Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture

Waldo Rocha Flores*, Egil Antonsen, Mathias Ekstedt
Industrial Information and Control Systems
Royal Institute of Technology
10044 Stockholm, Sweden
Telephone: +46 8 790 68 38
Fax: +46 8 790 68 39
waldorf@kth.se*, egila@kth.se, mathias.ekstedt@ics.kth.se
*Corresponding author

Abstract

This paper presents an empirical investigation on what behavioral information security governance factors drives the establishment of information security knowledge sharing in organizations. Data was collected from organizations located in different geographic regions of the world, and the amount of data collected from two countries – namely, USA and Sweden – allowed us to investigate if the effect of behavioral information security governance factors on the establishment of security knowledge sharing differs based on national culture.

The study followed a mixed methods research design, wherein qualitative data was collected to both establish the study's research model and develop a survey instrument that was distributed to 578 information security executives. The results suggest that processes to coordinate implemented security knowledge sharing mechanisms have a major direct influence on the establishment of security knowledge sharing in organizations; the effect of organizational structure (e.g., centralized security function to develop and deploy uniform firm-wide policies, and use of steering committees to facilitate information security planning) is slightly weaker, while business-based information security management has no significant direct effect on security knowledge sharing. A mediation analysis revealed that the reason for the non-significant direct relation between business-based information security management and security knowledge sharing is the fully mediating effect of coordinating information security processes. Thus, the results disentangles the interrelated influences of behavioral information security governance factors on security knowledge sharing by showing that information security governance sets the platform to establish security knowledge sharing, and coordinating processes realize the effect of both the structure of the information security function and the alignment of information security management with business needs.

A multigroup analysis identified that national culture had a significant moderating effect on the association between four of the six proposed relations. In Sweden – which is seen as a less individualist, feminine country – managers tend to focus their efforts on implementing controls that are aligned with business activities and employees' need; monitoring the effectiveness of the implemented controls, and assuring that the controls are not too obtrusive to the end user. On the contrary, US organizations establish security knowledge sharing in their organization through formal arrangements and structures. These results imply that Swedish managers perceive it to be important to involve, or at least know how their employees cope with the decisions that have been made, thus favoring local participation in information security management, while US managers may feel the need to have more central control when running their information security function.

The findings suggest that national culture should be taken into consideration in future studies – in particular when investigating organizations operating in a global environment – and understand how it affects behaviors and decision-making.

Keywords Information security, knowledge sharing, cultural differences, mixed methods research, partial least squares structural equation modelling, multigroup analysis.

1. Introduction

As the technological solutions with the purpose to prevent information system from being compromised have increased in effectiveness and robustness, attackers have been forced to find new means to attain their objectives. Many attackers have started to include social means in their malicious efforts and target employees accessing and using IT products and services (Applegate, 2009). The presence of new ways to compromise information security has moved the attention to a more holistic approach to information security management comprising technological, organizational and social components (Kayworth and Whitten, 2010). A holistic information security management approach emphasizes the importance of taking account of the "human" element when ensuring information security throughout the organization. That is, attitudes, beliefs, norms, behavioral patterns, leadership, culture, employee awareness etc. (e.g., Albrechtsen, 2007; Dhillon and Backhouse, 2001; Siponen, 2005). 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) information security approaches focusing on the 'individual' level of information security to understand why end-users engage in risky behavior; (2) information security approaches focusing on the managerial level to understand which organizational factors determine effective holistic information security management. Puhakainen and Siponen (2010), however, criticized information security approaches as lacking not only theoretically grounded methods, but also empirical evidence on their effectiveness. As a possible consequence of this critique, the recent years have witnessed an increase in investigations that meet these criteria, and have based their analyses on a variety of theories including theory of planned behavior (Bulgurcu et al., 2010), neutralization theory (Siponen and Vance, 2010), learning theory (Warkentin et al., 2011), organizational narcissism (Cox, 2012), and protection motivation theory (Ifinedo, 2012). A dominant part of the studies have focused on the first category (Warkentin and Willison, 2009) – that is, the 'individual' level of information security by either testing theories that explain an individual's compliance/non-compliance to information security policies (e.g., Ifinedo, 2012) or how perceptions of different information security countermeasures such as education and awareness training might lead to a decrease in information system abuse or misuse (e.g., D'Arcy, Hovav, and Galletta, 2008). While these studies have increased the understanding of information system misuse on an end-user level, they do not investigate the effect of factors on a managerial level of information security; e.g., the establishment of organizational structures and governance procedures to ensure that proper interventions are in place to support employees to not engage in risky behavior. Research focusing on behaviors of individuals related to the protection of information and information system assets goes under the name of behavioral information security research (Fagnot, 2008; Crossler et al., 2013). Consequently, the governance of information security behavior is referred to as behavioral information security governance and in line with the terminology used by Mishra and Dhillon (2006)).

Existing work related behavioral information security governance have proposed different approaches to help firms organize and structure their information security initiatives. First, conceptual and practical principles that neither are theoretical grounded nor offer empirical evidence have been proposed (e.g., 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), and the use of best practice frameworks have been criticized by Siponen and Willison (2009) for being generic or universal in scope and thus not pay enough attention to the differences between organizations and their information security requirements. Finally, qualitative conclusions have been drawn based on case studies or semi-structured interviews. Warkentin and Johnston (2007) conducted a comparative case study in which information security controls were considered within both a centralized and decentralized governance environment. The study identified, for instance, that users in the later environment are responsible for their own awareness training, while the development and implementation of formal training programs in the centralized environment are only carried out by IT personnel. Werlinger, Hawkey, and Beznosov (2009) built an integrated framework of information security challenges based on a total of 18 human, organizational, and technological challenges identified by conducting 36 semi-structured interviews with information security practitioners. Kayworth and Whitten (2010) developed a framework to support the attainment of information security strategy objectives. The components of the framework included nine organizational integration mechanisms (e.g., formal security unit, steering committee, information security embedded within key organizational processes) and four social alignment mechanisms (e.g., security awareness programs, executive commitment). While all the aforementioned approaches have increased the understating of problems related to behavioral information security governance, and potential solutions to those problems, none of them have developed and empirically tested a theoretical model that include behavioral information security governance constructs. In fact, by reviewing related work the authors of the present paper only found four studies that fulfil this criteria (Straub, 1990; Kankanhalli, 2003; Knapp et al., 2007; Chang and Wang, 2010). Considering the lack of empirical studies related to behavioral information security governance, the present study aims at complementing the body of literature on behavioral information security governance by exploring, developing, and empirically testing a theoretical model explaining the establishment of security knowledge sharing throughout an organization. The reason for focusing on a knowledge-related construct is twofold: (1) most employees, unfortunately, lack the sufficient information security knowledge (Belsis et al., 2005) that could minimize risks that, if realized, might lead to intrusions and security violations; (2) studies have identified that knowledge-related constructs are the main predictors of an individual's behavioral intentions and decision making and thus are critical to take into account to mitigate security risks (e.g. Hu et al., 2012; Bulgurcu et al., 2012).

Why do employees lack sufficient information security knowledge? Belsis et al. (2005) argue that the lack of sufficient information security knowledge among employees can be explained by the low-level user involvement when developing and establishing different security practices. This might lead to practices not being aligned with actual user needs. Another explanation is how rules and regulations regarding the protection of information assets are communicated. In general, security policies are used for this purpose, but oftentimes policies are static documents reflecting a firm's security goals at the time of their creation. Thus, if polices are not monitored and adapted to both the changing organizational environment and new external threats, security knowledge among employees is difficult to achieve and maintain. Finally, there might be a lack of specific expert knowledge among the personnel providing security services, and as a consequence provided security services are neither relevant to a firm's current context nor implemented effectively. One theoretical perspective that can help inform our understanding of the establishment of processes to enable management of employee behavior is knowledge sharing (Belsis et al., 2005; Zakaria, 2006) which has received much attention in the field of knowledge management as it is critical for organizations to achieve competitive advantage (Davenport and Prusak, 1998). 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 organizational 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. Knowledge sharing is manifested trough both formal (e.g., education, policy communication), and informal (e.g., informal consulting and advisory services) means, and supported by the use of technology (e.g., intranet-based knowledge management systems) (Cummings, 2004; Rhodes et al., 2008). Hence, we argue that knowledge sharing can be seen as a latent variable and policy communication or security awareness and training programs, for instance, are instances of security knowledge sharing (or manifestations of the latent variable). In other words: policy communication or security awareness and training programs are means or mechanisms to increase or maintain information security knowledge between individuals in an organization (Zakaria, 2006).

Based on the above discussed gaps in the literature related to behavioral information security governance, and the need to generate, capture and share information security knowledge to mitigate the risk of employees engaging in risky behavior, the purpose of this research is to examine and identify behavioral information security governance factors that have a significant influence on security knowledge sharing. To attain the first objective of the study, the following research question was formulated:

RQ1: Which behavioral information security governance factors have a significant influence on the establishment of security knowledge sharing in organizations?

An interesting question could now be raised: is the influence of behavioral information security governance factors on security knowledge sharing consistent across different settings? Previous studies in the field of behavioral information security have tested different theories to explain why organizational members engage in risky behaviors. However, although testing the same theory (e.g., deterrence theory, theory of planned behavior) the findings have been inconsistent (D'Arcy and Herath, 2011; Sommestad et al., 2013). One proposed explanation for these disparate findings is that the theoretical models have not been tested for their validity across different cultural settings (Karjalainen et al., 2013; Sommestad et al., 2013). This implies that national culture could be seen as a moderating variable and thus could have an effect on the relationships in the theoretical models by making them stronger, weaker or non-significant. Previous empirical information system studies supports this premise by showing that differences exists in cross-national organizational behavior when testing theory of planned behavior (Pavlou and Chai, 2002), and Technology Acceptance Model (TAM) (Bandyopadhyay and Bandyopadhyay, 2010).

However, the role of cultural factors in information security contexts has received limited attention. A prominent study conducted within the field of information security is the study by Dinev et al. (2009) in which user behavior towards protective information technologies was investigated by empirically testing a behavioral model using data collected from respondents in USA and South Korea (Dinev et al., 2009). Hofstede's (Hofstede, 1980) five national culture indices was further included as moderating variables. The results revealed that the national culture moderated three out of five proposed relationships in the model. Thus, there are strong reasons to believe that there is no security strategy or procedure that fit all contexts, indicating that organizations should consider cultural factors in order to design effective information security practices. The study by Dinev et al. (2009) is one of very few studies in the information security domain that have taken potential cultural effects into consideration. Crossler et al. (2013) argues that those effects need to be considered as national culture likely has a direct impact on various elements of information security, and calls for studies that are adapted to account for cross-cultural differences. The present study focuses on behavioral information security governance, and within that specific domain there are, to the knowledge of the authors, no study empirically examining if the results from testing developed theoretical models hold across different cultural settings. Consequently, the second objective of the study is to examine if the effect of behavioral information security governance factors on the establishment of security knowledge sharing differs based on national culture. Two different countries with contrasting cultures were studied: Sweden and the USA. Those countries are interesting to examine more closely as they both are democracies with well-developed economies, but represent two different cultures according to Hofstede's national culture indices (Hofstede, 2013). To attain the second objective of the study, the following research question was specified:

RQ2: Will the effect of behavioral information security governance factors on the establishment of security knowledge sharing differ between Swedish and US organizations?

The rest of the paper is structured as follows. In section 2, the theoretical foundation related to security knowledge sharing and national culture is presented. In section 3, the research model of the study is established through an exploratory study. The section that follows presents the confirmatory study testing the proposed research model in order to answer the study´s two research questions. Finally, the paper ends with a discussion of the results and conclusions of the work.

2. Theoretical background

In order to understand how knowledge sharing is manifested in information security contexts we first obtained a basic understanding of what knowledge sharing is, why it's important, and how it can be achieved in organizations. Therefore, general theory of knowledge sharing is first described. Then, we provide the limitations of the existing work on security knowledge as arguments for the present research. Further, as the second objective of the study is to examine if national culture moderates the effect of behavioral information security governance factors on security knowledge sharing, we present cross-cultural dimensions and argue for the potential existence of differences in the findings for Swedish and US organizations.

2.1 Knowledge sharing and limitations in security knowledge sharing research

As recognized by Davenport and Prusak (1998), knowledge sharing is not simple, as knowledge by itself is abstract and therefore difficult to grasp. Knowledge has been described as a mixture of experience, values, contextual information, and expert insight that supports an individual to evaluate and incorporate new experience and information (Davenport and Prusak, 1998). An individual that is able to efficiently handle both new experience and information, and apply it in different scenarios, is often described as a "knowledgeable individual". Human knowledge, data and information altogether defines organizational knowledge, and when properly shared among organizational members, is a valuable asset which can be used to aid decision making, improve efficiency, reduce training cost, and reduce risks due to uncertainty (Sarmento, 2005; Pai, 2006; Song, 2002).

Knowledge sharing can either be explicit or tacit. A simple explanation of explicit knowledge sharing is knowledge that can be articulated in words, codified, and transferred through guidelines, documents, and how-to videos. Tacit knowledge is more difficult to formally transfer as it resides in the minds of certain individuals and has not been codified in a structured form (Pai, 2006). However, Pai (2006) argue that effective knowledge sharing mechanisms can help individuals to effectively share both their implicit and tacit knowledge.

Knowledge can be generated by acquiring or developing it within the organization (Davenport and Prusak, 1998). In information security contexts, generation of knowledge can be manifested through information security specialists being hired to perform activities that increase information security knowledge, or having dedicated units within the organization 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 knowledge onto computers for easy browsing and use an intranet site to make information on work task-related information security risks accessible. Knowledge is transferred when people interact with each other by sharing experience or helping one another. Dedicated information security personnel can, for instance, engage in boundary-spanning activities to improve security knowledge sharing among organizational constituents. Companies can also provide informal information security consulting and advisory services to other areas of the company, provide workshops, exercises and training to transfer knowledge. Thus, establishment of knowledge sharing is beneficial as the individual knowledge possessed by information security professionals is transformed into organizational knowledge and transferred to end users and other stakeholders. This prevents security-related information and tacit knowledge from being laid scattered throughout the organization or preserved by information security personnel as their personal property (Belsis et al., 2005).

Knowledge sharing has been broadly studied in the information security economics literature. Gordon, Loeb, and Lucyshyn (2003) have examined how sharing knowledge (information) across firms affects the overall investment level in information security products. Gal-Or and Ghose (2005) analyzed how the sharing of security knowledge by two firms influences security investments and price competition between these firms. Liu, Ji, and Mookerjee (2011) examined the relationship between security investment decisions and knowledge sharing between two similar firms. Studies based on technical knowledge sharing management system and the effects on the improvement of information security sharing between different organizations have been conducted. For instance, Feledi and Fenz (2012) investigated how machine-readable information security knowledge was shared between information security experts from the different organizations on the basis of a web portal.

While both the economic impacts of information security investments and the use of technical knowledge sharing management systems on knowledge sharing have been studied in the aforementioned research studies, the establishment of security knowledge sharing in an organization to increase or maintain employees' security knowledge hasn't, to the knowledge of the authors, empirically been studied. Efforts have been made to conceptually understand the integration of information security and knowledge management principles based on the knowledge management ontology (Guo, 2008). Zakaria (2006) presents a framework for how basic security knowledge can be achieved through knowledge sharing activities. Belsis et al. (2005) explored the sources of information security knowledge and the potential role of an information security knowledge management system. A theoretical model to illustrate the structure of information security knowledge in an organization was developed based on field research involving five organizations and five security experts and consultants.

In the present study, we focus on governance factors. However, as the field of information security knowledge sharing is under-investigated, we are not convinced that general knowledge management theories apply in the information security field. Consequently, an exploratory study was employed in the first phase of the research process. The purpose of this first phase was to establish the study constructs that were quantitatively measured in the second phase.

2.2 Cross-cultural dimensions

A predominant used cultural framework in the IS research context (Srite and Karahanna, 2006) is the framework proposed and validated by Hofstede (1993) in which culture is defined as: "the collective programming of the mind that distinguishes one group or category of people from another" (Hofstede, 1993). The cultural framework is based on five distinct dimensions: Power distance (PDI), Individualism versus collectivism (IDV), Masculinity versus femininity (MAS), Uncertainty avoidance (UAI), and Long-term versus short-term orientation (LTO). The cumulative difference between USA and Sweden's individualism (20) and masculinity (57) indices is larger than the cumulative difference between Power distance (9), Uncertainty avoidance (17), and Long-term versus short-term orientation (9) indices. Thus, we believe that the moderating effect of national culture can be explained by these two cultural dimensions.

USA scores 91 and Sweden scores 71 in the individualism dimension, the USA is therefore seen as having a more individualist culture and Sweden as having a less individualist culture (Hofstede, 2013). In cultures where individualism is stronger the ties between individuals are loose and they are expected to take care of themselves and their immediate families only. On the contrary, in less individualist cultures individuals think it's more important to consider the interest of their group before themselves and individuals can expect their members of a particular in-group to look after them in exchange for loyalty (Hofstede, 2013). A less individualist culture may therefore lead to organizational members being more loyal to their organization than they would in a nation in where a individualist culture is more predominant (Boyacigiller and Adler, 1991). If adherence to organizational rules and regulation is seen as being loyal, managers in a less individualist culture may perceive they don't need to regulate employee behavior as explicit as they would in a more individualist culture. Information security executives pertaining to societies where individualism is more prominent (e.g. USA) may, therefore, perceive that they need to control and regulate their employees' behavior through formal means.

The USA scores 62 on the masculinity dimension and is considered a "masculine" society, while Sweden scores 5 on this dimension and is therefore a feminine society. The masculinity dimension measures the degree a society reinforces the traditional masculine work role model of achievement, competition, control and power. In a country in which masculinity is stronger, success is defined by winning or being the best in the field. Higher status is achieved by working and trying to be as good one can be. Typically, conflicts are resolved at the individual level and the goal is to win the discussion without negotiation. On the contrary, in a feminine society the dominant values are caring for others and quality of life is the sign of success. Managers tend to be more supportive to their people, they strive for consensus, decision-making is achieved through involvement, and conflicts are resolved by compromise and negotiation (Hofstede, 2013). Consequently, US information security managers will tend to not include their people in their security-related decisions, while Swedish managers may care for how their implemented decisions affect their people and involve them in decisions on potential changes in the organizational environment, thus favoring local participation. Furthermore, Tan et al. (2004) and Dinev et al. (2009) have argued that the masculinity index also moderates people's attitudes in the same direction as individualism does. Therefore, it's reasonable to believe that, a goal- and achievement-oriented information security manager from a masculine culture will be more prone to act based on his or her individually formed convictions and perceived need to control his or her people. On the other hand, a manager from a feminine culture perceives personal beliefs and need for formal control mechanism as less important and relationships to their people will be seen as more important.

3. Research model development

This study followed a mixed methods research design, and was carried out through two main stages: an exploratory stage, and a confirmatory stage. The reason for employing an exploratory study in the first stage of the research was that important constructs related to behavioral information security governance and its influence on security knowledge sharing were unknown, and relevant quantitative instruments were not available. The exploratory stage both resulted in the establishment of the study's research model and informed the second, quantitative stage in where a measurement instrument was developed and used to empirically test the research model. This methodology is known as a mixed methods research design (also labelled as multi-method research design and pluralist methodology) (Creswell and Plano Clark, 2011). Figure 1 illustrates the research process which is based on the suggestions by previous work (Lee, 1991; Trochim and Donnelly, 2006; MacKenzie et al., 2011; Creswell and Plano Clark, 2011). This section describes the research and results of the exploratory stage, and the confirmatory stage is described in section 4.

Figure 1: Main stages of the study

The aim of the first, exploratory stage was to identify study constructs and establish the research model. This aim was fulfilled by establishing a clear purpose of the exploratory study, collect qualitative data, and then combine these results with conceptualizing the constructs, and our understanding of the establishment of potential casual links between exogenous and endogenous study variables. Throughout the exploratory stage, each step was supported by searching literature, and using the findings to aid logical reasoning, in particular when identifying behavioral information security governance variables that influence the establishment of security knowledge sharing, and build the foundation for developing hypotheses.

The first step was to obtain a richer understanding of knowledge sharing in the information security context. This was achieved by conducting six semi-structured interviews with a sample of content experts. Those interviews yielded the first pool of constructs, which then led us to conceptualize the constructs in order to avoid problems with construct validity (due to measurement issues) and statistical conclusion validity (due to biasing effect of measurement model misspecification) of the model (MacKenzie et al., 2011). An appropriate conceptualization of the construct is important for several reasons (Jarvis et al., 2003): first, a poor construct definition leads to confusion about what the construct does and does not refer to; and second, indicators may not represent the focal construct, or overlap with other constructs due to not being adequately defined. The section that follows presents a description of how the data in the exploratory stage was collected.

3.1 Exploratory data collection

The six respondents included in the interviews were all experienced individuals working with information security on a regular basis for 5 to 20 years. Of the six respondents, 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, and they were chosen based on recommendations from peers. Four of the respondents were geographically located in Sweden, one in Finland (but working extensively in Sweden) and the last one in the USA. As the purpose of the exploratory stage was to gain a deeper insight into what factors that lead to the establishment of security knowledge sharing – in order to develop hypothesis for more definite investigation – the number of respondents was deemed to be sufficient for this phase of the research. Furthermore, the sixth and last interview did not produce any new radical insights into the respondents' view of the phenomena. The latter argument is given support by the literature recommending that interview data should be collected until theoretical saturation take place and a too high number of respondents will make thorough interpretations of the interviews difficult (Kvale, 1986).

Three of the interviews were carried out face-to-face at the respondent's respective places of business, and three were carried out over telephone due to geographical concerns. The interviews lasted between 60-150 minutes and were audio-recorded and transcribed. Handwritten notes were also taken by the interviewer and transcribed electronically. The interviews all had the same general approach, and consisted of two main objectives: to gain a deeper understanding of important concepts for establishing security knowledge sharing in organizations; and to discuss potential relationships between constructs towards developing the research model.

The conceptualization of constructs, had in this study, three main objectives: 1) provide a clear, concise and unambiguous conceptual definition of the constructs; 2) specify the conceptual theme of the constructs (e.g., assessing if the construct is unidimensional or multidimensional); 3) evaluate the comprehensiveness of the constructs' dimensions (i.e., the relevance each dimension has to its focal construct and if any dimensions are missing to capture its construct). In line with those objectives, the two following steps were carried out: first, effort was spent on defining the constructs as clear and unambiguous as possible; second, a survey – capturing data on our proposed conceptual definitions, our assessment of the construct conceptual theme, and the comprehensiveness of the constructs' dimensions – was designed and distributed to 120 content experts. The respondents were identified from scientific articles from searches in professional societies' databases such as the IEEE and in pure indexing databases such as SCOPUS. When selecting people to serve as raters, it is important to make sure that they have sufficient intellectual ability to understand and complete the survey (Hinkin and Tracey, 1999). We therefore argue that the raters both need knowledge in the field of information security and have sufficient intellectual ability. Consequently we approached content domain experts to act as raters. Using content experts, rather than members from enterprises has shown to provide reliable results and is commonly used in health research where the quality of measurement instrument is of significant importance (Lynn, 2006). Further, MacKenzie et al. (2011) recommends using content experts in the early phase of the instrument development phase.

In all, 18 respondents completed the survey. The number of respondents is satisfying as, when assessing comprehensiveness of included variables, it is recommended to include a minimum of three experts, while using more than ten is probably unnecessary (Lynn, 2006). To capture data on our conceptual definitions and assessment of the construct conceptual theme, open-ended questions were included. To assess the dimensions' relevance, the respondents were questioned to give their opinion on the degree of association the experts believe each dimension has to its focal construct. For each dimension the respondents were asked to assess the degree of association to its focal construct using a five-point Likert scale ranging from 1 to 5, where 1 = not associated, 2 = somewhat associated, 3 = quite associated, 4 = highly associated, and 5 = very highly associated. Open-ended questions were included to assess both if any important dimension missing to capture the construct domain, and the understandability of the dimensions, i.e., if the dimensions are named properly or should be renamed. For the interested reader, the complete results and changes to the instrument can be found in Rocha Flores and Korman (2012).

The following subsection presents the main findings from the two rounds of data collection that laid the foundation for the development of hypotheses in order to identify major behavioral information security governance factors influencing security knowledge sharing.

3.2 Results of the exploratory study

First, and in line with the first objective of the study, an organization's establishment of security knowledge sharing is used as the endogenous study variable in the study. Three exogenous study variables – that might have an impact on the establishment of security knowledge sharing – emerged from the exploratory study. Those were (key dimensions presented in the brackets): organizational structures (formal security unit/formal structure, steering committee/coordinating structure), information security processes (risk management, performance monitoring), and business-based information security management (business-aligned information security management, business knowledge of information security managers, business-driven information security activities). Constructs (i.e., the study’s independent variables) and example of respondent statements supporting their inclusion are provided in Table 1.

Construct	Examples of respondent statements
Organizational structure (OS)	“Structures are needed to facilitate the deployment of security efforts, and communication between executives, security personnel, and business representatives.” “Mangers from different units need to understand the importance of information security and how it can be used to support the business and not hinder it…..this can be achieved by regular formal and informal meetings”
Business-based information security management (BBISM)	“It is crucial to establish understanding and alignment between business and IT managers”. “Security mangers need to understand the business and the end-user for developing security policies and programs that focuses on the end-users perspective.”
Coordinating information security processes (CISP)	“Formal processes to assess risks, develop policies, plan the implementation of controls to share knowledge on information security, and monitor the effectiveness of implemented controls are crucial.” “The operational personnel need to know what is expected of them. Processes to facilitate communication of executive directives need to in place in order for operational personnel to know why security measures are important, how to implement them, and control how effective they are.

Table 1: Derived constructs from the interviews.

The conceptualization process included all study constructs (the study’s dependent variable was included in the conceptualization process), and resulted in the decision that two of the constructs were multidimensional – namely, security knowledge sharing and organizational structure. Security knowledge sharing and organizational structure were operationalized 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 organizational structure (FOS) and coordinating organizational structure (COS) represented organizational structure. These constructions are referred to as a type II second-order construct models (Jarvis et al., 2003). The two other constructs were assessed to be unidimensional, and operationalized as first-order constructs. The final constructs that were used to establish the study’s research model are presented in Table 2 together with their conceptual definition.

Construct	**Conceptual definition**
Coordinating information security processes (CISP)	The level at which the management of information security is coordinated through formal procedures.
Business-based information security management (BBISM)	The degree to which information security managers base their information security efforts on organizational business goals and needs.
Organizational structure (OS)	The degree to which organizational structures is implemented in the organization to support governance of information security.
Formal organizational structure (FOS)	The degree to which formalized structures are implemented in order to support the handling information security matters within the organization (e.g., coordinating incident responses, providing support to employees or providing advice upon an information security concern).
Coordinating organizational structure (COS)	The degree to which people responsible for information security and representatives from various business units have regular formal and informal meetings.
Security knowledge sharing (SKS)	The level at which an organization has established processes to capture and share knowledge about information security among organizational members through formal and informal information flows.
Formal knowledge sharing arrangements (FKSA)	The level at which formal arrangements aimed at training employees on information security, which could include issues such as training on general security threats and compliance with actual information security policies, are implemented in the organization.
Support for knowledge transfer (SFKT)	The utilization of formal and informal resources (e.g., informal/voluntary advisory services, IT solutions and/or devices) in order to aid spreading, sharing and maintenance of information security awareness and knowledge in the organization.

Table 2: Conceptual definition of constructs

3.3 Hypotheses development

Based on the exploratory study and our understanding of causal links between endogenous and exogenous variables, the hypotheses were formed, and a research model aiming at investigating the influence of behavioral information security governance factors on security knowledge sharing established. In the following, hypotheses are formally stated and arguments identified from literature supporting their relevance are presented.

3.3.1 The role of coordinating information security processes

Processes to coordinate information security activities were suggested to influence security knowledge sharing. As the examples of interview respondent statements in Table 1 show, the respondents perceived that information security efforts should be coordinated through assessing risks, develop and implement relevant controls, and monitor the effectiveness of those implemented controls. The literature agrees on the importance of coordinating processes. For instance, Kayworth and Whitten (2010) argues that processes that coordinate information security efforts support the integration of information security in key organizational business processes or services, and thereby both enables security to be a core element in the business environment and strengthen the link between high-level business requirements and operational security procedures. Based on the interviews and the conceptualization process, two key dimensions of coordinating processes were established: risk management and performance monitoring. The existing theory agrees on the importance of risk management and performance monitoring. For instance, Calder and Watkins (2008) argue that, 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. Assessment of information security vulnerabilities provides an understanding of risks that need to be mitigated for the protection of an organization’s information resources, and help management make informed security-related decisions (Sun et al., 2006). Further, to support the coordination of information security, controls need to be checked for their effectiveness in practice, and both adapted to any changes in the business environment that might pose a risk to their information systems or negatively affect the daily business operations, and to the users' perceived acceptable level of obtrusiveness. In order to test the proposed causal links between coordinating information security processes and security knowledge sharing, the following hypothesis was formulated:

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

3.3.2 The role of business-based information security management

The exploratory findings suggest that the information security strategy need to be aligned with the business strategy to ensure that information security is based on actual business needs, while not hindering the business from conducting its strategic and operational activities. The interview respondents, for instance, perceived that information security managers need to understand the business and the end-users' need in order to develop information security policies and programs that focuses on the end-user perspective.

The value generated from alignment within an organization is explained by the general strategic alignment theory proposed by Henderson and Venkatraman (1993). The same theory explains that alignment in a company is achieved when organizational units act on the overarching business strategy. That is, they outline strategies, plans, and investments based on an understanding of business objectives, values, and needs. Previous research have shown that organizations with business competent information security executives conduct proper management of information assets and effective allocation of resources (Chang and Wang, 2010). In line with the findings from the exploratory study, we believe that a deep understanding of the business environments, processes and the organizational goals should enable the development of effective information security strategies, provide information security services that fit organizational needs, and enable a more effective coordination of information security activities. Therefore, this study explores the role of information security executives with an understanding of organizational business goals and needs on an organization's coordinating information security processes and establishment of security knowledge sharing. In line with this purpose the following two hypotheses are proposed:

H2a: Business-based information security management is positively associated with the organization's establishment of security knowledge sharing.

H2b: Business-based information security management is positively associated with the organization's coordinating information security processes.

3.3.3 The role of organizational structure

The exploratory findings suggest that organizational structure should be taken into consideration when understanding security knowledge sharing. The interview respondents left comments highlighting the need for structures to facilitate the deployment of information security efforts, and communication between executives, security personnel, and business representatives.

The importance of structures has been debated for a long period of time. For instance, Child (1984) argued that structure has a central role to the design of an effective organization. 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, monitoring of performance, and operating mechanisms that transfer directives on what is expected of organizational members and how the directives should be followed (Child, 1984). In an information security context, structures ensure that the security function maintains alignment with business strategy, enable effective organization of information security and contribute to the successful implementation and coordination of information security plans (Kayworth and Whitten, 2010). In this study, organizational structure is manifested through the two following forms of structures: formalized structure (also referred to as a centralized information security function) to both support the development and deployment of uniform firm-wide policies and support the handling information security matters throughout the organization; and coordinating structure such as the utilization of a diversity of coordinating information security committees and teams that meet to discuss important information security issues both formally and informally. To understand, more thoroughly, the positive impact of organizational structure in the context of information security, the following hypotheses are postulated:

H3a: Organizational structure is positively associated with the establishment of the organization’s security knowledge sharing.

H3b: Organizational structure is positively associated with the organization’s coordinating information security processes.

H3c: Organizational structure is positively associated with the organization’s business-based information security management.

3.3.4 The role of national culture as a moderating variable

Based on the aforementioned discussion presented in section 2.2, we wanted to test if there were differences in the model paths based on national culture. The cultural dimensions that are investigated are individualism, and masculinity – the two dimensions in where the cumulative differences between the values of USA and Sweden are the largest. As we wanted to test the moderating effect of national culture on all paths in the model, we proposed five hypotheses suggesting this effect. Accepting those hypotheses means that there are grounds for believing that national culture significantly moderates the relationships in the proposed research model. The hypotheses tested in the present study are outlined as follows:

H4a: The effect of coordinating information security processes on security knowledge sharing will differ between US and Swedish organizations.

H4b: The effect of organizational structure on security knowledge sharing will differ between US and Swedish organizations.

H4c: The effect of business-based information security management on security knowledge sharing will differ between US and Swedish organizations.

H4d: The effect of organizational structure on coordinating information security processes will differ between US and Swedish organizations.

H4e: The effect of organizational structure on business-based information security management will differ between US and Swedish organizations.

H4f: The effect of business-based information security management on coordinating information security processes will differ between US and Swedish organizations.

To conclude the section in which the description of how the research model was developed, the complete model, with the hypotheses included, is presented in Figure 2.

Figure 2: Proposed research model

4. Confirmatory study

Once the research model was formed the next phase included data collection with the purpose to validate the hypotheses. However, in order to assure that the measurement instrument includes items that actually capture the theoretical meanings of each construct (i.e., establish construct validity) in the research model, effort was placed on the instrument validation process, as recommended by (MacKenzie et al., 2011). The following section describes the establishment of a measurement instrument with valid constructs.

4.1 Item development

The first step in the confirmatory study was to generate a set of measurement items that represents the conceptual domain of the construct. Measurement items can be identified through: conducting reviews of the literature; deduction from the theoretical definition of the construct; previous theoretical and empirical research on the focal construct; suggestions from experts in the field; and an examination of other items of the construct that already exist (Nunnally and Bernstein, 1994). Effort was first spent on deciding how the items were related their focal construct, i.e. if they were to be specified as reflective or formative items. The distinction between those two types of items is critically important as Monte Carlo simulations reported by Jarvis et al. (2003), and Petter et al. (2007) suggest that structural parameter estimates can be biased when indicators that should be modelled as having formative relationships with a construct are modelled as having reflective relationships. Thus, in the process of selecting items and develop scales, it’s crucial that the researcher consider the nature of the relationship between the indicators and the construct they are intended to represent.

In conclusion, 34 items were generated. Coordinating information security processes was specified with formative items, and the other five first-order constructs (FS, CS, BBISM, FKSA, and SFKT) 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 management, were identified from previous work (Chang and Wang, 2010; Spears and Barki, 2010). Thus, a major part of the items were developed specifically for this study.

4.2 Content validity assessment

When developing new items, MacKenzie et al. (2011) recommends to assess the content validity of the items before colleting primary data. Content validity “the degree to which items in an instrument reflect the content universe to which the instrument will be generalized (Straub et al. 2004, p. 424)”, is an assessment that consists of two stages: development and judgment-quantification (Lynn, 2006). The development stage consists of identification of study constructs, item generation, and instrument. Judgment-quantification, entails asking a number of experts to evaluate the validity of the items and as a set (DeVellis, 1991). In the present study, we quantitatively assessed the content validity using the item-sorting method proposed by Anderson and Gerbing (1991). This was done for all constructs except business-based information security management as these items were already proven reliable by previous empirical research (Chang and Wang, 2010; Spears and Barki, 2010). Besides providing a statistical result to assess the adequacy of content validity of each item, the method does not make any implicit assumptions about the direction of the relationship between the items and their corresponding factors or about the correlations between the items themselves. Therefore, it can be used to assess the content validity of either formative or reflective indicators. This is a fundamental advantage when developing formative items to capture a construct as a lack of content validity is a particularly serious problem for constructs with formative indicators (Petter et al., 2007). The investigated items were tested for their content validity by collecting data using an email survey distributed to 452 content domain experts, of which 56 completed the survey.

We also asked for comments on wording, if the survey items were clearly understood and if they perceived that any items were missing to represent the constructs. Based on this pre-test the measurement instrument was revised, and the initial item pool of containing 34 developed items was reduced to 18 items with an adequate degree of content validity (for more information on specific changes, the interested reader is referred to Rocha Flores and Antonsen (2013)). 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 (Podsakoff et al., 2003). By adding four, already tested and reliable, items representing business-based information security, the final survey included 20 items (cf. Appendix A), all measured on a 11-point licker scale from 0 to 10 inspired by Paternoster and Simpson (1996) and Siponen and Vance (2010).

4.3 Primary data collection

The SANS security mailing list/GPWN-list (SANS, 2013), was initially adopted as a sampling frame. The mailing list comprises information security executives, senior managers, 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 and Grover, 1999). In this study, the key informants included such high-level executives as CISOs, Security Officers, CEOs, CIOs, and IT managers. From this sampling frame, 548 potential respondents were identified. Information security executives from 30 organizations known to the research department were also approached and asked to complete the survey. In total, the sample therefore included 578 potential respondents. Data was collected between November of 2012 and June 2013. 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 578 e-mail requests that where sent, 38 bounced. After two reminders 105 had opened the survey and 82 respondents had completed the survey, which gives an effective response rate of 15.2 %. At first glance, the response rate may seem rather low. However, Rogelberg and 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 due to the two following reasons: 1) the data is collected in the critical domain of information security in which executives often are not willing to leave out data; and 2) managers have been oversurveyed due to the increased popularity of using online surveys to capture organizational managers' attitudes and beliefs related to different types of organizational issues (Rogelberg and Stanton, 2007).

The respondents in the sample represent organizations from a diverse set of industries. Twenty-six percent of the responding organizations are in IT industries; Twenty-three percent are in manufacturing and retail; 12 percent are in the government and academic sector; 10 percent are in financial services and insurance industries; 9 percent are in telecommunication services; 7 percent are in Energy; 4 percent are in Health care; 4 percent are in wastewater treatment services; and 6 percent were categorized as "other". A significant part of the organizations were located in the United States (36.6 percent), Sweden (36.6 percent), Finland (6.1 percent) and United Kingdom (3.6 percent). However, answers were also received from Spain, Greece, Canada, Norway, Denmark, Ireland, and Japan. 41 percent of the organizations had more than 5000 employees; 21 percent had between 100-499 employees; 17 percent had less than 100 employees; 13 percent had between 1000-5000 employees; and 8 percent had 500-999 employees. A significant number (78 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 defense section, information security manager, Cyber security manager, Head of sub-division and Business manager of Critical Infrastructure & industrial security. Further, 90 percent had work with information security within an organization for 10 or more years.

4.4 Data analysis techniques

Partial least squares structural equation modelling (PLS-SEM) was used to test the measurement model's psychometric properties and structural model. The variance-based technique, PLS-SEM, was used instead of covariance-based techniques due to three reasons. First, PLS-SEM does not require large samples. The study by Reinartz et al. (2009) showed that variance-based techniques offer better estimation than other techniques in samples under 250 (the sample size of the current study is 82). Second, the study's model includes a formative construct (CISP) in the model, and PLS-SEM is better suited for better handling potential indeterminacy problems than other techniques such as LISREL (Joreskog and van Thillo, 1972). Third, PLS-SEM is a non-parametric technique; hence there is no need to guarantee the normality of the data (Hair et al., 2011).

Before assessing the quality of the measurement model, the data set was first screened, using SPSS (version 19)(IBM Corporation 2010), 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.

SmartPLS the software package (version 2.0.M3)(Ringle et al., 2005), was then used for the estimations. To interpret and analyse the structural model, a two-step approach to structural modelling was used (Barclay et al., 1995): first, the quality of the measurement model was assessed to ensure the validity and reliability of the items; second, the structural model was analyzed in order to test the hypotheses and quality of the structural model.

4.5 Quality of measurement model

Construct validity for the formative construct, coordinating information security processes (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 (VIF) less than 5 indicates acceptable shared variance (Hair et al., 2011). One of the formative items (CISP2) indicated to cause correlation (VIF > 5), and was therefore removed for further analysis. As Table 3 shows, the remaining formative items had acceptable weights (t-values > 1.65) and acceptable VIFs.

Indicator	VIF	Outer weights	t-values
CISP1	1.910	0.489***	3.417
CISP3	2.308	0.210*	1.800
CISP4	1.874	0.451***	3.519

Table 3: Formative construct validity for coordinating information security processes

Notes: n.s indicates statistically nonsignificant; * indicates statistical significance at p < 0.1; ** at p < 0.05; and *** indicates statistical significance at p < 0.01

The reflective measures were assessed through internal consistency reliability, indicator reliability, and convergent validity and discriminant validity. Cronbachs alpha (CA) and Composite reliability (CR) should be higher than 0.7 for adequate internal consistency reliability (Hair et al., 2011). As the second and third column in Table 4 shows, all values are above the threshold (>0.7). This suggests adequate internal consistency reliability. Indicator loadings should be higher than 0.7 for acceptable indicator reliability (Hair et al., 2011). As Table 5 shows, all indicators load to their respective construct with a value above the threshold value (>0.7). This suggests that problems with indicator reliability were not an issue in this study. If the average variance extracted (AVE) yields a value above 0.5, convergent validity is established. Looking at Table 4, we can see that all values are above the threshold; we can therefore conclude that convergent validity was ensured. Discriminant validity is established if the two following requirements are fulfilled: 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 cross loadings (Hair et al., 2011). As table 4 shows, the square root value of each constructs' AVE (diagonal values in bold) are higher than all values on the rows below. Table 5 shows that indicator loadings (values in bold) are higher than all of its cross loadings (values to the right of indicator loadings). Those two premises lead to the conclusion that the criterion for discriminant validity is satisfied. In conclusions, all validation tests suggest that the items are both valid and reliable and could thus be used to evaluate the structural model.

	CA	CR	AVE	BBIS	CISP	COS	FKSA	FOS	SFKT
BBIS	0.928	0.949	0.823	**0.907**					
CISP	n/a	n/a	n/a	0.741	n/a				
COS	0.868	0.910	0.718	0.624	0.759	**0.847**			
FKSA	0.855	0.912	0.777	0.685	0.790	0.666	**0.881**		
FOS	1.000	1.000	1.000	0.508	0.684	0.662	0.583	**1.000**	
SFKT	0.924	0.943	0.767	0.616	0.737	0.725	0.693	0.611	**0.876**

Table 4: Correlations, Cronbachs alpha (CA), Composite reliability (CR) and Average variance extracted (AVE)

	BBIS	COS	FKSA	FOS	SFKT
BBIS1	**0.863**	0.583	0.691	0.442	0.535
BBIS2	**0.950**	0.550	0.614	0.463	0.544
BBIS3	**0.942**	0.577	0.571	0.492	0.534
BBIS4	**0.872**	0.551	0.601	0.446	0.615
COS1	0.456	**0.849**	0.555	0.525	0.526
COS2	0.527	**0.898**	0.554	0.606	0.617
COS3	0.551	**0.779**	0.499	0.448	0.672
COS4	0.583	**0.859**	0.644	0.652	0.650
FKSA1	0.644	0.629	**0.830**	0.497	0.598
FKSA2	0.454	0.538	**0.885**	0.510	0.576
FKSA3	0.704	0.595	**0.926**	0.533	0.655
FOS1	0.508	0.662	0.583	**1.000**	0.611
SFKT1	0.638	0.653	0.664	0.468	**0.836**
SFKT2	0.364	0.569	0.505	0.599	**0.846**
SFKT3	0.422	0.619	0.530	0.519	**0.875**
SFKT4	0.631	0.649	0.677	0.596	**0.913**
SFKT5	0.619	0.680	0.644	0.497	**0.906**

Table 5: Indicator loadings and cross loadings for reflective indicators

4.6 Evaluation of structural model

In order to assess the significance of the structural path coefficients, bootstrapping re-sampling with 82 cases and 1000 re-samples was used. The R² values of the endogenous constructs measures how much variance is explained by the exogenous constructs. R² values of 0.67, 0.33, or 0.19 can be described as substantial, moderate, or weak, respectively (Chin, 1988). As Figure 3 shows, all hypotheses, except H2b could be accepted. The R² value for the dependent variable, security knowledge sharing (SKS) is 0.73, which indicates that the constructs in the model explains 73 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 SKS. Organizational structure (OS) explains 41 percent of the variance in business-based information security management (BBISM); organizational structure together with BBISM explains 72 percent of variance in CISP. As SKS and OS were operationalized as formative second-order constructs, the significance of the first-order weights was examined. The weights indicated that each dimension significantly contribute to their underlying construct. Among the behavioral information security governance factors, CISP has the strongest direct effect on security knowledge sharing, with a regression coefficient of β = 0.42. The impact of OS on CISP and BBISM is significant, with β = 0.54 and β = 0.64, respectively. The association between BBISM and CISP is also significant, with β = 0.40. Finally, OS have a significant direct effect on SKS, with β = 0.35.

An interesting question could be raised here: are there any indirect effects present in the model? And can those effects explain the lack of significant relationship between BBISM and SKS? Though the existence of indirect effects was not hypothesized, and no information of arguments or empirical tests regarding these potential mediating effects was found in the literature, it was decided to analyze that data using meditation test. The analysis is presented in the following subsection.

4.7 Mediation analysis

The test for mediation effect we followed the method suggested by Baron and Kenny (1986). The results from the mediation analysis are presented in Table 6. Three tests for mediation were conducted independently: CISP mediates the relationship between OS and SKS; CISP mediates the relationship between BBISM and SKS; and BBISM mediates the relationship between OS and SKS. Column 1 shows the regression coefficients of each path independently of the mediating variable (MV); that is, the mediating variable has not yet been introduced in the mediation model. An initial requirement for investigating mediation effect is that all regression coefficients in column 1 should be significant (Baron and Kenny, 1986). As column 1 for the three tests shows, the regressions coefficients for all paths are significant and thus fulfil the initial requirement. Then, when introducing the mediating variable to the model (shown in column 2), path c should reduce, indicating an effect of the mediating variable on the dependent variable (DV). If path c both reduces and become insignificant, the mediator fully mediates the effect of the independent variable (IV); and if path c reduces, but is still significant, the mediator partially mediates the effect between the IV and DV. The mediation tests revealed that CISP partly mediates the effect of OS, and fully mediates the effect of BBISM, on SKS. Thus, business-based information security management in an organization affects security knowledge sharing completely trough a processes that coordinates information security activities. Finally, the analysis revealed that BBISM partly mediates the effect of OS on SKS.

Figure 3: Results of Structural Model Testing (full sample, n=82)

Notes: n.s indicates statistically nonsignificant; * indicates statistical significance at p < 0.1; ** at p < 0.05; and *** indicates statistical significance at p < 0.01

IV:OS **MV:CISP**			**IV:BBIS** **MV:CISP**			**IV:OS** **MV:BBISM**		
	1	2		1	2		1	2
Path a (OS→CISP)	0.791***	0.791***	Path a (BBISM→CISP)	0.741***	0.741***	Path a (OS→BBISM)	0.638***	0.638***
Path b (CISP→SKS)	0.815***	0.520***	Path b (CISP→SKS)	0.815***	0.673***	Path b (BBISM→SKS)	0.691***	0.321***
Path c (OS→SKS)	0.784***	0.373***	Path c (BBISM→SKS)	0.691***	0.192 n.s	Path c (OS→SKS)	0.784***	0.580***
Partial mediation			Full mediation			Partial mediation		

Table 6: Mediation analysis results (full sample, n=82). The first column displays correlation before including the mediator variable, and the second column shows correlation with the mediator variable included.

Notes: n.s indicates statistically nonsignificant; * indicates statistical significance at p < 0.1; ** at p < 0.05; and *** indicates statistical significance at p < 0.01

4.8 Analysis of national cultural differences

The second objective of the study was to identify if there exist any differences in the model’s path based on national culture. A multigroup analysis was conducted to attain this objective. The full dataset comprised 82 organizations from different geographical regions of the world. However, this study focused on investigating difference between US and Swedish organizations. The full sample included 30 US and 30 Swedish firms; therefore, these firms were represented as two separate groups containing 30 cases each. The next step was to run the PLS algorithm for each model separately. The results for the two groups are presented in Table 7 and 8.

To examine whether the differences in the results between the two models were significant, the approach to multigroup analysis proposed by Chin and Dibbern (2010) was followed. This approach was also used by Eberl (2010) and Navarro et al. (2011) to assess group differences. A multigroup analysis can be divided in two steps. First, a sample of each subpopulation is analyzed, resulting in groupwise parameter estimates. Then, the significance of the differences between groups is evaluated. Both Chin and Dibbern (2010) and Keil et al. (2000) propose to use a t-test based on the pooled standard errors obtained via a resampling procedure. That is, bootstrapping from each sample is made to test whether there is a significant difference between two group-specific parameters. Using this method to asses significance in group differences can cause problems if similar sample size is not tenable (Chin and Dibbern, 2010). However, as the size of the two samples in the currents study is equal, we conclude that there is no reason for us to believe that measurement problems are an issue in the analysis. As can be seen when observing Table 7, significant differences exist for 4 of the 6 paths. The largest significant difference is between the relations: CISP→SKS and OS→SKS. There is also a significant difference between the relations: OS→CISP; and BBISM→CISP. No significant differences were, however, found in relations between BBISM→SKS and OS→BBISM.

Path	Path coefficient		Δ Path (Sweden-USA)
	Sweden (n=30)	USA (n=30)	
CISP→SKS	0.750***	0. 298 n.s	**0.452****
OS→SKS	0.122 n.s	0.534***	**-0.411****
BBISM→SKS	-0.067 n.s	0.129 n.s	-0.196 n.s
OS→CISP	0.291**	0.569***	**0.291****
OS→BBISM	0.675***	0.725***	0.050 n.s
BBISM→CISP	0.619***	0.404***	**0.215***

Table 7: Path coefficients and significance of pat differences for Swedish and US sample

Notes: n.s indicates statistically nonsignificant; * indicates statistical significance at p < 0.1; ** at p < 0.05; and *** indicates statistical significance at p < 0.01

Additionally, Table 8 shows the coefficients of determination R^2 for the Swedish (n=30) and US sample (n=30).

Construct	Group	R^2
SKS	Sweden	0.612
	USA	0.850
CISP	Sweden	0.705
	USA	0.850
BBISM	Sweden	0.456
	USA	0.526

Table 8: Results of coefficients of determinations

The data was collected via self-reported survey, thus the potential for both nonresponse bias and common method bias (CMB) should be addressed (Podsakoff, 1986; Doty and Glick, 1998). To address potential nonresponse bias the last respondent method was used as recommended by Armstrong and Overton (1977) and previously used by researchers (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). Inspired by the technique used in Bulgurcu et al. (2010) 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. If no significant differences between the first and the last third of the respondents' data on any of the measures analyzed are identified, nonresponse bias is not an issue in this study. This test procedure revealed no significant differences between the first and the last third of the respondents' data on any of the items analyzed. This suggests that nonresponse bias was not an issue in this study.

The threat of common methods bias (CMB) was addressed as follows. Ex ante, CMB was addressed by counterbalancing the order of questions in the questionnaire to discourage participants from figuring out the relationship between the dependent and independent variables that was attempted to be established. 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 (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 4). 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.

To conclude this section, a summarization of the results of the hypotheses tests is presented in Table 8. An important note is that coefficients values, t-statistic values, and p-values for hypothesis 4a to 4f are not presented, because these hypotheses were investigated when conducting the analysis of national cultural differences (cf. Table 7).

Hypothesis	**Supported/ rejected**	**Path coefficient**	**t-value**	**p-value**
H1: Coordinating information security processes is positively associated with the organization’s establishment of security knowledge sharing.	Supported	0.424	3.399	***
H2a: Business-based information security management is positively associated with the organization’s establishment of security knowledge sharing.	Rejected	0.151	1.550	n.s
H2b: Business-based information security is positively associated with the organization’s coordinating information security processes.	Supported	0.399	4.861	***
H3a: Organizational structure is positively associated with the establishment of the organization’s security knowledge sharing.	Supported	0.352	3.315	***
H3b: Organizational structure is positively associated with the organization’s coordinating information security processes.	Supported	0.536	7.404	***
H3c: Organizational structure is positively associated with the organization’s business-based information security.	Supported	0.638	8.103	***
H4a: The effect of coordinating information security processes on security knowledge sharing will differ between US and Swedish organizations.	Supported			
H4b: The effect of organizational structure on security knowledge sharing will differ between US and Swedish organizations.	Supported			
H4c: The effect of business-based information security management on security knowledge sharing will differ between US and Swedish organizations.	Rejected			
H4d: The effect of organizational structure on coordinating information security processes will differ between US and Swedish organizations.	Supported			
H4e: The effect of organizational structure on business-based information security management will differ between US and Swedish organizations.	Rejected			
H4f: The effect of business-based information security management on coordinating information security processes will differ between US and Swedish organizations.	Supported			

Table 9: Results of the testing of hypotheses in the study

Notes: n.s indicates statistically nonsignificant; * indicates statistical significance at p < 0.1; ** at p < 0.05; and *** indicates statistical significance at p < 0.01

5. Discussions and conclusions

The first main objective was to examine and identify which behavioral information security governance factors have a significant effect on security knowledge sharing in organizations. The second main objective was to test the validity of the results across different cultural settings. Specifically, we examined if the effect of behavioral information security governance factors on the establishment of security knowledge sharing differs between Swedish and US organizations. The discussion is organized around these two main objectives.

5.1 Significant behavioral information security factors

The first objective was attained through developing and empirically testing a research model, which includes three broad classes concerning an organization’s structure of information security function, its processes to coordinate implemented controls, and its alignment to, and understanding of, actual business needs and goals. A mixed methods research design was employed to attain this objective. The research design included a first, exploratory stage that both resulted in the establishment of the study’s research model and informed the second, quantitative stage, where a measurement instrument was developed. The instrument was then used to collect and analyze data from 82 information security executives from a diverse set of organizations located in different geographic regions in the world.

The empirical tests of the model, using the full sample (n=82), revealed that coordinating information security processes and organizational structure had a significant direct effect on the establishment of security knowledge sharing, while no significant effect was identified in the hypothesized direct association between business-based information security management and security knowledge sharing. Thus, hypotheses H1, H3a were fully supported, while H2a was not. Of the supported hypotheses, coordinating information security processes had the strongest significant direct effect. A mediation analysis revealed that the reason for the nonsignificant direct relation (H2a) is the fully mediating role of coordinating information security processes. The mediation tests confirmed that coordinating information security processes has an important role by partially mediating the effects of organizational structure, and fully mediating the effects of business-based information security management, on security knowledge sharing. Consistent with the proposed research model, we found that both business-based information security management and organizational structure had significant direct effects on coordinating information security processes. Hence, hypotheses H2b, and H3b were fully supported. The findings also indicated that organizational structure significantly influences the organization's business-based information security management, which supports hypothesis H3c.

The model's constructs explain 73 percent of variance ($R^2 = 0.73$) in security knowledge sharing, indicating that the model has a strong explanatory power. The model's explanatory power in regards to business-based information security management is moderate ($R^2 = 0.41$). This result is not remarkable as it's predicted, in the model, by only one construct. Therefore, more constructs should be included for a better prediction model if business-based information security management is used as the dependent variable. Coordinating information security processes is predicted by the direct effects of organizational structure and business-based information security management whereof organizational structure also has a significant indirect effect through the mediating role of business-based information security management. The explanatory power is strong ($R^2 = 0.72$), and as organizational structure have both a significant direct and indirect effect, the results suggest that organizational structure has an important role in establishing coordinating processes.

Our results show that a process to coordinate implemented controls based on the level of an organization's risk appetite, and assess the obtrusiveness and performance limitations of implemented controls to business activities, is critical for establishing security knowledge sharing. Furthermore, formal information security structure (or centralized information security function) to develop and deploy uniform firm-wide policies, and steering committees to facilitate information security planning, lead to effective establishment of security knowledge sharing. Previous research have highlighted the importance of processes to govern information security, but have put the variable on the same level as its related information security mechanisms (e.g., organizational structures)(Kayworth and Whitten 2010). However, our study disentangles the interrelated influences of behavioral information security governance factors on security knowledge sharing by showing that: (1) organizational structures have both a significant direct and indirect effect on security knowledge sharing, implying that structure both ensures that the security function maintains alignment with business strategy and sets the platform for organizations to establish security knowledge sharing; and (2) process related to coordinating information security activities is a significant mediator and thus realizing the effects of both the structure of the information security function and the alignment of information security management with actual business needs. One explanation for the direct and indirect effect of organizational structures could be that having a centralized information security function with dedicated IT personnel responsible for activities such as the implementation of formal training programs, lead to knowledge sharing arrangement actually being established. While when the governance environment is decentralized, the establishment of knowledge sharing is carried out by the users themselves. This results supports the findings from the study by Warkentin and Johnston (2007), in which a comparative case study including both a centralized and decentralized governance environment was conducted. The results are consistent with research within general management in two ways. First, the results highlight the importance of organizational structures to deploy processes, mechanisms for their coordination and monitoring, and to enable strategic- and operational decision-making (Child, 1984). Second, the important role of processes as constructs explaining the relationships between input variables and desired outcomes have been highlighted in the field of team structures and effectiveness (Stewart and Barrick, 2000; Klarner et al., 2013).

We have presented limitations in the extant research in the behavioral governance perspective of information security. Further, our review of the literature in security knowledge sharing research shows a significant gap of empirical studies aiming at understanding how firms establish mechanism to increase or maintain security knowledge among their employees. This study, therefore, complements the existing research by offering theoretical explanation and empirical evidence on what drives organizations' to establish security knowledge sharing. To our best knowledge this is the first study that investigates, more thoroughly, the reasons to why such an establishment occurs in organizations. Furthermore, the measurement instrument developed to capture the under-investigated determinants of security knowledge sharing can be used by other researchers to test other theoretical model or further validate the findings from this study.

In summary, an organization's processes to coordinate implemented controls, and structure of information security function both have significant direct effect on security knowledge, where coordinating processes have a slightly stronger effect. Business-based information security management has not a direct effect – but has an indirect effect, through the mediating effect of coordinating processes – on security knowledge sharing. This answers the first research question posed by the study (RQ1).

5.2 The effect of national culture

The second objective of the current study was to examine if national culture moderates the relationships in our research model. Two different countries with contrasting cultures were studied: Sweden and the USA. The results show that 4 of 6 paths were significantly different. Thus, the results of the study points at significant differences in how US and Swedish organizations run their information security function.

For Swedish organizations the correlation between formal and coordinating structures and security knowledge sharing is non-significant, while there is a strong significant correlation between coordination process and security knowledge sharing. The results imply that in Sweden – which is seen as a less individualist, feminine country – managers tend to focus their efforts on implementing controls that are aligned with business activities and employees' need; monitoring the effectiveness of the controls, and assuring that the controls that are not to obtrusive in regards to the people they affect. This implies that managers perceive it to be important to involve, or at least know how their employees cope with the decisions that have been made, thus have positive attitudes towards local participation. On the contrary, for US organizations the results show that structure and control has stronger association to security knowledge sharing than coordinating processes. Thus, it seems that US security executives are more prone to implement formal arrangements in order to assure information security in their organization. This implies that US organizations may feel the need to develop policies centrally, make them visible and strongly enforcing them. The results are consistent with the cultural theories explaining that a manager from a more individualist and masculine culture perceives the need to control their employees and not involve them in decisions. Two examples showing the need for more or less control among executives from a more individualist culture is revealed in the 2013 Global State of Information Security Survey conducted by PWC Advisory Services & Security. The results from the survey showed that 54 % of North American firms conduct background checks of individuals before employing them and have implemented employee security awareness training programs, while 42 % of European firms have implemented the same information security measures (PWC Advisory Services and Security, 2013).

Furthermore, the results are consistent with the study by Jackson (2000), in where the findings showed that firms in less regulated countries (e.g. USA), may feel the need have formal policies and make them visible, to avoid employees “bending the rules”. This might not be evident in firms operating in more regulated countries such as Sweden, where the market is more is regulated by a government appointed body and where little emphasis is put on ethical legislation or assuring that employees follow the firms’ code of conduct and behavior.

In addition, Langlois and Schlegelmilch (1990) argue that codes of ethics are in the US more concerned with relations with federal and state governments and emphasize “company policy towards employees”, while codes in European countries are more concerned with employee relations and tends to promote employee responsibility and a “belongingness” to the organization. This further elevates the main difference between US and Swedish organizations: formal structures and arrangements and less interaction with employees vs. local participation and the need to involve employees in any decision taken.

In summary, national culture moderates 4 out of 6 proposed hypotheses focusing on individualist and masculine cultural dimensions. Thus, the effect of behavioral information security governance factors on the establishment of security knowledge sharing differ between Swedish and US organization differs. This answers the second research question posed by the study (RQ2).

5.3 Managerial implications

Firms worldwide invest a vast amount of money to ensure information security throughout their organization, and although those investments are highly prioritized, knowing how to organize their information security efforts is still challenging. The results from our empirical investigation can support managers in their decision-making process by offering insights into how behavioral information security governance factors interrelate with each other and that a process related to coordinating security activities precedes establishment of mechanisms to increase security knowledge among employees. While current practical recommendations often are based on the assumption that governance factors influence outcomes independently of each other (e.g., ISACA, 2006; Brotby, 2009), our results show that having formal information security structures and steering committees have both direct and indirect effect on the establishment of security knowledge sharing, however, coordinating information security process underlie that relationship, and is thus essential for establishing security knowledge sharing, which in turn has shown to mitigate risks for security violations (Hu et al., 2012; Bulgurcu et al., 2012). This process is also essential for realizing the effect of business-based information security on security knowledge sharing, as it fully mediates this relationship. Top managers should therefore recognize the importance of ongoing coordination activities such as assessing risk related to both their information systems and business process, and evaluate the performance and impact of implemented controls.

Many practical information security guidelines are too generic and do not take cultural factors into consideration. Our cultural analysis points to the importance of national culture when designing effective information security programs. Recognizing the impact of national culture could help firms design a more effective information security function that fits the cultural context of the country in which the firm operates. National culture needs to be taken into consideration – in particular for organizations operating in a global environment – and organizations need to understand how it affects behaviors and decision-making. Thus, there is not a general solution to establish security knowledge sharing that works world-wide. The findings from this study elevate the importance of including culture as a factor for effective governance of behavioral information security, and in particular when establishing security knowledge sharing.

5.4 Limitations and future work

There exist several limitations which should be taken into account when interpreting the results. First, a general limitation is that we assume that the studied behavioral information security governance variables and 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 organization, 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 behavioral information security governance factors that influence security knowledge sharing, and if differences exist based on culture, not characteristics of the firm. Furthermore, while we focused on national culture, difference might exist between firms within a country. Hofstede’s cultural measures – that are used in our study – generalize culture to an entire national population; that is, there is an assumption that culture effects apply to all individuals (or firms) in that nation. This assumption has been challenged and that culture should be studied at the individual level as well (Markus and Kitayama, 1991; Kolodziej-Smith et al., 2013). In our study, we did not test if characteristics of a firm (e.g. size, industry in which the firm operate in) yield differences in the developed theoretical model. Differences between firms within a country could be identified based on unobserved heterogeneity. It would therefore be interesting to collect more data using our approach to analyze any potential differences based on unobserved heterogeneity as proposed by Sarstedt and Ringle (2010). We acknowledge the potential impact of these factors and therefore recommend including them in future work.

This paper focused on factors to establish mechanisms to increase and maintain security knowledge among employees, thus authorized users (“insiders”). Consequently, one interesting continuation of the present work is to investigate if security knowledge sharing could support the management of both intentional and unintentional insider misbehavior. An example of intentional insider misbehavior is a deviant action such as sabotage or stealing, and an example of unintentional insider misbehavior is when an insider is manipulated by an attacker to click on a malicious link (Crossler et al., 2013). Future studies may examine how implemented security knowledge sharing mechanism influence insiders beliefs and attitudes toward information security, and in turn affect both intentional and unintentional insider misbehavior. Unintentional insider misbehavior can be measured through direct observations of behavior such as via phishing experiments (Rocha Flores et al., 2014), and intentional misbehavior can be measured through real time monitoring (Kandias et al., 2010; Kandias et al., 2013). Regarding management techniques related to insider behavior, Coles-Kemp and Theoharidou (2010) have proposed an approach considering the ISO 27000 standard for information security management. However, as previously mentioned the use of such best practice frameworks standards has been criticized for being too generic or universal in scope and thus not pay enough attention to the differences between organizations and their information security requirements (Siponen and Willison, 2009). The findings from our study provide theories related to security knowledge sharing that have been developed and empirically validated. Thus, there are opportunities for researchers to further explore the effect of security knowledge sharing on insider misbehavior, or its role in other subfields of behavioral information security.

References

Albrechtsen E. A qualitative study of users’ view on information security. Comput Secur. 2007 Jun;26(4):276–89.

Anderson JC, Gerbing DW. Predicting the performance of measures in a confirmatory factor analysis with a pretest assessment of their substantive validities. J Appl Psychol. 1991;76(5):732–40.

Applegate SD. Social Engineering: Hacking the Wetware! Inf Secur J A Glob Perspect. Taylor & Francis; 2009 Feb 6;18(1):40–6.

Armstrong JS, Overton TS. Estimating Nonresponse Bias in Mail Surveys. J Mark Res. 1977;14:396–402.

Bagozzi RP, Yi Y, Phillips LW. Assessing construct validity in organizational research . Adm Sci Q. 1991;36(3):421–58.

Bandyopadhyay K, Bandyopadhyay S. User acceptance of information technology across cultures. Int J Intercult Inf Manag. Inderscience Publishers; 2010;2(3):218.

Barclay D, Higgins C, Thompson R. The partial least squares (PLS) approach to causal modeling: personal computer adoption and use as an illustration. . Technol Stud. 1995;2(2):285–309.

Baron RM, Kenny DA. The Moderator-Mediator Variable Distinction in Social Psychological Research – Conceptual, Strategic, and Statistical Considerations . J Pers Soc Psychol. 1986;51(6):1173–82.

Belsis P, Kokolakis S, Kiountouzis E. Information systems security from a knowledge management perspective. Inf Manag Comput Secur. Emerald Group Publishing Limited; 2005 Jan 7;13(3):189–202.

Boyacigiller NA, Adler NJ. The Parochial Dinosaur: Organizational Science in a Global Context. Acad Manag Rev. Academy of Management; 1991 Apr 1;16(2):262–90.

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

Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q. 2010 Sep 1;34(3):523–48.

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

Chang K, Wang C. Information systems resources and information security. Inf Syst Front. 2010 Apr 27;13(4):579–93.

Chang S, Ho C. Organizational factors to the effectiveness of implementing information security management. Ind Manag Data Syst. 2006;106(3):345 – 361.

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

Chin W, Dibbern J. An Introduction to a Permutation Based Procedure for Multi-Group PLS Analysis: Results of Tests of Differences on Simulated Data and a Cross Cultural Analysis of the Sourcing of Information System Services Between Germany and the USA. In: Vinzi VE, Chin WW, Henseler J, Wang H, editors. Handb Partial Least Squares. Springer Berlin Heidelberg; 2010. p. 171–93.

Chin WW. The partial least squares approach to structural equation modeling. In: Marcoulides GA, editor. Mod Methods Bus Res . Mahwah, NJ: Lawrence Erlbaum Associates.; 1988. p. 295–358.

Coles-Kemp L, Theoharidou M. Insider Threat and Information Security Management. In: Probst CW., Hunker J., Bishop M., Gollmann D, editors. Insid Threat Cyber Secur Adv Inf Secur . Springer US; 2010. p. 45–71.

Cox J. Information systems user security: A structured model of the knowing–doing gap. Comput Human Behav. 2012 Sep;28(5):1849–58.

Creswell JW, Plano Clark VL. Designing and Conducting Mixed Methods Reserach. 2nd ed. Thousand Oaks, CA: SAGE; 2011.

Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville R. Future directions for behavioral information security research. Comput Secur. 2013 Feb;32(null):90–101.

Cummings JN. Work Groups, Structural Diversity, and Knowledge Sharing in a Global Organization. Manage Sci. INFORMS; 2004 Mar 1;50(3):352–64.

D'Arcy J, Herath T. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. Eur J Inf Syst. Nature Publishing Group; 2011 Jun 14;20(6):643–58.

D'Arcy J, Hovav A, Galletta D. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Inf Syst Res. 2008 Jun 20;20(1):79–98.

Davenport TH, Prusak L. Working Knowledge: How Organizations Manage What They Know. Boston : Harvard Business School Press; 1998.

DeVellis RF. Scale development: Theory and applications. Newbury Park, CA: Sage; 1991.

Dhillon G, Backhouse J. Current directions in IS security research: towards socio-organizational perspectives. Inf Syst J. 2001;Volume 11(2):127–53.

Dinev T, Goo J, Hu Q, Nam K. User behaviour towards protective information technologies: the role of national cultural differences. Inf Syst J. 2009 Jul;19(4):391–412.

Doty DH, Glick WH. Common Methods Bias: Does Common Methods Variance Really Bias Results? Organ Res Methods. 1998 Oct 1;1(4):374–406.

Dzazali S, Zolait AH. Assessment of information security maturity: An exploration study of Malaysian public service organizations. J Syst Inf Technol. Emerald Group Publishing Limited; 2012 Mar 17;14(1):23–57.

Eberl M. An Application of PLS in Multi-Group Analysis: The Need for Differentiated Corporate-Level Marketing in the Mobile Communications Industry. In: Vinzi VE, Chin WW, Henseler J, Wang H, editors. Handb Partial Least Squares . Springer Berlin Heidelberg; 2010. p. 487–514 .

Fagnot IJ. Behavioral information security. In: Janczewski L, Colarik A, editors. Encycl cyber Warf cyber Terror. PA: USA: Hershey; 2008. p. 199–205.

Feledi D, Fenz S. Challenges of Web-Based Information Security Knowledge Sharing. 2012 Seventh Int Conf Availability, Reliab Secur. IEEE; 2012. p. 514–21.

Gal-Or E, Ghose A. The Economic Incentives for Sharing Security Information. Inf Syst Res. INFORMS; 2005 Jun 1;16(2):186–208.

Gordon LA, Loeb MP, Lucyshyn W. Sharing Information on Computer Systems Security: An Economic Analysis. 2003;22(6).

Guo H. Knowledge for Managing Information System Security: Review and Future Research Directions. CONF-IRM 2008 Proc. 2008. p. Paper 37.

Hair J, Ringle C, Sarstedt M. PLS-SEM: Indeed a Silver Bullet. J Mark Theory Pract. 2011;19(2):139–52.

Henderson JC, Venkatraman N. Strategic alignment: leveraging information technology for transforming organizations. IBM Syst J. 1993 Jan 1;32(1):4–16.

Hinkin TR, Tracey JB. An Analysis of Variance Approach to Content Validation. Organ Res Methods. 1999 Apr;2(2):175–86.

Hofstede G. Culture’s Consequences: International Differences in Work Related Values. Beverly Hills, CA: SAGE; 1980.

Hofstede G. National cultural dimensions [Internet]. Natl. Cult. Dimens. 2013 [cited 2013 Jun 13]. Available from: http://geert-hofstede.com/dimensions.html

Hu Q, Dinev T, Hart P, Cooke D. Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. Decis Sci. 2012 Aug 28;43(4):615–60.

IBM Corporation. SPSS Statistics. IBM Corporation; 2010.

Ifinedo P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Comput Secur. 2012 Feb;31(1):83–95.

ISACA. Information Security Governance Guidance for Boards of Directors and Executive Management, 2nd Edition. Rolling Meadows, Illinois; 2006.

Jarvis CB, MacKenzie SB, Podsakoff PM. A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research. J Consum Res. The University of Chicago Press; 2003 Sep 21;30(2):199–218.

Joreskog KG, van Thillo M. LISREL: A General Computer Program for Estimating a Linear Structural Equation System Involving Multiple Indicators of Unmeasured Variables. 1972 Nov 30;

Kandias M, Mylonas A, Virvilis N, Theoharidou M, Gritzalis D. An Insider Threat Prediction Model. In: Katsikas S, Lopez J, Soriano M, editors. Trust Priv Secur Digit Bus Lect Notes Comput Sci. Berlin Heidelberg: Springer; 2010. p. 26–37.

Kandias M, Stavrou V, Bozovic N, Gritzalis D. Proactive insider threat detection through social media. Proc 12th ACM Work Work Priv Electron Soc - WPES ’13 [Internet]. New York, New York, USA: ACM Press; 2013 [cited 2014 Mar 5]. p. 261–6. Available from: http://dl.acm.org/citation.cfm?id=2517840.2517865

Kankanhalli A. An integrative study of information systems security effectiveness. Int J Inf Manage. 2003 Apr;23(2):139–54.

Karjalainen M, Siponen M, Petri P, Suprateek S. One Size Does Not Fit All: Different Cultures Require Different Information Systems Security Interventions. PACIS 2013 Proc. 2013. p. Paper 98.

Kayworth T, Whitten D. Effective Information Security Requires a Balance of Social and Technology Factors. MIS Quartely Exec. 2010;9(3):303–15.

Keil M, Tan BCY, Wei K-K, Saarinen T, Tuunainen V, Wassenaar A. A Cross-Cultural Study on Escalation of Commitment Behavior in Software Projects. MIS Q. Society for Information Management and The Management Information Systems Research Center; 2000 Jun 1;24(2):299.

Klarner P, Sarstedt M, Hoeck M, Ringle CM. Disentangling the Effects of Team Competences, Team Adaptability, and Client Communication on the Performance of Management Consulting Teams. Long Range Plann. 2013 Jun;46(3):258–86.

Knapp KJ, Marshall TE, Rainer RK, Ford FN. Information Security Effectiveness: Conceptualization and Validation of a Theory. Eyob E, editor. Int J Inf Secur Priv . IGI Global; 2007 Jan 31;1(2):37–60.

Kolodziej-Smith R, Friesen D, Yaprak A. Does Culture Affect how People Receive and Resist Persuasive Messages? Research Proposals about Resistance to Persuasion in Cultural Groups. Glob Adv Bus Commun. Antwerp; 2013. p. Article 5.

Kvale S. Interviews. An introduction to qualitative research interviewing. Thousand Oaks, CA: Sage Publications; 1986.

Langlois CC, Schlegelmilch BB. Do Corporate Codes of Ethics Reflect National Character? Evidence from Europe and the United States. J Int Bus Stud. Nature Publishing Group; 1990 Dec 1;21(4):519–39.

Lee AS. Integrating Positivist and Interpretive Approaches to Organizational Research. Organ Sci. 1991 Nov 1;2(4):342–65.

Liu D, Ji Y, Mookerjee V. Knowledge sharing and investment decisions in information security. Decis Support Syst. 2011;52(1):95–107.

Lynn MR. Determination and Quantification Of Content Validity. Nurs Res. 2006;35(6):382–6.

MacKenzie SB, Podsakoff PM, Podsakoff NP. Construct measurement and validation procedures in MIS and behavioral research: integrating new and existing techniques. MIS Q. 2011 Jun 1;35(2):293–334.

Markus HR, Kitayama S. Culture and the self: Implications for cognition, emotion, and motivation. Psychol Rev. 1991;98(2):224–53.

Mishra S, Dhillon G. Information Systems Security Governance Research: A Behavioral Perspective. 2nd Annu Symp Inf Assur. New York State; 2006.

Navarro A, Acedo F, Losada F, Ruzo E. Integrated Model of Export Activity: Analysis of Heterogeneity in Managers’ Orientations and Perceptions on Strategic Marketing Management in Foreign Markets. J Mark Theory Pract. 2011;19(2):187–204.

Nunnally JC, Bernstein I. Psychometric Theory . 3rd ed. New York: McGraw Hill.; 1994.

Pai J-C. An empirical study of the relationship between knowledge sharing and IS/IT strategic planning (ISSP). Manag Decis. Emerald Group Publishing Limited; 2006 Jan 1;44(1):105–22.

Paternoster R, Simpson S. Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime. Law Soc Rev. 1996;30(3):549–84.

Pavlou PA, Chai L. What Drives Electronic Commerce Across Cultures? A Cross-Cultural Empirical Investigation of the Theory of Planned Behavior . J Electron Commer Res . 2002;3(4):240–53.

Pavlou PA, Liang H, Xue Y. Understanding and mitigating uncertainty in online exchange relationships: a principal- agent perspective. MIS Q. 2007 Mar 1;31(1):105–36.

Petter S, Straub D, Rai A. Specifying formative constructs in information systems research. MIS Q. 2007;31(4):623–56.

Podsakoff PM. Self-Reports in Organizational Research: Problems and Prospects. J Manage. 1986 Dec 1;12(4):531–44.

Podsakoff PM, MacKenzie SB, Lee J-Y, Podsakoff NP. Common method biases in behavioral research: a critical review of the literature and recommended remedies. J Appl Psychol. 2003 Oct;88(5):879–903.

Puhakainen P, Siponen M. Improving employees' compliance through information systems security training: an action research study. MIS Q. 2010 Dec 1;34(4):757–78.

PWC Advisory Services, Security. The Global State of Information Security® Survey 2013 [Internet]. 2013. Available from: http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml

Reinartz W, Haenlein M, Henseler J. An empirical comparison of the efficacy of covariance-based and variance-based SEM. Int J Res Mark. 2009 Dec;26(4):332–44.

Rhodes J, Hung R, Lok P, Lien BY-H, Wu C-M. Factors influencing organizational knowledge transfer: implication for corporate performance. J Knowl Manag. Emerald Group Publishing Limited; 2008 May 30;12(3):84–100.

Ringle CM, Wende S, Will A. SmartPLS. Hamburg: University of Hamburg; 2005.

Rocha Flores W, Antonsen E. The development of an instrument for assessing information security in organizations: Examining the content validity using quantitative methods. Proc 2013 Int Conf Inf Resour Manag. Natal, Brazil, May 22-24; 2013.

Rocha Flores W, Holm H, Svensson G, Ericsson G. Using Phishing Experiments and Scenario-based Surveys to Understand Security Behaviours in Practice. Inf Manag Comput Secur. 2014;(To be available).

Rocha Flores W, Korman M. Conceptualization of Constructs for Shaping Information Security Behavior: Towards a Measurement Instrument. Proc th 7th Annu Work Inf Secur Priv. Orlando, Florida, USA, December 16; 2012.

Rogelberg SG, Stanton JM. Introduction: Understanding and Dealing With Organizational Survey Nonresponse. Organ Res Methods. 2007 Apr 1;10(2):195–209.

SANS. gpwn-list [Internet]. 2013 [cited 2012 Nov 1]. Available from: https://lists.sans.org/mailman/listinfo/gpwn-list

Sarmento A. Knowledge management: at a cross-way of perspectives and approaches. Inf Resour Manag J. 2005;18(1):1–7.

Sarstedt M, Ringle CM. Treating unobserved heterogeneity in PLS path modeling: a comparison of FIMIX-PLS with different data analysis strategies. J Appl Stat. Taylor & Francis; 2010 Aug;37(8):1299–318.

Segars AH, Grover V. Profiles of Strategic Information Systems Planning. Inf Syst Res. INFORMS; 1999 Sep 1;10(3):199–232.

Siponen M, Vance A. Neutralization: new insights into the problem of employee systems security policy violations. MIS Q. 2010 Sep 1;34(3):487–502.

Siponen M, Willison R. Information security management standards: Problems and solutions. Inf Manag. 2009;46(5):267–70.

Siponen MT. An analysis of the traditional IS security approaches: implications for research and practice. Eur J Inf Syst. 2005 Sep 1;14(3):303–15.

Sobh T, Elleithy K, editors. Information Management for Holistic, Collaborative Information Security Management. Emerg Trends Comput Informatics, Syst Sci Eng. New York, NY: Springer New York; 2013. p. 211–24.

Sommestad T, Hallberg J, Lundholm K, Bengtsson J. Variables influencing information security policy compliance: a systematic review of quantitative studies. Inf Manag Comput Secur. Emerald Group Publishing Limited; 2013 Nov 19;22(1):3.

Song S. An internet knowledge sharing system. J Comput Inf Syst. 2002;42(3):25–30.

Srite M, Karahanna E. The role of espoused national cultural values in technology acceptance. MIS Q. Society for Information Management and The Management Information Systems Research Center; 2006 Sep 1;30(3):679–704.

Stewart GL, Barrick MR. TEAM STRUCTURE AND PERFORMANCE: ASSESSING THE MEDIATING ROLE OF INTRATEAM PROCESS AND THE MODERATING ROLE OF TASK TYPE. Acad Manag J. Academy of Management; 2000 Apr 1;43(2):135–48.

Straub D, Boudreau M-C, Gefen D. Validation Guidelines for IS Positivist Research. Commun Assoc Inf Syst. 2004;13(1):380–427.

Straub DW. Effective IS Security: An Empirical Study. Inf Syst Res. INFORMS; 1990 Sep 1;1(3):255–76.

Sun L, Ivastave RP, Mock TJ. An Information Systems Security Risk Assessment Model Under the Dempster-Shafer Theory of Belief Functions. J Manag Inf Syst. 2006 Apr;22(4):109–42.

Tan FB, Urquhart C, Yan S. A conceptual model for online shopping behaviour: trust and national culture. . Proc 5th Int Bus Res Forum. Temple University, Philadelphia, PA, USA.; 2004.

Trochim WMK, Donnelly JP. The Research Methods Knowledge Base . 3rd ed. Atomic Dog; 2006. p. 362.

Wang S, Noe RA. Knowledge sharing: A review and directions for future research. Hum Resour Manag Rev. 2010;20(2):115–31.

Warkentin M, Johnston AC. It Governance and Organizational Design for Security Management. In: Straub DW, Goodman S, Baskerville RL, editors. Inf Secur Policy, Process Pract. 2007. p. 46 – 68.

Warkentin M, Johnston AC, Shropshire J. The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. Eur J Inf Syst. Nature Publishing Group; 2011 Jan 25;20(3):267–84.

Warkentin M, Willison R. Behavioral and policy issues in information systems security: the insider threat. Eur J Inf Syst. Nature Publishing Group; 2009 Apr 1;18(2):101–5.

Veiga A Da, Eloff JHP. An Information Security Governance Framework. Inf Syst Manag. ACM Press; 2007 Oct 2;24(4):361–72.

Werlinger R, Hawkey K, Beznosov K. An integrated view of human, organizational, and technological challenges of IT security management. Inf Manag Comput Secur. Emerald Group Publishing Limited; 2009 Mar 20;17(1):4–19.

Zakaria O. Internalisation of Information Security Culture amongst Employees through Basic Security Knowledge. In: Fischer-Hübner S, Rannenberg K, Yngström L, Lindskog S, editors. Secur Priv Dyn Environ. Boston: Kluwer Academic Publishers; 2006. p. 437–41.

Appendix A. Items for constructs

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 organization saves and renews important knowledge on both general information security and threats related to information security onto the computer for easy browsing.