Establishment of Security Knowledge Sharing in Organisations: An Empirical Study

W.R. Flores

Department of Industrial Information and Control Systems, Royal Institute of Technology, Stockholm, Sweden
e-mail: waldorf@ics.kth.se

Abstract

The purpose of the present study is to empirically investigate what drives the establishment of security knowledge sharing in organisations. Based on a theoretical understanding a research model was developed and tested by collecting and analysing data from 62 security executives from a diverse set of organisations located in different geographic regions in the world. The empirical tests of a structural model revealed that all proposed hypotheses are accepted, except the hypotheses proposing a positive link between business-based information security and the establishment of security knowledge sharing. Organisational structure has a major direct influence on the establishment of security knowledge sharing in organisations, while the effect of coordinating information security process is moderate. A mediation analysis revealed that the reason for the nonsignificant direct relation between business-based information security and security knowledge sharing is the fully mediating effect of coordinating information security process. Thus, coordinating information security process has an important role on security knowledge sharing by either partially or fully mediating the effects of both organisational structure and business-based information security on security knowledge sharing. Implications and recommendation for future research are further discussed.

Keywords

Information security, knowledge sharing, partial least squares structural equation modelling

1. Introduction

The increased dependence and use of IT products and services has forced organisations to manage risks and ensure information security related to those products and services. Organisations often try to ensure information security by establishing a security infrastructure based on technological solutions. These solutions are useful, and their effectiveness and robustness has made it more difficult to successfully attack computer systems using purely technical means. Many attackers have therefore started to include social means in their malicious efforts and target the humans accessing and using IT products and services (Applegate 2009). The danger of focusing exclusively on technological solutions and the presence of new ways to compromise information security has moved the attention to a more holistic approach to information security, comprising of both technological and social factors (Kayworth & Whitten 2010). Such a socio-technical approach emphasizes the importance of taking account of the human element in establishing information security in an organisation. The understanding of how to manage various

elements of information security is however limited (Dhillon & Backhouse 2001) and empirically research on organisational drivers for the establishment of information security components is even more under-investigated. Factors that are discussed in the extant literature is usually assumed to have an impact on different information security components independently of each other (ISACA 2006; Kayworth & Whitten 2010). As a consequence there is a need to consider research that investigates how to govern and manage dimension of information security in general and socio-organisational dimensions of information security in particular.

Awareness of risks with IT usage, and knowledge on how to prevent, detect and react to security breaches are important facets of a social approach to information security (Dontamsetti & Naranayan 2009; Applegate 2009). In order to increase employee security knowledge, organisations establish different social mechanisms (Kayworth & Whitten 2010). These mechanisms can be manifested through processes of capturing and transferring knowledge of information security, such as establishing security awareness programs, conducting security exercises and implementing IT-based knowledge sharing solutions (Rocha Flores & Ekstedt 2012). The establishment of security knowledge sharing arrangements in a firm depends on how information security is organised and structured. In line with this premise, its logical to argue that it is important to understand determinants of the establishment of information security knowledge sharing in firms. The purpose of the study is therefore to obtain a deeper understanding of how firms structure and organise themselves to enable sharing of information security knowledge to organisational members. In line with the purpose of the study, the following research question was formulated:

Which determinants have a major influence on the establishment of security knowledge sharing in organisations?

In an attempt to answer the research question, data from 62 information security executives from a diverse set of organisations was collected and analysed. The rest of the paper is structured as follows. In the following section, theory is outlined and the hypotheses are developed. The section that follows presents the methodology used to conduct the research. The data is then analysed and presented. Finally, the paper ends with the results being discussed and conclusions being drawn.

2. Theory and Hypothesis Development

2.1 Security Knowledge Sharing

As the focus of information security has shifted from the use of technology-based resources to more tacit resources, human knowledge sharing has emerged as an important factor to manage IT-related risks. In general, knowledge sharing has three dimensions: generation of knowledge, codification of knowledge and transferring of knowledge. In an organisational context, knowledge can either be generated by acquiring or developing it within the organisation (Davenport & Prusak 1998). Thus, organisations can hire information security specialists to perform activities that increase knowledge of information security, or have dedicated units within the

organisation that are responsible for those activities. Codification of knowledge refers to the process of making knowledge accessible to those who need it. Companies can save and renew important information security knowledge onto computers for easy browsing and use an intranet site to make information on work task-related risks accessible. Knowledge is transferred when people interact with each other by sharing experience or helping one another. Information security personnel can, for instance, engage in boundary-spanning activities to improve security knowledge sharing among organisational constituents (Kayworth & Whitten 2010). Companies can also provide informal consulting and advisory services to other areas of the company, provide workshops, exercises and training to transfer knowledge (Davenport & Prusak 1998). In the present study security knowledge sharing is conceptualized in two dimensions; formal knowledge sharing arrangements and support for knowledge transfer. Thus, this study aims at understanding what leads firms to establish those two dimensions of knowledge sharing.

2.2 Determinants of Security Knowledge Sharing

The effectiveness of organisational knowledge sharing is influenced by key organisational factors such as structure, processes and strategy (Rhodes et al. 2008). These factors are now described more thoroughly. The descriptions provide the basis for the development of hypotheses linking organisational determinants to the establishment of security knowledge sharing.

Processes to coordinate information security support the integration of information security in key organisational business processes or services and enable security to be a core element in the business environment and thereby strengthen the link between high-level business requirements and operational security procedures (Kayworth & Whitten 2010). In order to coordinate any information security activities, it is first imperative to assess the need for security by identifying vulnerabilities that can negatively affect business operations (Calder & Watkins 2008). Identifying security vulnerabilities in an organisation provides an understanding of risks that need to be mitigated for the protection of its information resources help management make informed information security-related decisions (Sun et al. 2006). In order to coordinate information security, controls need to be checked for their effectiveness in practice. It is therefore imperative that organisations continually receive information on any changes in its business environment that might pose a risk to their information systems (Sun et al. 2006). Establishing performance monitoring ensures that the proper security controls are in place and adapted to the needs of the recipients. Thus, it is a logical deduction to believe that coordinating information security processes influence the establishment of knowledge sharing activities in an organisation. Therefore, the following hypothesis is proposed:

H1: Coordinating information security processes is positively associated with the organisation's establishment of security knowledge sharing.

The information security strategy need to be aligned with the business strategy to ensure that information security is based on actual business needs and not hinders the business from conducting their strategic and operational activities (Kayworth & Whitten 2010). Thus, it is crucial to balance the need to enable the business against the need to secure information assets. Aligning any security activities to business needs is a prerequisite for effective security. Strategic alignment is manifested if a firm's departments act on the firm's business strategy by outlining strategies, plans, and investments that are based on an understanding and knowledge of the business objectives, value, or needs (Henderson & Venkatraman 1993). A deep understanding of the business environments, processes and the organisational goals enables the development of effective IS strategies, provides information services that fit organisational needs and enable IT workforce to conduct proper risk assessments Firms with business competent security executives conduct proper management of information assets and effective allocation of resources (Chang & Wang 2010). Therefore, this paper explores the role of security executives with an understanding of organisational business goals and needs on an organisation's coordinating information security and establishment of security knowledge sharing. This state is referred as business-based information security, and the following two hypotheses are proposed:

H2a: Business-based information security is positively associated with the organisation's coordinating information security processes.

H2b: Business-based information security is positively associated with the organisation's establishment of security knowledge sharing.

Successful companies generally attribute a significant part of their success to good organisation. The design of organisations is therefore one of management's major priorities (Child 1984). Structure has a central role to the design of an effective organisation. Structure is defined as means for attaining the objectives and goals for an organisation (Drucker 1974). In an information security context, structure enables effective organisation of information security and contributes to the successful implementation of information security plans. Further, structure supports the assignment of both technical and human resources to the tasks which have to be done and provide mechanisms for their coordination. Structure also establishes and enables strategic- and operational decision-making and monitoring of performance, and also operating mechanisms that transfers directives on what is expected of organisational members and how the directives can be followed (Child 1984). In this study, organisational structure is manifested through formal structure such as the existence of an organizational unit with explicit responsibility for organizing and coordinating information security, and coordinating structures such as the existence of responsible functions (e.g. senior-level information security executives), and a constitution of a diversity of coordinating security committees and teams that meet to discuss important security issues both formally and informally (Kayworth and Whitten 2010). To understand the impact of organisational structure in the context of information security, the following hypotheses are postulated:

H3a: Organisational structure is positively associated with the establishment of the organisation's security knowledge sharing.

H3b: Organisational structure is positively associated with the organisation's coordinating information security processes.

H3c: Organisational structure is positively associated with the organisation's business-based information security.

The proposed research hypotheses are summarized in figure 1. The interested reader can find further details on the definitions of the investigated constructs and how they were conceptualized in Rocha Flores & Korman (2012).

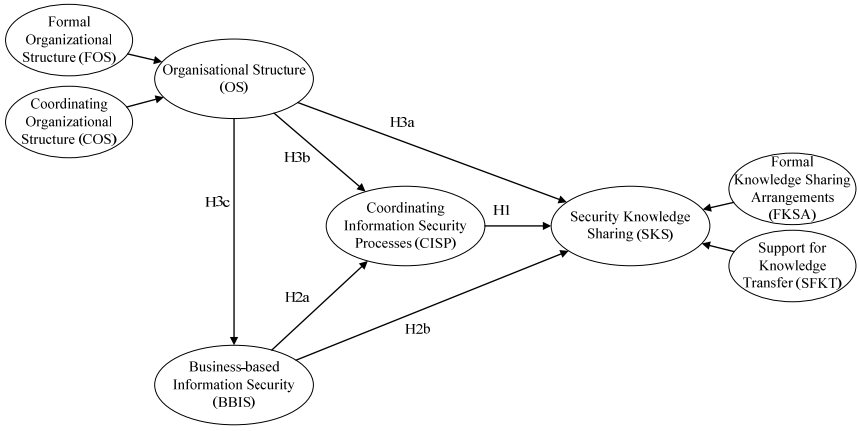

Figure 1: Research model

3. Research Methodology

Due to the challenges in collecting empirical data in the critical domain of information security (Kotulic & Clark 2004), we used the survey method to test our proposed research model.

3.1 Item Development and Content Validity Assessment

The survey items were based on two previous studies; an inductive study with six information security specialists (Rocha Flores & Ekstedt 2012), and a conceptualization of constructs in which an assessment of dimension comprehensiveness and relevance with empirical data from 18 content domain experts was conducted (Rocha Flores & Korman 2012). Security knowledge sharing and organisational structure were operationalised as formative second-order constructs composed of two reflective first-order constructs each: formal knowledge sharing arrangements (FKSA) and support for knowledge transfer (SFKT) represented security knowledge sharing; and formal organisational structure (OS) and coordinating organisational structure (COS) represented organisational structure. These constructions are referred to as a type II second-order construct models (Jarvis et al. 2003). Coordinating information security processes (CISP) was specified with formative items, and the other five first-order construct were specified with reflective

multiple items. When possible, the items were based on existing scales that have been proven reliable. Items representing business-based information security (BBIS), were identified from previous work (Chang & Wang 2010; Spears & Barki 2010). Thus, a major part of the items were developed specifically for this study. When developing new items, MacKenzie et al. (2011) recommends to assess the content validity of the items before colleting primary data. Therefore, we first quantitatively assessed the content validity using the item-sorting method proposed by Anderson & Gerbing (1991). This was done for all constructs except BBIS, by obtaining data from 56 content domain experts. We also asked for comments on wording and if the survey items were clearly understood and if they perceived that any items were missing to represent the construct. Based on this pre-test the survey instrument was revised and the initial item pool of containing 34 newly developed items was reduced to 18 items with an adequate degree of content validity. We however decided to exclude two more items for further analysis as they could not be answered by our intended sample without a potential problem associated with common method bias (P. M. Podsakoff et al. 2003). By adding four, already tested and reliable, items representing BBIS, the final survey included 20 items (Cf. Appendix), all measured on a 11-point licker scale from 0 to 10 inspired by Paternoster & Simpson (1996) and Siponen & Vance (2010).

3.2 Primary Data Collection

The SANS security mailing list (GPWN-list), was initially adopted as a sampling frame. The mailing list comprises security executives, senior managers, and managers with operational responsibilities and other practitioners with an interest in information security such as security analysts, security architects and pen-testers. To choose 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 & Grover 1999). In our study, the key informants included such high-level executives as CISOs, Security Officers, CEOs, CIOs, and IT managers. From this sampling frame, we identified 548 potential respondents. We also approached security executives from 10 organisations that were known to the research department and asked them to complete the survey. In total, the sample therefore included 558 potential respondents. Data was collected in November and December of 2012. The survey was hosted by a widely used internet-based application (SurveyMonkey). Two reminders were sent to non-responding participants after a first week and a third week in order to increase the response rate. Out of 558 e-mail requests that where sent, 38 bounced or were unregistered from the mailing list. After two reminders 85 had opened the survey and 62 respondents had completed the survey, which gives an effective response rate of 11.1 %. At first glance, the response rate may seem rather low. However, Rogelberg & Stanton (2007) argue that the response rate alone is an inaccurate and unreliable proxy for study quality. The response rate in this study is understandable given that data is collected in the critical domain of information security and that managers have been oversurveyed due to the increased popularity of using online surveys to capture organisational managers' attitudes and beliefs related to different types of organisational issues (Rogelberg & Stanton 2007).

To address potential nonresponse bias the last respondent method was used as recommended by (Armstrong & Overton 1977) and used in Bulgurcu et al. (2010). The method assumes that non-respondents are like the projected last respondent in the last wave of data collection (final reminder). The dataset was split in three groups and a series of independent t-tests was conducted to identify any significant differences in means between the first and the last third of the respondents' data. This test procedure revealed no significant differences between the first and the last third of the respondents' data on any of the items analysed. This suggests that nonresponse bias was not an issue in this study.

The respondents in the sample represent a diverse set of industries and their organisation represents diverse industry groups. Twenty-nine percent of the responding organisations are in IT industries; 16 percent are in the government and academic sector; 15 percent in manufacturing and retail; 11 percent are in financial services and insurance industries; 11 percent are in telecommunication services; 5 percent in Energy; 5 percent in Health care; and 8 percent were categorised as "other". A significant part of the organisations were located in the United States (41.9 percent), Sweden (16.1 percent), Finland (8.1 percent) and United Kingdom (4.8 percent). However, we also received answer from Japan, Egypt, Bermuda, Israel and Turkey. 40 percent of the organisations had more than 500 employees; 19 percent had less than 100 employees; 14 percent between 1000-5000 employees; 14 percent between 100-499; and 12 percent 500-999 employees. A significant number (71 percent) of the respondents are senior executives with job titles such as CISOs, CSOS, CIOs, CEOs, and IT managers. Other titles that the respondents reported to have are; Director of information security, Head of cyber defence section, Information security manager, Cyber security manager, Head of sub-division and Business manager of Critical Infrastructure & industrial security. Further, 87 percent had work with information security within an organisation for 10 or more years.

4. Data Analysis and Results

Partial least squares structural equation modelling (PLS-SEM) was used to test the measurement model's psychometric properties and structural model. PLS-SEM was used instead of covariance-based techniques due to the sample size, the including of a formative construct in the model, and that the focus of the study is to explain variance of the included endogenous variables (Hair et al. 2011). The data set was first screened to identify any outliers as recommended by Hair et al. (2011). This process yielded the identification of four outliers, which were removed for further analysis. We then turned to using SmartPLS the software package (version 2.0.M3)(C.M. Ringle et al. 2005) for the estimations.

4.1 Quality of Measurement Model

Construct validity for the formative construct (CISP) was assessed by examining indicator weights and signs of multicollinearity. Formative measures should not be highly correlated and the variance of a formative indicator should not be explained by the other constructs' indicators. A variance inflation factor less than 5 indicates acceptable shared variance (Hair et al. 2011). One of the formative items indicated to cause correlation (VIF > 5), and was therefore removed for further analysis. As table 1 shows, the remaining formative items had significant weights and acceptable VIFs (* at $p < 0.05$; and ** at $p < 0.01$).

Indicator	VIF	Outer weights
CISP1	1,723	0,478**
CISP2	2,415	0,280*
CISP4	2,068	0,398**

Table 1: Formative construct validity for Coordinating information security processes

The reflective measures were assessed through internal consistency reliability, indicator reliability, and convergent validity and discriminant validity. Composite reliability and Cronbachs alpha should be higher than 0.7 for adequate internal consistency reliability. Indicator loadings should be higher than 0.7 for acceptable indicator reliability. If the average variance extracted (AVE) yields a value higher than 0.5, convergent validity is established. Discriminant validity is established if the square root of each constructs' AVE is higher than the correlation with any other construct and indicator loadings is higher than all of its crossloadings (Hair et al. 2011). As tables 2 and 3 show, all items were assessed to be both valid and reliable and could thus be used to evaluate the structural model.

	CA	CR	AVE	BBIS	CISP	COS	FKSA	FOS	SFKT
BBIS	0.927	0.949	0.822	**0.907**					
CISP	n/a	n/a	n/a	0.716	n/a				
COS	0.887	0.923	0.750	0.612	0.792	**0.866**			
FKSA	0.749	0.888	0.799	0.624	0.771	0.702	**0.894**		
FOS	1.000	1.000	1.000	0.505	0.684	0.693	0.591	1.000	
SFKT	0.918	0.939	0.754	0.630	0.778	0.824	0.649	0.622	0.868

Table 2: Correlations, Cronbachs alpha, Composite reliability and AVE

	BBIS	**COS**	**FKSA**	**FOS**	**SFKT**
BBIS1	**0.866**	0.575	0.656	0.447	0.537
BBIS2	**0.950**	0.557	0.574	0.483	0.551
BBIS3	**0.939**	0.557	0.523	0.485	0.569
BBIS4	**0.870**	0.529	0.508	0.417	0.620
COS1	0.501	**0.885**	0.630	0.656	0.713
COS2	0.495	**0.910**	0.608	0.649	0.736
COS3	0.503	**0.763**	0.465	0.411	0.690
COS4	0.625	**0.898**	0.712	0.656	0.721
FKSA1	0.657	0.669	**0.901**	0.539	0.604
FKSA2	0.454	0.584	**0.887**	0.516	0.555
FOS1	0.505	0.693	0.591	**1.000**	0.622
SFKT1	0.636	0.698	0.599	0.462	**0.830**
SFKT2	0.392	0.659	0.516	0.605	**0.850**
SFKT3	0.424	0.723	0.509	0.522	**0.864**
SFKT4	0.651	0.744	0.623	0.609	**0.894**
SFKT5	0.616	0.750	0.567	0.501	**0.901**

Table 3: Item loadings and cross loadings for reflective indicators

Finally, the threat of the common methods bias (CMB) was addressed. Ex ante, we addressed CMB by removing two items that we believed our sample were not appropriate to answer (the question was more targeted to end users), counterbalancing the order of questions in the questionnaire to discourage participants from figuring out the relationship between the dependent and independent variables that we were trying to establish. Further, the respondent's anonymity and providing no incentive for completing the survey reduced the likelihood of bias caused by social desirability or respondent acquiescence (P. M. Podsakoff et al. 2003). Ex-post, we performed a test for CMB recommended by Bagozzi et al. (1991) and used by Pavlou et al. (2007) wherein the correlation matrix was examined to identify any highly correlated constructs ($r > 0.9$). In our model, all constructs had correlations below the threshold (Cf. table 2). The ex ante and ex post tests suggest that the possibility of CMB is not of great concern and therefore it's unlikely that CMB confounds the interpretation of the results.

4.2 Evaluation of Structural Model

In order to assess the significance structural path coefficients, bootstrapping re-sampling method with 62 cases and 1000 re-samples was used. The R^2 values of the endogenous constructs measures how much variance is explained by the exogenous constructs. R^2 values of 0.75, 0.50, or 0.25 can be described as substantial, moderate, or weak, respectively. As figure 2 shows, all hypotheses, except H2b are accepted. The R^2 value for the dependent variable of security knowledge sharing is 0.78, which indicates that the constructs in the model explains 78 percent of the variance in the dependent variable. Thus, the proposed model has a strong explanatory power and explains a substantial amount of variance in security knowledge sharing. Organisational structure explains 39 percent of the variance in business-based information security, and together with business-based information security organisational structure explains 78 percent of variance in coordinating information security processes. As security knowledge sharing and organisational structure were

operationalised as formative second-order constructs, the significance of the first-order weights were examined. The weights indicated that the each sub-dimension significantly contribute to their underlying factor. Among the determinants of establishment of security knowledge sharing, organisational structure has the strongest direct effect on the dependent variable. The direct effect has a regression coefficient of $\beta = 0.55$. The links between organisational structure and coordinating information security processes and business-based information security are significant, with $\beta = 0.60$ and $\beta = 0.62$, respectively. The link between business-based information security and coordinating information security processes is also significant with $\beta = 0.38$. Finally, coordinating information security have a significant direct effect on knowledge sharing with $\beta = 0.27$. To assess the mediating effect of coordinating information security processes, three tests of mediation was tested using Sobel's (Sobel 1987). The test revealed that coordinating information security processes partly mediates the effect of organisational structure, and fully mediates the effect of business-based information security, on security knowledge sharing. Thus, business-based information security in an organisation affects security knowledge sharing completely trough a processes that coordinates information security. Finally, business-based information security partly mediates the effect of organisational structure on security knowledge sharing.

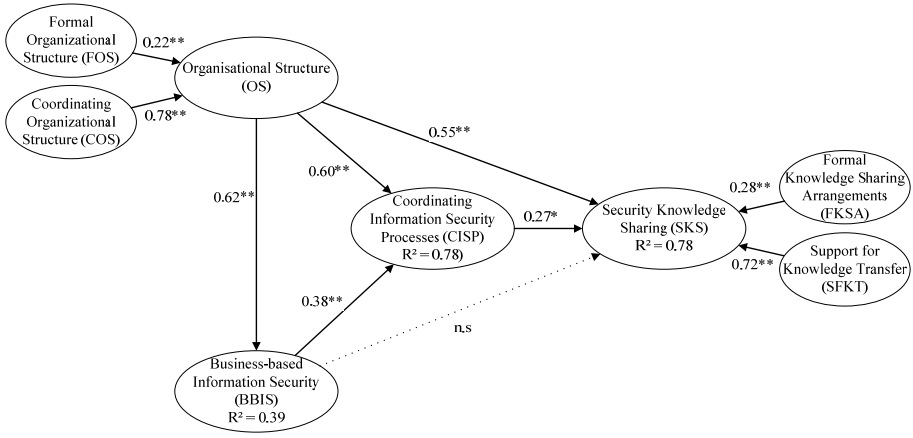

Figure 2: Results of Structural Model Testing

Notes: n.s indicates statistically non-significant; * at $p < 0.05$; and ** at $p < 0.01$.

5. Discussions and Conclusions

This study examines the effect of three organisational factors – organisational structures, business-based information security and coordinating information security processes – in an attempt to increase the understanding of determinants of the establishment of security knowledge sharing in organisations. Based on theoretical understanding, a research model was developed and tested by collecting and analysing data from 62 security executives from a diverse set of organisations located in different geographic regions in the world. The empirical tests of a

structural model revealed that all our proposed hypotheses are accepted, except the hypotheses proposing a positive direct link between business-based information security and the establishment of security knowledge sharing. The results of the study imply that organisational structure has a major direct influence on the establishment of security knowledge sharing in organisations. A mediation analysis indicates that the reason for the nonsignificant direct relation is the mediating role of coordinating information security process. The mediation analysis reveals that coordinating information security process has an important role on security knowledge sharing by either partially or fully mediating the effects of organisational structure and business-based information security on security knowledge sharing.

The literature of factors to govern various information security components is often anecdotal or qualitative and has investigated them from a standpoint that assumes their independence from one another. This study therefore provides empirical evidence on what drives organisations' to establish security knowledge sharing.

There exist several limitations which should be taken into account when interpreting the results. First, a general limitation is that we assume that the establishment of security knowledge sharing can be measured using survey methods. Second, although we collected data on type of industry and size of the organisation, we didn't investigate the direct effect of these two factors on the establishment of security knowledge sharing. The reason for this is that we explicitly wanted to investigate governance or management factors that influence security knowledge sharing and not characteristics of the firm. We acknowledge the potential impact of these factors and therefore recommend including them in future work. Third, we collected data from a diverse set of industries and countries and we can therefore say that the study is both a cross-cultural and cross-national study. However, we chose to not highlight this fact, as we believe that the sample size is too small for us to draw any conclusions on identified differences based on this observed heterogeneity which we argue are important to draw if data is collected from multiple industries and countries. It would therefore be interesting to collect more data using our approach to analyse any potential differences based on heterogeneity.

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.

Applegate, S.D., 2009. Social Engineering: Hacking the Wetware! *Information Security Journal: A Global Perspective*, 18(1), pp.40–46.

Armstrong, J.S. & Overton, T.S., 1977. Estimating Nonresponse Bias in Mail Surveys. *Journal of Marketing Research*, 14, pp.396–402.

Bagozzi, R.P., Yi, Y. & Phillips, L.W., 1991. Assessing construct validity in organizational research . *Administrative Science Quarterly*, 36(3), pp.421–458.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I., 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), pp.523–548.

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

Chang, K. & Wang, C., 2010. Information systems resources and information security. *Information Systems Frontiers*, 13(4), pp.579–593.

Child, J., 1984. *Organization: A guide to Problems and Practice* 2nd ed., London: Paul Chapman Publishing Ltd.

Davenport, T.H. & Prusak, L., 1998. *Working Knowledge: How Organizations Manage What They Know*, Boston : Harvard Business School Press.

Dhillon, G. & Backhouse, J., 2001. Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, 11(2), pp.127–153.

Dontamsetti, M. & Naranayan, A., 2009. Impact of the Human Element on Information Security. In *Social and Human Elements of Information Security Emerging Trends and Countermeasures*. IGI Global, pp. 27–43.

Drucker, P.F., 1974. New templates for today's organizations. . *Harvard Business Review*, (January-February).

Hair, J.F., Ringle, Christian M. & Sarstedt, M., 2011. PLS-SEM: Indeed a Silver Bullet - Tags: STRUCTURAL equation modeling MARKETING. *Journal of Marketing Theory & Practice*, 19(2), p.139.

Henderson, J.C. & Venkatraman, N., 1993. Strategic alignment: leveraging information technology for transforming organizations. *IBM Systems Journal*, 32(1), pp.4–16.

ISACA, 2006. *Information Security Governance Guidance for Boards of Directors and Executive Management, 2nd Edition*,

Jarvis, C.B., MacKenzie, S.B. & Podsakoff, P.M., 2003. A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research. *Journal of Consumer Research*, 30(2), pp.199–218.

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

Kotulic, A.G. & Clark, J.G., 2004. Why there aren't more information security research studies. *Information & Management*, 41(5), pp.597–607.

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.

Paternoster, R. & Simpson, S., 1996. Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime. *Law & Society Review*, 30(3), pp.549–584.

Pavlou, P.A., Liang, H. & Xue, Y., 2007. Understanding and mitigating uncertainty in online exchange relationships: a principal- agent perspective. *MIS Quarterly*, 31(1), pp.105–136.

Podsakoff, P.M. et al., 2003. Common method biases in behavioral research: a critical review of the literature and recommended remedies. *The Journal of applied psychology*, 88(5), pp.879–903.

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

Ringle, C.M., Wende, S. & Will, A., 2005. SmartPLS.

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. & Korman, M., 2012. Conceptualization of Constructs for Shaping Information Security Behavior: Towards a Measurement Instrument. In *Seventh Annual Workshop on Information Security and Privacy (WISP) 2012*.

Rogelberg, S.G. & Stanton, J.M., 2007. Introduction: Understanding and Dealing With Organizational Survey Nonresponse. *Organizational Research Methods*, 10(2), pp.195–209.

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

Siponen, M. & Vance, A., 2010. Neutralization: new insights into the problem of employee systems security policy violations. *MIS Quarterly*, 34(3), pp.487–502.

Sobel, M.E., 1987. Direct and Indirect Effects in Linear Structural Equation Models. *Sociological Methods & Research*, 16(1), pp.155–176.

Sun, L., Ivastave, R.P. & Mock, T.J., 2006. An Information Systems Security Risk Assessment Model Under the Dempster-Shafer Theory of Belief Functions. *Journal of Management Information Systems*, 22(4), pp.109–142.

Appendix

The items that were used are presented as follows:
FOS1: We have an organizational unit with explicit responsibility for organizing and coordinating information security efforts as well as handling incidents.
COS1: There is a committee, comprised of representatives from various business units, which coordinates corporate security initiatives.
COS2: There is a committee, which deals with matters of strategic information security and related decision making.
COS3: Tactical and operative managers are involved in information security decision making, which is related to their unit, responsibilities and/or subordinates.
COS4: In our organization, people responsible for security and representatives from various business units meet to discuss important security issues both formally and informally.
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~~ (removed)
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.

BBIS1: Our security department is very well informed about each unit's business operations, strategies and risks related to them.
BBIS2: Our security department aligns their strategies with our organization's business strategies.
BBIS3: Our security department understands the business goals of our organization.
BBIS4: Strategic decisions on information security policies and solutions are largely business-driven; that is, they are based on business objectives, value, or needs.
FKSA1: Formal information security exercises take place in our organization (e.g., training of backup procedures or reaction on security incidents).
FKSA2: In our organization, there is a formal program for information security awareness, training and education.
SFKT1: Our organization provides informal/voluntary consulting and advisory services in information security for our employees.
SFKT2: There is an intranet site dedicated to information security (e.g., general threats and howtos, policy and guidelines).
SFKT3: 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.
SFKT4: Information technology is actively used to share knowledge and experience regarding information security within our organization.
SFKT5 Our organisation saves and renews important knowledge on both general information security and threats related to information security onto the computer for easy browsing.