Proceedings of the Ninth International Symposium on
Human Aspects of Information Security & Assurance (HAISA 2015)

Exploring the Link Between Behavioural Information Security Governance and Employee Information Security Awareness

W. Flores and M. Ekstedt

Industrial Information and Control Systems, Royal Institute of Technology
e-mail: waldorf@kth.se; mathias.ekstedt@ics.kth.se

Abstract

This paper explores the relation between a set of behavioural information security governance factors and employees' information security awareness. To enable statistical analysis between proposed relations, data was collected from two different samples in 24 organisations: 24 information security executives and 240 employees. The results reveal that having a formal unit with explicit responsibility for information security, utilizing coordinating committees, and sharing security knowledge through an intranet site significantly correlates with dimensions of employees' information security awareness. However, regular identification of vulnerabilities in information systems and related processes is significantly negatively correlated with employees' information security awareness, in particular managing passwords. The effect of behavioural information security governance on employee information security awareness is an understudied topic. Therefore, this study is explorative in nature and the results are preliminary. Nevertheless, the paper provides implications for both research and practice.

Keywords

Information security, behavioural information security governance, information security awareness

1. Introduction

The presence of new ways to compromise information security has moved the attention from an security approach with a technological focus to a more holistic approach to information security management (Kayworth and Whitten, 2010). Several approaches focusing on the "human" side of holistic information security management have, therefore, been proposed by researchers. These approaches can roughly be divided in two categories: (1) approaches focusing on the 'individual' level of information security to understand behaviours of individuals (goes under the name of behavioural information security research (Fagnot, 2008; Crossler et al., 2013)); (2) approaches focusing on the managerial level to understand which factors determine effective holistic information security governance and management (in this paper referred to as behavioural information security governance in line with the terminology used by Mishra and Dhillon (2006)). A dominant part of the studies have focused on the first category (Warkentin and Willison, 2009). These studies have increased the understanding of factors explaining information system misuse on an end-user level. However, there are limited studies investigating the effect of

behavioural information security governance, e.g., the establishment of organisational structures, processes and the implementation of security awareness programs on end-users perceptions of information security.

Although there are studies investigating the topic of behavioural information security governance, many of these studies have largely remained anecdotal (Puhakainen and Siponen, 2010). Existing work have proposed conceptual and practical principles that neither are theoretical grounded nor offer empirical evidence (e.g., Da Veiga and Eloff, 2007; Brotby, 2009; Sobh and Elleithy, 2013). Other works have based their empirical studies on best practice frameworks such as ISO/IEC 27002 (e.g., Chang and Ho, 2006; Dzazali and Zolait, 2012). Qualitative conclusions have also been drawn based on case studies or semi-structured interviews. Warkentin and Johnston (2007) attempted to understand the implications of two types of information security governance – centralized and decentralized governance. This comparative case study identified that organisations with a decentralized governance structure employees are responsible for their awareness training, while in organisations with a centralized governance structure formal awareness training were exclusively carried out by centralized IT personnel. Kayworth and Whitten (2010) developed a framework to support the attainment of information security strategy objectives. The components of the framework included nine organisational integration mechanisms (e.g., formal security unit, steering committee, information security embedded within key organisational processes) and four social alignment mechanisms (e.g., security awareness programs, executive commitment). All these aforementioned studies have increased the understanding of behavioural information security governance, and provided theoretical insights into the potential effects of an organisation's level of information security. However, none of them have empirically tested this effect, in particular, its effect of employees' information security awareness.

The purpose of this paper is to empirically examine the link between a set of behavioural information security governance factors and employees' information security awareness. This purpose is fulfilled by formulating the following research question:

RQ1: Which behavioural information security governance factors have a significant influence on employee information security awareness?

The rest of the paper is structured as follows. In section 2, the theoretical foundation related to behavioural information security governance and information security awareness is presented. In section 3, the methodology of the study is described. The section that follows presents the results from the empirical study employed in order to answer the study´s research question. The final section discusses the results and concludes the paper.

2. Establishing a theoretical foundation

The theoretical foundation of this paper is based on findings from an explorative research stage. This stage led to the development of a theory proposing how

behavioural information security governance might have an effect on employees' information security awareness. During this stage qualitative data was collected through interviews with six experts working with information security on a regular basis for 5 to 20 years. Of the six experts, three worked as senior information security consultants at two different information security consultancy firms; one worked as head of information security at a software application development firm; and the final two respondents were currently academics but with many years of practical experience as information security consultants (Rocha Flores and Ekstedt, 2013). The findings from the interviews were combined with searching literature to aid logical reasoning when establishing the theoretical foundation. In order to assure that we included relevant dimensions of behavioral information security governance and information security awareness, the comprehensiveness of the included factors was evaluated. This was done by collecting data through a survey completed by 18 content experts. For a more in-depth description of the underlying theory, the interested reader is recommended to turn to the following sources: Rocha Flores and Ekstedt (2012); Rocha Flores and Korman (2012); Rocha Flores and Antonsen (2013); Rocha Flores et al., (2014a). In sum, three factors were included to test the effects of behavioural information security governance on information security awareness: organisational structures, coordinating information security processes, and security knowledge sharing. In the following, these are described together with the information security awareness factor.

2.1. Organisational structures

Proper organisational structures facilitate the deployment of security efforts, and communication between executives, security personnel, and business representatives. This can help end-users to understand the importance of information security and how it can be used to support the business and not hinder it. Furthermore, structures ensure that the security function maintains alignment with business strategy, enable effective organisation of information security and contribute to the successful implementation and coordination of information security plans (Kayworth and Whitten, 2010). In this study, organisational structure is manifested through the two following forms of structures: formal structure (also referred to as a centralized information security structure) and coordinating structure such as the utilization of a diversity of coordinating information security committees.

2.2. Coordinating information security processes

Processes to coordinate information security efforts support the integration of information security in key organisational business processes (Kayworth and Whitten, 2010). This enables security to be a core element in the business environment and strengthen the link between high-level business requirements and operational security procedures. In our study, two key dimensions of coordinating processes were derived: risk management and performance monitoring. In order to coordinate any information security activities, the need for security should first be assessed by identifying vulnerabilities that can negatively affect business operations (Calder and Watkins, 2008). To support the coordination of information security,

controls need to be checked for their effectiveness in practice. They also need to be adapted to users' perceived level of obtrusiveness, and any changes in the business environment that might pose an IT-risk or negatively affect business operations.

2.1 Security knowledge sharing

Security knowledge sharing enable management of employee information security behaviour (Belsis et al., 2005; Zakaria, 2006). In the field of knowledge sharing, knowledge is considered as information processed by individuals including ideas, facts, expertise, and judgments relevant for the individual, team, and organisational performance (Wang and Noe, 2010). Knowledge sharing refers to the provision of task information and know-how to help others and to collaborate with others to solve problems, develop new ideas, or implement policies or procedures. The objective with security knowledge sharing is to increase or maintain information security knowledge among individuals in an organisation. In organisations, security knowledge sharing is manifested trough both formal means (e.g., security education and awareness training, policy communication), and informal means (e.g., informal consulting and advisory services). The sharing of knowledge is facilitated by the use of technology (e.g., intranet-based knowledge management systems) (Cummings, 2004; Rhodes et al., 2008).

2.3. Information security awareness

Achieving employee information security awareness has been recognized as a critical outcome of information security management programs (Werlinger et al., 2009; Kayworth and Whitten, 2010). Therefore, studies have focused on assessing information security awareness in order to identify strategies to increase employees' awareness (Karakasiliotis et al., 2006; Dodge et al. 2007; Rocha Flores et al., 2014c). In this study information security awareness is defined as an employee's general knowledge about information security threats, and his or her knowledge of specific information security policies related to information security. This means that an employee can be aware of threats related to information security based on past experience or interest. The employee can also be aware of the organisations specific information security policies regulating proper security behaviour. This is a result of specific training on policies that the organisation has provided their employees. Hence, information security awareness can be shaped by the individual's own interest and experiences or by interventions carried out by the organisation's information security management group.

3. Methodology

To test the effect of behavioural information security governance on information security awareness, empirical studies were conducted at 24 organisations. We aimed to examine all relationships between dimensions of behavioural information security governance and information security awareness. Figure 1 shows which relationships that were examined on a high abstraction level. Figure 2 shows how the empirical study was carried out.

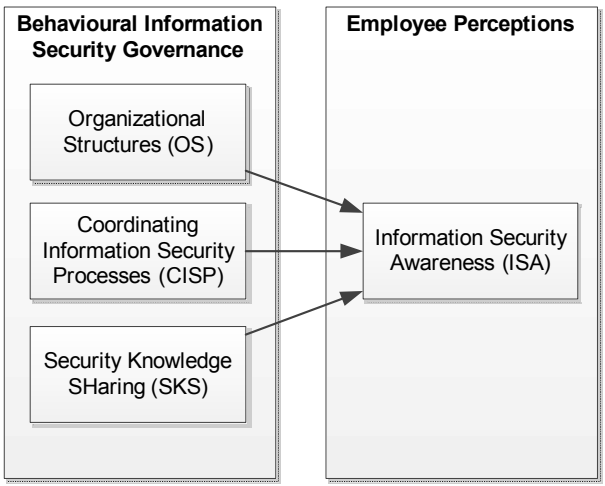

Figure 1: Examined relationships on a high level of abstraction

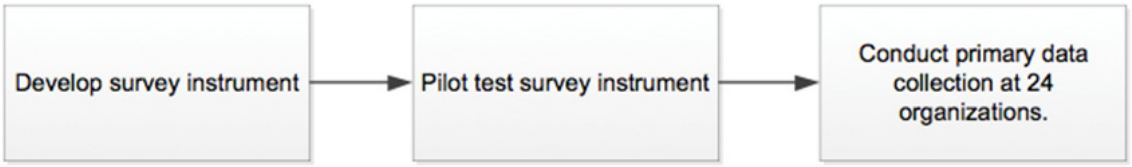

Figure 2: Research process

3.1. Development of survey questions

In the present study we correlated all survey questions related to the dimensions of behavioural information security governance and information security awareness. All survey questions were inspired on existing scales, but adapted and rewritten for the context of our study. Questions related behavioural information security governance were developed based on our understand of the factors through previous research (Rocha Flores and Ekstedt, 2012; Rocha Flores and Korman, 2012; Rocha Flores and Antonsen, 2013; Rocha Flores et al., 2014a). Questions related to the general information security awareness were based on Bulgurcu et al. (2010) and adapted to this study. Questions related to information security policy awareness were based on interviews with the six information security experts during the first stage of the research.

3.2. Assess content validity of survey questions

When developing new survey questions, MacKenzie et al. (2011) recommends to assess the content validity of the questions before colleting primary data. We quantitatively assessed the content validity using the item-sorting method (Anderson and Gerbing, 1991). The survey questions were tested for their content validity by collecting data using an email survey distributed to 452 content domain experts, of which 51 completed the survey. We also asked for comments on wording and if the survey questions were clearly understood. For more information on specific changes, the interested reader is referred to Rocha Flores and Antonsen (2013).

3.1 Pilot test and finalizing the survey questions

A pilot test was conducted by distributing the survey to 200 IT users known to the research department and working in different organisations and industries. After one reminder 47 employees had completed the survey. The survey asked for comments on wording, if the survey items were clearly understood and if the survey could be improved. Based on this pilot test minor corrections were made to the wording of the survey questions. All questions in the final survey measured on an 11-point Likert scale from 0 to 10, where 10 was strongly agree and 0 was strongly disagree. The final survey questions are outlined in Table 1.

Organisational structures (OS)
OS1: We have an organisational unit with explicit responsibility for organizing and coordinating information security efforts as well as handling incidents.
Coordinating organisational structures (COS)
OS2: There is a committee, comprised of representatives from various business units, which coordinates corporate security initiatives.
OS3: There is a committee, which deals with matters of strategic information security and related decision-making.
OS4: Tactical and operative managers are involved in information security decision-making, which is related to their unit, responsibilities and/or subordinates.
OS5: In our organisation, people responsible for security and representatives from various business units meet to discuss important security issues, both formally and informally.
Coordinating information security processes (CISP)
CISP1: Information about risks across business processes is considered.
CISP2: Vulnerabilities in the information systems and related processes are identified regularly.
CISP3: Threats that could harm and adversely affect critical operations are identified regularly.
CISP4: Performance of information security controls is measured, for example with regards to the amount of protection they provide as well as the obtrusiveness and performance limitations they pose to personnel, systems and business activities.
Security knowledge sharing
SKS1: Formal information security exercises take place in our organisation (e.g., training of backup procedures or reaction on security incidents).

SKS2: In our organisation, there is a formal program for information security awareness, training and education.
SKS3: Our organisation provides informal/voluntary consulting and advisory services in information security for our employees.
SKS4: There is an intranet site dedicated to information security (e.g., general threats and howtos, policy and guidelines).
SKS5: There is an intranet site, a quality control system or another information system or portal, which contains work- and task-related information security information such as cues, reminders or warnings bound to an action, process or a situation.
SKS6: Information technology is actively used to share knowledge and experience regarding information security within our organisation.
SKS7: Our organisation saves and renews important knowledge on both general information security and threats related to information security onto the computer for easy browsing.
Information security awareness
ISA1: I am aware of the potential threats and negative consequences that inadequate information security in my work can cause.
ISA2: I understand the risks posed by inadequate information security in general.
ISA3: I am aware of how acceptable use of IT products and services (e.g. computers, the Internet, e-mail, etc.) are described in our policy.
ISA4: I am aware of how acceptable installation of software is described in our policy.
ISA5: I know how our policy governs management of sensitive and confidential information.
ISA6: I am aware of my obligations under our policy regarding the use and management of passwords for my work computer.

Table 1: Survey items

3.3. Primary data collection

To statistically test the proposed relationships, we attempted to collect data from as many organisations as possible. To identify potential respondents the key informant methodology was used. The key informant methodology advocates that respondents should be identified based on their position, experience, and professional knowledge rather than by the traditional random sampling procedure (Segars and Grover, 1999). In this study, we decided to include two key informants. The first group of respondents was each organisation's high-level executives such as CISOs, Security Officers, CEOs, CIOs, and IT managers. This group was given the survey on behavioural information security governance factors. The second group was

employees of each organisation, and these employees were given the survey including the information security awareness construct.

To identify potential respondents, security executives from organisations that were both known and unknown to the research department were contacted and invited to participate in the research study. In total, executives from 50 organisations were contacted trough telephone or email. They received a letter explaining the purpose of the study and were asked about their organisations' willingness to participate in the research study. Each information security executive was instructed to select and ensure that at least a sample of 10 employees from their organisations would complete the survey. In total, 24 companies participated in the study. The data collection procedure was identical for each of the participant organisations. To facilitate the data collection the researchers worked in close cooperation with the executives from participating organisations. The survey was hosted by a widely used internet-based application (SurveyMonkey 2014). After two reminders, 1420 employees from the 24 organisations had completed the survey. Of the organisations five are in energy; seven in manufacturing; four in IT industries; three wastewater treatment services; two in the government and academic sector; and one each in financial services, healthcare, and retail/wholesale. Three of the participant organisations had more than 5000 employees; three of the participant organisations had between 1000-5000 employees; three of the participant organisations had between 500-999 employees; five of the participant organisations had between 100-499 employees; and ten had less than 100 employees. Among the respondents, 63 percent where male and 37 percent female; 53 percent were older than 45 years, and 47 percent younger than 45 years.

As previously described, each information security executive was instructed to ensure that at least a sample of 10 employees from their organisations would complete the survey. In 11 organisations the sample was exactly 10 employees, and in the remaining 13 the sample was large than 10. As this was something that the researchers could not control, and a statistical analysis of data was to be conducted, 10 respondents were randomly selected per organisation with a sample larger than 10. Hence, the total sample comprised 240 employees from 24 different organisations.

4. Analysis and results

In order to analyse the relationship between investigated variables, Pearson correlation was used (Cohen and Cohen 1983). To enable correlation tests, the mean value of the responses to each survey question from the 10 selected respondents were calculated. This yielded a unique score per survey question for each organisation. The results from testing the relationships are shown in Table 2.

	ISA1	ISA2	ISA3	ISA4	ISA5	ISA6
OS1	.251	.480**	.347*	.488**	.248	.121
OS2	-.164	.002	-.099	.041	-.076	-.202
OS3	-.122	.065	-.072	.031	-.009	-.178
OS4	.063	.233	.163	.177	.189	.031
OS5	.123	.371*	.235	.434*	.159	.016
CISP1	-.068	.083	-.118	.002	-.029	-.270
CISP2	-.228	-.081	-.177	-.124	-.159	-.401*
CISP3	.041	.078	.114	.118	.228	.083
CISP4	.114	.118	.228	.041	.083	.078
SKS1	.010	-.034	-.078	-.079	.037	-.156
SKS2	-.144	.063	.154	.287	.000	.109
SKS3	-.001	.048	.082	.057	.152	-.102
SKS4	.215	.382*	.390*	.488**	.257	.167
SKS5	.221	.138	.144	.163	.120	.047
SKS6	.205	.302	.158	.162	.148	.011
SKS7	.200	.258	.158	.080	.184	-.011

Table 2: Overall results from correlation analysis
Notes: * indicates statistical significance at $p < 0.05$; ** at $p < 0.01$.

As the results display our empirical analysis reveal that there are 9 significant relationships between the investigated behavioural information security governance variables and information security awareness. Specifically, formal information security structure has a significant correlation with employees understanding of the risks posed by inadequate information security in general (r = 0.347**), employees awareness of how the policy describe acceptable use of IT products and services (r = 0.480**), and how acceptable installation of software is described in the policy (r = 0.488**). Furthermore, establishing routines that people responsible for security and representatives from various business units meet to discuss important security issues correlates with both employees understanding of the risks posed by inadequate information security in general (r = 0.371**) and awareness of how acceptable installation of software is described in the policy (r = 0.434**). A positive significant correlation was identified between the establishment of an intranet site dedicated to information security and employees understanding of the risks posed by inadequate information security in general (r = 0.382**), employees awareness of how the policy describe acceptable use of IT products and services (r = 0.390**), and how acceptable installation of software is described in the policy (r = 0.488**). Finally, regular identification of vulnerabilities in information systems and related processes is significantly negatively correlated with employees' awareness of policy regulating obligations regarding the use and management of passwords for work computers (r = -0.401**).

5. Discussion and conclusions

Our study has empirically investigated the effect of behavioural information security governance on employee information security awareness. To the best of our

knowledge this is the first empirical study investigating this link. The study can therefore be seen as exploratory, which limits the generalizability of our findings. Our results points to the usefulness of having a specific unit with explicit responsibility for organizing and coordinating information security, and routines that people responsible for security and representatives from various business units meet to discuss important security issues both formally and informally. One explanation could be that information security is highly prioritised in organisations that have these structures in place. This might be manifested by leaders promoting information security and communicating the role and responsibility of the information security department of the organisation. This could then serve as the foundation to shape an information security culture, which in turn directly influences employees' awareness of information security threats. As there is a relative hierarchical distance between the structural mechanisms and employee perceptions, future studies should attempt to disentangle the interrelated influences of formal structures and employees perceptions of information security.

Support for security knowledge transfer by using technology such as intranet site dedicated to information security (e.g., general threats and howtos, policy and guidelines), seem beneficial as it influence employees' perception of information security. Apparently, employees are keen to use technology to learn about information security and making them aware of common threats. This is beneficial, as using different tools (e.g. e-learning tools) to share knowledge about information and educate employees is a cheap investment and can easily reach all members of an organisation.

Finally, regular identification of vulnerabilities in information systems and related processes is significantly negatively correlated with employees' awareness of policy regulating obligations regarding the use and management of passwords for work computers. At this point we do not have a strong explanation why this relationship is negative. One might believe that vulnerability analysis would increase information security. However, one explanation could be that vulnerability analysis, as posed by the question, is regarded as a technical measure to identify weaknesses in the information system, and not in humans accessing these information systems. Could it be that companies investing in technical vulnerability analyses lack in providing 'social' controls to their employees? Consequently, companies might be overinvesting in technical countermeasure leading to less focus on countermeasures related to employees'' information security awareness. Naturally, future research should investigate this question further.

There exist several limitations which should be taken into account when interpreting the results. First, out of 114 relationships that were statistically tested, only 9 showed significant correlation. Hence, this questions the effect of the dimensions of behavioural information security governance that we identified through the explorative stage of the research. Consequently, future research should include other governance variables that could potentially have a stronger link to employee information security awareness.

Second, although our study identified significant correlation between dimensions of behavioural information security governance and information security awareness, the sample is still small. Therefore, conclusions based on the results from our correlation analysis should be drawn cautiously. However, the study sheds a light on the effect of behavioural information security governance on employee information security awareness, which is an understudied topic. Therefore, this study contributes by providing results that researcher can use in their future studies.

6. References

Anderson, J.C. & Gerbing, D.W., 1991. Predicting the performance of measures in a confirmatory factor analysis with a pretest assessment of their substantive validities. *Journal of Applied Psychology*, 76(5), pp.732–740.

Brotby, K., 2009. *Information Security Governance*, John Wiley & Sons, Inc.

Calder, A. & Watkins, S., 2008. *IT governance A manager´s guide to Data Security and ISO 27001/ISO 27002* 4th ed., Kogan Page.

Chang, S. & Ho, C., 2006. Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, 106(3), pp.345 – 361.

Cohen, J. & Cohen, P., 1983. *Applied multiple regression/correlation analysis for the behavioral sciences*, NJ: Erlbaum: Hillsdale.

Crossler, R.E. et al., 2013. Future directions for behavioral information security research. *Computers & Security*, 32(null), pp.90–101.

Cummings, J.N., 2004. Work Groups, Structural Diversity, and Knowledge Sharing in a Global Organization. *Management Science*, 50(3), pp.352–364.

Dodge, R., Carver, C. & Ferguson, A., 2007. Phishing for user security awareness. *Computers & Security*, 26(1), pp.73–80.

Dzazali, S. & Zolait, A.H., 2012. Assessment of information security maturity: An exploration study of Malaysian public service organizations. *Journal of Systems and Information Technology*, 14(1), pp.23–57.

Fagnot, I.J., 2008. Behavioral information security. In L. Janczewski & A. Colarik, eds. *Encyclopedia of cyber warfare and cyber terrorism*. PA: USA: Hershey, pp. 199–205.

Karakasiliotis, A., Furnell, S. & Papadaki, M., 2006. Assessing end-user awareness of social engineering and phishing. In *Australian Information Warfare and Security Conference*. Citeseer, p. 60.

Kayworth, T. & Whitten, D., 2010. Effective Information Security Requires a Balance of Social and Technology Factors. *MIS Quartely Executive*, 9(3), pp.303–315.

MacKenzie, S.B., Podsakoff, P.M. & Podsakoff, N.P., 2011. Construct measurement and validation procedures in MIS and behavioral research: integrating new and existing techniques. *MIS Quarterly*, 35(2), pp.293–334.

Mishra, S. & Dhillon, G., 2006. Information Systems Security Governance Research: A Behavioral Perspective. In *2nd Annual Symposium on Information Assurance*. New York State.

Puhakainen, P. & Siponen, M., 2010. Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, 34(4), pp.757–778.

Rhodes, J. et al., 2008. Factors influencing organizational knowledge transfer: implication for corporate performance. *Journal of Knowledge Management*, 12(3), pp.84–100.

Rocha Flores, W. et al., 2014. Using Phishing Experiments and Scenario-based Surveys to Understand Security Behaviours in Practice. *Information Management & Computer Security*, 22(4).

Rocha Flores, W. & Antonsen, E., 2013. The development of an instrument for assessing information security in organizations: Examining the content validity using quantitative methods. In *Proceedings of the 2013 International Conference on Information Resources Management*. Natal, Brazil, May 22-24.

Rocha Flores, W., Antonsen, E. & Ekstedt, M., 2014. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, 43(June), pp.90–110.

Rocha Flores, W. & Ekstedt, M., 2012. A Model for Investigation Organizational Impact on Information Security Behavior. In *Seventh Annual Workshop on Information Security and Privacy (WISP) 2012*.

Rocha Flores, W. & Ekstedt, M., 2013. Countermeasures for Social Engineering-based Malware Installation Attacks. In *Proceedings of the 2013 International Conference on Information Resources Management*. Natal, Brazil, May 22-24.

Rocha Flores, W. & Korman, M., 2012. Conceptualization of Constructs for Shaping Information Security Behavior: Towards a Measurement Instrument. In *Proceedings of th 7th Annual Workshop on Information Security and Privacy*. Orlando, Florida, USA, December 16.

Segars, A.H. & Grover, V., 1999. Profiles of Strategic Information Systems Planning. *Information Systems Research*, 10(3), pp.199–232.

Sobh, T. & Elleithy, K. eds., 2013. Information Management for Holistic, Collaborative Information Security Management. In *Emerging Trends in Computing, Informatics, Systems Sciences, and Engineering*. Lecture Notes in Electrical Engineering. New York, NY: Springer New York, pp. 211–224.

SurveyMonkey, 2014. SurveyMonkey: Free online survey software & questionnaire tool. Available at: https://www.surveymonkey.com/.

Da Veiga, A. & Eloff, J.H.P., 2007. An Information Security Governance Framework. *Information Systems Management*, 24(4), pp.361–372.

Wang, S. & Noe, R.A., 2010. Knowledge sharing: A review and directions for future research. *Human Resource Management Review*, 20(2), pp.115–131.

Warkentin, M. & Johnston, A.C., 2007. It Governance and Organizational Design for Security Management. In D. W. Straub, S. Goodman, & R. L. Baskerville, eds. *Information Security: Policy, Processes, and Practices*. pp. 46 – 68.

Warkentin, M. & Willison, R., 2009. Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, 18(2), pp.101–105.

Werlinger, R., Hawkey, K. & Beznosov, K., 2009. An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, 17(1), pp.4–19.

Zakaria, O., 2006. Internalisation of Information Security Culture amongst Employees through Basic Security Knowledge. In S. Fischer-Hübner et al., eds. *Security and Privacy in Dynamic Environments*. IFIP International Federation for Information Processing. Boston: Kluwer Academic Publishers, pp. 437–441.