received significant attention from researchers. This is due to the fact that information security cannot be accomplished by technical means only (Sheng et al., 2010), and as Slusky & Partow-Navid, (2012, P 22) stated: "information security is 90% people and process and 10% technology". Meanwhile, researchers (e.g. Shaw et.al, 2009) admitted that poor security behaviour of employees (e.g. user security errors, carelessness, and negligence) has caused many security threats. Although the need for ISP has been stressed by researchers, they have provided slightly different definitions of this concept. In this study we will focus on strategic and operational level of ISP or as Cram et al. (2017) stated non-technical level. By strategic we mean ISPs that address top managements strategic direction regarding information security and by operational we mean issue-specific guideline and procedures that should be complied by employees in their daily activities (Belsis et al., 2005). However, introducing ISP in organizations does not grantee security of information; nor does it necessarily reduce the number of security incidents. This is mostly because employees do not comply with ISPs (Siponen et al., 2009). Considering this point some researchers (Stahl et al., 2012; Karlsson et al.,

2017) have shown that construction and implementation of ISPs can sometimes impair employees' information security behaviour. They have found that ISPs can be cumbersome, incompatible with existing work practices and contradictory. Moreover, reading a big document of the organization ISP may not be interesting or even doable for all employees at different levels since they do not know which part is exactly related to them or the document is complicated for them to read. Considering the problems of ISP document and difficulties that employees have with it, constructing "tailored policies" for different employees by policy makers might be a way forward. By tailored policies we mean instead of providing a monolith ISP document for the organization and expect all employees to read it and find the part that is related to their job, we can construct ISPs that are specific for different employees based on their needs and responsibilities.

Understanding the employees' work situation and needs is a prerequisite for tailoring of ISPs. Renaud and Goucher (2012) stated it is common that employees cannot understand what is required from them or how to achieve it because of misunderstanding between policy writer and the employee. One way to understand the employees' needs is involving them in the process of construction ISPs. User involvement is common in information systems and has been discussed in this field for a long time (e.g. Baroudi et al., 1986; Barki & Hartwick, 1989). Extended research has shown that involving users in development of information systems leads to information systems that better correspond to users' needs and their work situations. In the information security field, the concept of user involvement has been emphasized by several researchers as well (e.g. Dhillon & Torkzade, 2001). According to Albrechtsen and Hovden (2010) sharing knowledge and experience between employees and information security professionals (policy-makers) is important since it would create common insight among these two groups.

A number of literature reviews considering ISP management have been conducted in recent years (e.g. Cram et al., 2017; Flowerday and Tuyikeze, 2016; Järveläinen (2016). Although the concept of tailored ISP and user involvement have been mentioned in some of these literature reviews (specifically in Järveläinen (2016) study), they have not been studied as the core part. It means that today we do not know to what extent researchers have contributed to these areas. Hence, the aim of this paper is to survey existing research on ISP construction to understand to what extent the concept of tailored ISP and user involvement have been considered by researchers. Specifically, we pose the following research questions: *i) To what extent tailored ISP has been considered in ISP construction? ii) To what extent user involvement has been considered in ISP construction?*

2 Related research

A few literature reviews have considered the ISP construction phase along with other phases in ISP management (Tuyikeze & Flowerday, 2014; Cram et al 2017; Järveläinen (2016). Tuyikeze & Flowerday, (2014) reviewed 21 documents to understand the ISP development life cycle and design a model for the formulation,

implementation and enforcement of an ISP in an organization. Their model was inferred from 10 categories and in 2 categories out of 10 (employee support and information security policy stakeholders) user involvement has been discussed. In these categories Tuyikeze & Flowerday, (2014) emphasized that involving multiple stakeholders in the process of developing ISPs is vital since it gives a sense of ownership to employees and facilitates acceptance and adoption of ISPs. The concept of tailored ISPs has not been mentioned in their study.

Cram et al. (2017) reviewed 114 ISP related publications from 34 journals and synthesized the current knowledge in a research framework. The authors categorized the existing ISP literature into five relationships that cover the whole ISP development process. In the first relationship (influences on the construct and implementation of ISPs), Cram et al. (2017), identified three groups of factors that influence on construct and implementation characteristics of ISPs. The first factor checks the role of standards, guidelines, and regulations in shaping ISPs based on the size and type of the organization. The second factor that influencing ISP construct and implementation is considering the format and structure of ISPs and the final factor is the role of risk management. Cram et al. (2017), believed that the point that has been missed in the current literature is drawing attention to theory since in most of the researches the focus is on the practical considerations of managers responsible for ISPs construct and implementation. Based on that, they suggested that applying a more control theory-centric approach related to ISP construct and implementation, can help researchers to gain understanding about the different ways that an ISP can be constructed, which could lead to downstream compliance impacts. They did not elaborate on the different ways and consequently, they did not address tailored ISP. By applying a control theory-centric approach that includes concepts such as control style (which means for example the degree of participation and acceptance of controls by employees), Cram et al. (2017) suggested future research can focus on which choices managers have in constructing ISPs. That concept of user participation was not further discussed in their literature review.

Järveläinen (2016) research is the only literature review that emphasized on the importance of having customized ISPs which are system-specific rather than organization-specific. The concept of customized security policy in their research is exactly what we mean by tailored ISPs. They reviewed 46 papers focusing ISP development and proposed an integrated business continuity planning (BCP) and ISP development approach to construct customized security policies and continuity plans for critical processes in organizations. They actually explained Similarities and differences of ISP and BCP development methods (based on the prior literature) and included the strengths of them in to a new integrated approach. Järveläinen (2016) actually tried to propose an integrated approach of BCP and ISP to improve awareness and understanding of these two concepts and also help to create customized security policies. However, they did not mention the current states of tailored ISPs in the literature and also to what extent this concept has been developed. The importance of involving users in constructing ISPs has also been discussed in Järveläinen (2016) research. They mentioned that involving employees

in the process of constructing ISPs from all business units can increase their awareness. However, they did not discuss how and when users should be involved.

3 Method

A systematic literature mapping study was conducted to answer the research questions. Mapping study is a method which provide a coarse-grained overview (Pedersen et al. 2008). This method suits our study since we are not interested in deep analysis of existing literature and only want to focus on presenting the frequencies of considering tailored policies and also user involvement in the process of ISP construction; Thus, it will make possible for us to see the level of emphasize on these concepts in the prior researches and consequently leads us to identify the gap and possibilities for future research. To the best of our knowledge mapping study as a research method does not seem to have been widely used in information security area before, but it has been applied in software engineering sub-discipline several times (e.g. Axelsson & Skoglund, 2016; Kitchenham & Brereton, 2013). In their mapping study Condori-Fernandez et al. (2009) tried to answer frequency centric research questions similar to ours.

Conducting this study, we used Elsevier's database Scopus and Clarivate Analytics' database Web of Science to search for potential papers. Web of Science covers over 12,000 of the high impact journals and over 150,000 conference proceedings (Franke and Brynielsson 2014), and Scopus has a good coverage of the journals on the Association of Information Systems' journal ranking list and specific information security journals and conferences (Karlsson et al., 2015). These two databases together provided a good coverage with regards to information security policy construction. We used large set of search string that was a combination of "information (system) security policy/rule/guideline" and "management/development/implementation/desing/requirement/deployment/effectiveness/planning/requirment". The papers published on the databases between 1990 and 2017 were included in our study. The year 1990 was selected because Straub and Nance (1990) published their paper on computer abuse; it is an early example of information security management research that relate to ISPs. Our search included journal papers and conferences papers regardless of the geographic region in order to have an inclusive view of the field. Meanwhile, search fields included paper title, abstract and keywords. The use of multiple search strings resulted in a gross list of 1083 research papers, including duplicates. After eliminating duplicates, we had 427 papers. Then, the abstract was read by considering the following inclusion criteria which led us to 57 articles: 1) Paper is written in English, 2)Paper should be peer-reviewed and considered as journal papers or conferences papers and not book chapter or conference review, 3) Paper is focusing on ISPs as a study object, 4) Paper is focusing on ISPs construction in organizations.

We chose the abovementioned inclusive search strategy to ensure we would not miss any papers by setting the search parameters too narrow. Since we could not get access to 12 articles, so we ended up with analysing a net list of 45 papers

The abstract and introduction section of all 45 papers were read to understand if the paper considers tailoring ISPs to different users and/or if the paper considers involving users in ISPs constructing. When the paper considered any of these concepts, we continued our analysis by reading the discussion and conclusion as well. This led us to have a result that includes two categories: Yes (the paper talk about the concept(s)), No (the paper does not say anything about the concept(s)). However, there were also some papers that had some ideas which was close to what we mean by tailored ISP, although these studies did not deliver any result regarding this concept. These papers were categorized as borderline papers. The result was documented in an Excel spreadsheet by the author.

4 Result

The result of the mapping study is presented in this section and the overall analysis is shown in Table 1. The leftmost column contains the author's name(s) that was included in the mapping study, the second column shows if the papers talk about tailored policy, and the third column shows if papers considered involving users in constructing ISP. In the table, (Yes) means that the concept has been considered, and (No) means the papers has not discussed anything regarding the concept. In the second column (B) means that the papers are borderline.

The table shows that 44 papers did not consider tailored ISP and the other 2 papers are borderline. One of these papers (Almusharraf et al., 2015) talks about the importance of having flexible policies to be able to address all issues that influence organizations and complexities regarding daily business activities. The focus was on alignment between norm and rule compliance, which can help in mitigating security breaches, so the authors did not deliver anything about constructing flexible ISPs. Coertze and von Solms (2013) talks about a personalized and tailor-made word document that can be modified and adjusted to fit the specific needs of organizations and not the ISP that is tailored to individual users. Although the idea of tailored ISPs is somehow considered in these two papers the authors did not discuss more about this concept.

Author(s)	Tailored policy	User involvement
Abdelwahed et al, 2017; Abraham & Chengalur-smith, 2011; Al-Hamdani & Dixie, 2009; Al-Mukahal & Alshare, 2015; Bhardwaj et al., 2016; Buthelezi et al., 2016; Cherdantseva & Hilton, 2013; Cheung, 2014; Coertze et al., 2011; Choi, 2016; Corpuz, 2011; Corpuz & Barnes, 2010; Cosic & Boban, 2010; Doherty & Fulford, 2006; Gritzalis, 1997; Höne & Eloff, 2002 (a) Höne, Eloff, 2002 (b); Hong et al., 2006; Karlsson, et al., 2017; Knapp et al., 2009; Kolkowska & Decker, 2012; Koziel, 2011; Kurtel, 2008; Lapke & Dhillon, 2015; Lopes & Oliveira, 2015; Mader & Srinivasan,	No	No

2005; Palmer et al., 2001; Simms, 2009; Siponen & Iivari, 2006; Talbot & Woodward, 2009; Tuyikeze & Pottas, 2010; Von Solms et al., 2011; Yusufovna, 2008		
Almusharraf et al., 2015; Coertze & von Solms, 2013	B	No
Flowerday & Tuyikeze, 2016; Gaunt, 1998; Ismail & Widyarto, 2016; Kadam, 2007; Karyda et al., 2003; Karyda et al., 2005; Lindup, 1995; Maynard et al., 2011; Niemimaa., 2016; Renaud & Goucher, 2012	No	Yes

Table 1: Result of the mapping study

When it comes to involving users in constructing ISPs, we found 10 papers out of 46 that consider this issue. Lindup's (1995) study is one of the first papers that talk about involving users in ISP construction by identifying the problem of formulating ISP by a centralized group and suggested to use treaty instead. Karyda et al. (2003-2005), and Renaud and Goucher (2012) paid attention to user participation in the ISP construction process as a contextual factor for having a successful ISP. This point was considered by Gaunt (1998) as well when he talked about user consultation and involvement in preparation of ISPs. Ismail and Widyarto (2016) in the first phase of their conceptual model for ISP development showed that selecting an ISP team is important when construct a comprehensive ISP. They asserted that the proper policy team members should be consist of ICT security team, technical writer, technical personnel, legal counsel, human resource, and requires educations of the user group. They also declared that having opinions of all members in the team is needed to gain feedback and share knowledge; and ISP construction can be initiated when all these experts sit together. Maynard et al. (2011) is the only study that specifically talks about involving users in developing ISP among 46 papers, explains which stakeholders that should be involved in constructing ISP. However, this study does not specify how and where the stakeholders should be involved. Niemimaa (2016) conducted an ethnographic study to understand the construct of an organization-wide ISP and the practices that lead to successful ISP. In her study, she presented different users that were involved in the process; Yet, the user in her study were top representatives in the organization. Finally, Flowerday and Tuyikeze (2016) proposed a framework that determines several constructs to develop and implement ISP in an effective way. In their study, they have a section that address the issue Who should be involve in constructing and implementing ISPs. One of the groups that was mentioned were the "end-users". According to them, involving users in constructing ISPs "*results in their "buy-in" and support, while also creating a sense of ownership of the information security policy"* (Flowerday &Tuyikeze, 2016, P10). However, they did not explain how and when this involvement should be used.

5 Discussion and Conclusion

A literature mapping study was conducted to understand to what extent tailored information security policy (ISP) and user involvement have been considered in the literature. The findings revealed that there is no paper that considers a tailored ISP for employees; although some researchers mentioned the idea, none of them

discussed it as the result of their research. Järveläinen (2016) in his literature review argued that organizations can have several kinds of security policies for different employees and purposes. Based on that he identified the need for having tailored ISPs. However, this identification of need was not based on prior research and his focus was on proposing a solution. Our findings confirm this gap that tailored ISPs have not considered by researchers. Consequently, more research should be done regarding this concept. Our suggestion for future research is a) investigating how to construct an (effective) tailored ISP, and b) investigating the effect of tailored ISP on employee's compliance.

The findings also showed that user involvement in ISP construction got some attention from researchers (e.g. Maynard et al., 2011; Niemimaa, 2016). In contrast to the previous literature reviews in this area that only have emphasized on the importance of involving employees in the process of constructing ISPs (Tuyikeze & Flowerday, 2014; Järveläinen, 2016) the result of our study adds more in-depth overview regarding this concept in the literature. Actually, our study revealed the lack of attention about involving users in constructing ISPs and we could not find any paper that discusses how and where and when users should be involved. Accordingly, more studies are needed regarding user involvement specially in constructing tailored ISPs. Future research can focus on providing a roadmap on how to involve users in constructing tailored ISPs which can also be used as a practical guide for practitioners.

There were some limitations in this study that should be considered in future researches. Our study was based on research on Scopus and Web of science. We do not claim that we have identified all studies on ISP construction, however, we have used a good sample from the relevant outlets. Furthermore, we could not access all of the identified papers in our research which could affect the result of the study. Finally, analysing the papers is not free of subjective judgments which was needed to place the papers in the correct category (Yes/No/B).

6 References

Abdelwahed, A. S., Mahmoud, A. Y., & Bdair, R. A. (2016). Information Security Policies and their Relationship with the Effectiveness of the Management Information Systems of Major Palestinian Universities in the Gaza Strip. *International Journal of Information Science and Management (IJISM)*, *15*(1).

Abraham, S., & Chengalur-Smith, I. N. (2011). The Role of Conflict Resolution in Designing and Implementing Information Security Policies: An Institutional Perspective. In *AMCIS*.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers & Security, 29(4), 432-445.

Al-Hamdani, W. A., & Dixie, W. D. (2009, September). Information security policy in small education organization. In 2009 Information Security Curriculum Development Conference (pp. 72-78). ACM.

Al-Mukahal, H. M., & Alshare, K. (2015). An examination of factors that influence the number of information security policy violations in Qatari organizations. Information & Computer Security, 23(1), 102-118.

Almusharraf, A., Dhillon, G., & Samonas, S. (2015). Mismatched Understanding of Is Security Policy: A Repgrid Analysis.

Axelsson, J., & Skoglund, M. (2016). Quality assurance in software ecosystems: A systematic literature mapping and research agenda. Journal of Systems and Software, 114, 69-81.

Barki, H., & Hartwick, J. (1989). Rethinking the concept of user involvement. MIS quarterly, 53-63.

Baroudi, J. J., Olson, M. H., & Ives, B. (1986). An empirical study of the impact of user involvement on system usage and information satisfaction. Communications of the ACM, 29(3), 232-238.

Belsis, P., Kokolakis, S., & Kiountouzis, E. (2005). Information systems security from a knowledge management perspective. Information Management & Computer Security, 13(3), 189-202.

Bhardwaj, A., Subrahmanyam, G. V. B., Avasthi, V., & Sastry, H. (2016). Design a Resilient Network Infrastructure Security Policy Framework. Indian Journal of Science and Technology, 9, 19.

Buthelezi, M. P., Van Der Poll, J. A., & Ochola, E. O. (2016, December). Ambiguity as a Barrier to Information Security Policy Compliance: A Content Analysis. In 2016 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 1360-1367). IEEE.

Cherdantseva, Y., & Hilton, J. (2013, September). A reference model of information assurance & security. In 2013 International Conference on Availability, Reliability and Security (pp. 546-555). IEEE.

Cheung, S. K. (2014). Information Security Management for Higher Education Institutions. In Intelligent Data analysis and its Applications, Volume I (pp. 11-19). Springer, Cham.

Choi, M. (2016). Leadership of information security manager on the effectiveness of information systems security for secure sustainable computing. Sustainability, 8(7), 638.

Coertze, J., & von Solms, R. (2013, August). A software gateway to affordable and effective Information Security Governance in SMMEs. In 2013 Information Security for South Africa (pp. 1-8). IEEE.

Coertze, J., Van Niekerk, J., & Von Solms, R. (2011, August). A web-based information security management toolbox for small-to-medium enterprises in Southern Africa. In 2011 Information Security for South Africa (pp. 1-8). IEEE.

Condori-Fernandez, N., Daneva, M., Sikkel, K., Wieringa, R., Dieste, O., & Pastor, O. (2009, October). A systematic mapping study on empirical evaluation of software requirements

specifications techniques. In 2009 3rd International Symposium on Empirical Software Engineering and Measurement (pp. 502-505). IEEE.

Corpuz, M., & Barnes, P. H. (2010). Integrating information security policy management with corporate risk management for strategic alignment. In Proceedings of the 14th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2010).

Cosic, Z., & Boban, M. (2010, September). Information security management—Defining approaches to Information Security policies in ISMS. In IEEE 8th International Symposium on Intelligent Systems and Informatics (pp. 83-85). IEEE.

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: a review and research framework. European Journal of Information Systems, 26(6), 605-641.

Dhillon, G., & Torkzadeh, G. (2001). Value-focused assessment of information system security in organizations. ICIS 2001 Proceedings, 72.

Doherty, N. F., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. Computers & Security, 25(1), 55-63.

Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. computers & security, 61, 169-183.

Franke, U. and J. Brynielsson (2014). "Cyber situational awareness–a systematic review of the literature." Computers & Security 46: 18-31.

Gaunt, N. (1998). Installing an appropriate information security policy. International Journal of Medical Informatics, 49(1), 131-134.

Gritzalis, D. (1997). A baseline security policy for distributed healthcare information systems. Computers & Security, 16(8), 709-719.

Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2006). An empirical study of information security policy on information security elevation in Taiwan. Information Management & Computer Security, 14(2), 104-115.

Höne, K., & Eloff, J. H. P. (2002a). Information security policy—what do international information security standards say?. Computers & Security, 21(5), 402-409.

HöNe, K., & Eloff, J. H. P. (2002b). What makes an effective information security policy?. Network Security, 2002(6), 14-16.

Ismail, W. H. B. W., & Widyarto, S. A. (2016). Formulation and Development Process of Information Security Policy in Higher Education. In 1st International Conference on Engineering and Aplied Science (InCEAS)

Järveläinen, J. (2016). Integrated Business Continuity Planning and Information Security Policy Development Approach.

Kadam, A. W. (2007). Information security policy development and implementation. Information Systems Security, 16(5), 246-256.

Karlsson, F., Hedström, K., & Goldkuhl, G. (2017). Practice-based discourse analysis of information security policies. Computers & Security, 67, 267-279.

Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture–state-of-the-art review between 2000 and 2013. Information & Computer Security, 23(3), 246-285.

Karyda, M., Kokolakis, S., & Kiountouzis, E. (2003, May). Content, context, process analysis of IS security policy formation. In IFIP International Information Security Conference (pp. 145-156). Springer, Boston, MA.

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. Computers & Security, 24(3), 246-260.

Kitchenham, B., & Brereton, P. (2013). A systematic review of systematic review process research in software engineering. Information and software technology, 55(12), 2049-2075.

Knapp, K. J., Morris Jr, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. computers & security, 28(7), 493-508.

Kolkowska, E., & De Decker, B. (2012, June). Analyzing value conflicts for a work-friendly ISS policy implementation. In IFIP International Information Security Conference (pp. 339-351). Springer, Berlin, Heidelberg.

Koziel, G. (2011). Information security policy creating. Actual Problems of Economics, (12), 126.

Kurtel, K. (2008). Information Security Policy: positioning the technological components of information security services under the perspective of electronic business. In Security of Information and Networks: Proceedings of the First International Conference on Security of Information and Networks (SIN 2007) (p. 302). Trafford Publishing.

Lapke, M., & Dhillon, G. (2015). Disassociations in Security Policy Lifecycles. International Journal of Information Security and Privacy (IJISP), 9(1), 62-77.

Lindup, K. R. (1995). A new model for information security policies. Computers & security, 14(8), 691-695.

Lopes, I., & Oliveira, P. (2015). Applying action research in the formulation of information security policies. In New Contributions in Information Systems and Technologies (pp. 513-522). Springer, Cham.

Mader, A., & Srinivasan, S. (2005, September). Curriculum development related to information security policies and procedures. In Proceedings of the 2nd annual conference on Information security curriculum development (pp. 49-53). ACM.

Maynard, S. B., Ruighaver, A. B., & Ahmad, A. (2011). Stakeholders in security policy development.

Niemimaa, E. (2016). Crafting an Information Security Policy: Insights from an Ethnographic Study.

Palmer, M. E., Robinson, C., Patilla, J. C., & Moser, E. P. (2001). Information security policy framework: best practices for security policy in the e-commerce age. Information Systems Security, 10(2), 1-15.

Petersen, K., Feldt, R., Mujtaba, S., & Mattsson, M. (2008, June). Systematic mapping studies in software engineering. In Ease (Vol. 8, pp. 68-77).

Renaud, K., & Goucher, W. (2012). Health service employees and information security policies: an uneasy partnership?. Information Management & Computer Security, 20(4), 296-311.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. Computers & Education, 52(1), 92-100.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010, April). Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 373-382). ACM.

Simms, D. J. (2009, March). Information security optimization: From theory to practice. In 2009 International Conference on Availability, Reliability and Security (pp. 675-680). IEEE.

Siponen, M. (2006). Six design theories for IS security policies and guidelines. Journal of the Association for Information systems, 7(1), 19.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2009). Technical opinion Are employees putting your company at risk by not following information security policies? Communications of the ACM, 52(12), 145-147.

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 38(1), 60-80.

Slusky, L., & Partow-Navid, P. (2012). Students information security practices and awareness. Journal of Information Privacy and Security, 8(4), 3-26.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215-225.

Stahl, B. C., Doherty, N. F., & Shaw, M. (2012). Information security policies in the UK healthcare sector: a critical evaluation. Information Systems Journal, 22(1), 77-94.

Straub, D. and W. Nance (1990). "Discovering and Disciplining Computer Abuse in Organizations: A Field Study." MIS Quarterly 14(1): 45-60.

Talbot, S., & Woodward, A. (2009). Improving an organizations existing information technology policy to increase security.

Topa, I., & Karyda, M. (2015, september). Identifying Factors that Influence Employees' Security Behavior for Enhancing ISP Compliance. In International Conference on Trust and Privacy in Digital Business (pp. 169-179). Springer, Cham.

Tuyikeze, T., & Flowerday, S. (2014). Information Security Policy Development and Implementation: A Content Analysis Approach. In HAISA (pp. 11-20).

Tuyikeze, T., & Pottas, D. (2011). An information security policy development life cycle. In Proceedings of the South African Information Security Multi-Conference (SAISMC), Port Elizabeth, South Africa (pp. 165-176).

Von Solms, R., Thomson, K. L., & Maninjwa, P. M. (2011, August). Information security governance control through comprehensive policy architectures. In 2011 Information Security for South Africa (pp. 1-6). IEEE.

Yusufovna, S. F. (2008, October). Advanced security policy implementation for information systems. In 2008 International Symposium on Ubiquitous Multimedia Computing (pp. 244-247). IEEE.