Received 18 July 2016
Revised 13 December 2016
19 March 2017
8 June 2017
Accepted 9 June 2017

Information security management and the human aspect in organizations

Harrison Stewart
Faculty of Information Technology, Univeril Technology Industry, Hamburg, Germany, and University of Derby, Derby, UK, and

Jan Jürjens
Fraunhofer Institute for Software Technology (IST), University of Koblenz-Landau, Universitat Koblenz-Landau, Koblenz, Germany

Abstract

Purpose – The aim of this study is to encourage management boards to recognize that employees play a major role in the management of information security. Thus, these issues need to be addressed efficiently, especially in organizations in which data are a valuable asset.

Design/methodology/approach – Before developing the instrument for the survey, first, effective measurement built upon existing literature review was identified and developed and the survey questionnaires were set according to past studies and the findings based on qualitative analyses. Data were collected by using cross-sectional questionnaire and a Likert scale, whereby each question was related to an item as in the work of Witherspoon *et al.* (2013). Data analysis was done using the SPSS.3B.

Findings – Based on the results from three surveys and findings, a principle of information security compliance practices was proposed based on the authors' proposed nine-five-circle (NFC) principle that enhances information security management by identifying human conduct and IT security-related issues regarding the aspect of information security management. Furthermore, the authors' principle has enabled closing the gap between technology and humans in this study by proving that the factors in the present study's finding are interrelated and work together, rather than on their own.

Research limitations/implications – The main objective of this study was to address the lack of research evidence on what mobilizes and influences information security management development and implementation. This objective has been fulfilled by surveying, collecting and analyzing data and by giving an account of the attributes that hinder information security management. Accordingly, a major practical contribution of the present research is the empirical data it provides that enable obtaining a bigger picture and precise information about the real issues that cause information security management shortcomings.

Practical implications – In this sense, despite the fact that this study has limitations concerning the development of a diagnostic tool, it is obviously the main procedure for the measurements of a framework to assess information security compliance policies in the organizations surveyed.

Social implications – The present study's discoveries recommend in actuality that using flexible tools that can be scoped to meet individual organizational needs have positive effects on the implementation of information security management policies within an organization. Accordingly, the research proposes that organizations should forsake the oversimplified generalized guidelines that neglect the verification of the difference in information security requirements in various organizations. Instead, they should focus on the issue of how to sustain and enhance their organization's compliance through a dynamic compliance process that involves awareness of the compliance regulation, controlling integration and closing gaps

Originality/value – The rapid growth of information technology (IT) has created numerous business opportunities. At the same time, this growth has increased information security risk. IT security risk is an important issue in industrial sectors, and in organizations that are innovating owing to globalization or changes in organizational culture. Previously, technology-associated risk assessments focused on various

Information & Computer Security
Vol. 25 No. 5, 2017
pp. 494-534

2056-4961
DOI 10.1108/ICS-07-2016-0054

technology factors, but as of the early twenty-first century, the most important issue identified in technology risk studies is the human factor.

Keywords Information security, Culture and technology, Employee behaviour in technology, IT human aspects, Security and leadership

Paper type Research paper

1. Introduction

The rapid growth of information technology (IT) has increased security risks in both industrial and financial sectors. Currently, human activity is considered the most critical factor in the management of information security. Information security risks related to human activity are observed in employees from large- and medium-sized businesses where employees violate company security policies or personally engage in security theft (Vance *et al.*, 2013). These issues occur because of various factors such as poor information security awareness among employees, poor employee information security training and poorly managed teams. These factors are major threats to a company's information security. Compliance to a company security policy and frequent information security training of employees can positively impact the human aspects of security.

To eliminate the lack of security awareness and deficiencies among employees so as to enhance their approaches to information security management, it is essential to take a deeper look into these factors.

In some organizations, the human resource department plays a major role in IT security by checking, controlling and redirecting employee conduct toward successful information security management. Simply put, human resource departments are managed by an organization's management board, and the management board is responsible for planning, acquisition, information security training, as well as directing human activities, in the business domain. This indicates that the management board is responsible for controlling and directing these activities to enhance the awareness of information security among employees. Although senior management alone cannot guarantee successful risk management, it is essential for senior management individuals to execute and control information security activities (Boss *et al.*, 2009; McFadzean *et al.*, 2006).

Organizational security policies are sets of rules and regulations that govern an organization's network, and they are intended to prevent fraud and embezzlement (Compston, 2009). These policies ban criminal activities – for example, an employee hacking into a computer system or network, employees visiting inappropriate websites or the stealing of company software by/or enabled by employees. Puhakainen and Siponen (2010) argue that security awareness training has a positive impact on employee conduct, and it allows conduct to conform to company security policy.

Compliance is defined as the conforming to a rule or a policy. We hypothesize that policies are not effective in an organization that lacks policy compliance (i.e. a policy is not effective in the absence of compliance). There are two components of compliance that should be highlighted:

(1) Without compliant employees, security policies are not guaranteed.

(2) Compliance enhances the efficacy of information system security controls (Guo, 2013; Herath and Rao, 2009b).

Harrison and White (2010) added that, compliance will only occur and be effective if enforced correctly by senior managers. However, according to previous studies, there are numerous managers who lack commitment to information security management, and this

calls for education and persuasion via external or internal regulators (Ahmad *et al.*, 2012; Chang and Ho, 2006; Hsu, 2009; Hu *et al.*, 2007; Smith *et al.*, 2010). Compliance analysis is the process of comparing the applied controls with the referenced standards. Furthermore, compliance analysis is a tool used for inspecting the conformity level of the business and for finding problems that arise after the generated information security policies have been implemented.

In any case, regardless of the possibility that the previously mentioned tools or techniques are used, they come short and do not cover the entire picture of information security management. Therefore, this study addresses the following research questions:

RQ1. Do the organizations' management boards lack the skills to plan, train and direct human activities toward security awareness?

RQ2. What are the beliefs of employees regarding the outcomes of information security violations and how such violations affect information security management?

RQ3. What kind of compliance guidance for information security do organizations need to adopt, and on what essential points should this guidance focus?

RQ4. Is there any interrelation between technology and human factors that work together for the successful deployment and implementation of information security management in an organization?

We have answered the above hypothesis in their respective sections. In Section 4, our findings and analysis will answer the *RQ1* and *RQ2* and will be further illustrated in Table IV. *RQ3* will be answered in Section 6, where we will propose our nine-five-circle (NFC) principle that can be used to enhance the development and implementation of information security management policies in an organization. Section 6.2.3 will answer our last hypothesis, whereby we confirm that technology and human factors are interrelated and work together for the successful deployment and implementation of information security management in an organization.

Information security policies have a major impact on the management of security and the success of a business. According to Trcek *et al.* (2007), humans are the critical factor of information security; however, there is always complexity in the interactions between humans and technical elements. Trcek *et al.* (2007) argued that humans are the blueprint of information security, while Loster (2005) added that employee roles should be considered in the planning and implementation phases of information security policies and management. Therefore, in this study, we hypothesize that humans play a major role in security management, and this role should not be ignored.

1.1 The gap

The massive advancement in the IT sector has increased the technological needs of organizations. With widespread use and access to World Wide Web services, security has become the most critical aspect for many organizations. Many researchers have proposed measures to solve these issues; however, the quantification of security measures is still considered a challenge by many studies. According to Yeniman *et al.* (2011), employee ignorance increases data breaches and data security vulnerabilities. In an empirical study conducted by Jaeger (2013) regarding the reasons behind data breaches, 38 per cent of data breaches are due to loss of paper files; 27 per cent are due to human carelessness (e.g. losing data memory devices); and 11 per cent of data breaches are due to hacking. These data suggest that employees have a major influence on information security risk and data

breaches. Rubenstein and Francis (2008) reported on the lack of compliance toward information security, as well as violations of access policies. Vance *et al.* (2013) argued that lack of information security training and violations of policy occur due to unskilled or poor managers.

1.2 Aim

The aim of this study is to encourage management boards to recognize that employees play a major role in the management of information security. Thus, these issues need to be addressed efficiently, especially in organizations in which data are a valuable asset. Engaging workplace employees in security awareness is a social event that also strengthens the security of a company's information. A strong company foundation in security awareness among employees ensures that employees are informed of company security policies. Employees trained in security awareness also improve innovation and increase work productivity. Therefore, this current study also aims to highlight the importance of formal and informal security awareness of employees to enhance employee productivity.

In recent decades, many organizations have focused on technology-based solutions – e.g. intrusion detection mechanisms to address information security (PricewaterhouseCoopers, 2008). However, Safa *et al.* (2015) argued that these approaches do not guarantee a secure business in the context of information security management. Furthermore, technology-based approaches often increase administrative and supportive costs and seldom dispose of the risk (Cavusoglu *et al.*, 2009; Dhillon and Backhouse 2001; Siponen 2005). The implementation of such technologies can be tedious for employees when exploring information systems due to the informational gaps that come with software and hardware. Pahnila *et al.* (2007) also argued that, despite such huge investments, both software and hardware often do not decrease the security problems faced by these organizations. Numerous studies have also investigated how employees are targeted by hackers through different channels (e.g. social media); therefore, investing in multiple technology defense layouts has little impact on information security (Abawajy 2014; Arce, 2003; Jansson and von Solms, 2013, Schultz *et al.*, 2001; Zhang *et al.*, 2009).

1.3 Paper structure

We began this paper with a brief introduction concerning the issues, the reasoning and the need for this study, including the aims and objectives of the research.

In Section 2, a literature review will be presented to analyze existing situations. This analysis will be based on the present study's findings, as well as analyses reported by other researchers. Gaps in current knowledge will be indicated, such as the lack of a single theory for poor security awareness.

In Section 3, a conceptual framework will be developed to evaluate a security situation. Here, a questionnaire pertaining to the situation, with multiple choice answers, will be prepared and provided to 600 individuals of varying ages, sex, field of employment, positions, designations, and income groups. The results of the survey will be quantified, and presented graphically. These data will help to identify major and minor causal factors between human aspects and information security risk.

Section 4 explores the methodology in which the proposed framework will be evaluated and verified via quantitative analysis. The reliability and validity of the findings will be further tested using statistical software tools (e.g. SPSS and SEM). These techniques will provide an outcome to fulfill the research aims. We hypothesize that lack of information security management training and lack of situational awareness among employees will be the top reasons for poor information security management.

In Section 5, we present inferential limitations encountered during this study.

Section 6 will be based on the results from the methodology section. Herein, we will present a new compliance guideline based on the NFC framework to enhance the deployment and implementation of information security policy compliance.

In Section 7, we present the implications of this research, based on practice and future research possibilities.

Section 8 concludes with important points that organizations should consider when choosing IT security standards. We point out that the important points and suggestions generated herein may only work with specific types of organizations.

2. Literature review

There have been numerous studies on information security management – for example, the information security viability model proposed by Kankan-Halli *et al.* (2003), and the planning of security and risk management approach proposed by Soo Hoo (2000). Cavusoglu *et al.* (2004a, 2004b) studied investment in information security and assessment. While these studies have improved our comprehension of information security from different viewpoints, their outcomes have not been able to solve all the security issues that face organizations.

During the past decades, a significant amount of research has been done on numerous aspects of information security management – for example, external abuse (Simmonds *et al.*, 2004; Vivo *et al.*, 1998), internal assaults (Guo and Yuan, 2012; Harrington, 1996; Straub and Nance, 1990), policies acceptance strategies (Siau *et al.*, 2002; Son, 2011) and computer crimes (Cronan *et al.*, 2006). These studies indicate a great increase in the field of information security management research between 2000 and 2007 (Chen *et al.*, 2010); however, much of this research focuses on internet abuse (Lim and Teo, 2005), individual behavior, compliance and impact of deterrence on employee conduct (Hovav and D'Arcy, 2012). Research at the organization level has not received a lot of attention. Lee and Kozar (2008) proposed the adoption of security technology and practices, while Siponen and Vartiainen (2004) proposed traditional standard methods due to the complexity of security standards adoption. According to Kotulic and Clark (2004), the relative lack of firm-level research may mirror the reluctance of firms to uncover information with respect to their security strategies and breaches; subsequently, organizations choose to evade collaboration in security practices. Richardson (2011) demonstrated a drop in security personnel response to security measure surveys as compared to earlier studies. Numerous meta-analyses in data security have been performed that recommend a holistic approach to dealing with current information security management issues. These studies propose several ways to deal with information security to obtain a bigger picture of information security. A few distinct frameworks have been proposed to address information security. These frameworks incorporate simulation models, formal models, dynamic models and economic models for security (Dhillon and Backhouse, 2001; Siponen, 2005; Sunyaev *et al.*, 2009).

2.1 Human role in information security

Other studies have also demonstrated that many organizations neglect the centrality of human behavior in information security management, and that this has caused failures in information security. Webb *et al.* (2014) proposed a situation-aware information security risk management (SA-ISRM) model to supplement the ISRM procedure; however, their model was only focused on the deficiencies of ISRM. Here, the researchers neglected security policy compliance based on individual employees. Li *et al.* (2010) argued how recent studies on information security management have neglected the perceived benefit of degenerate

behavior, individual norms and organizational settings. Their research model used an online survey that was sent to organization employees. However, their work was only based on internet use policy (IUP) compliance. Thus, they focused on employees in an organization with an internet use policy and realized the risks posed by employees in the context of security management in an organization. They also recommended the significance of considering compliance decisions as driven by a cost–benefit analysis, limited by individual standards and organizational setting factors. Therefore, their work did not cover all the elements of human behavior and social structure in the organization, such as human ability, culture, information security management, top personnel, technology and how all these factors interrelate and work together. Here, we emphasize that both Li *et al.* (2010) and Webb *et al.* (2014) indicate the limitations of a number of theory-based empirical studies on employee security policy compliance that we address in this study.

Da Veiga and Martins (2016) conducted a questionnaire survey where they studied the interrelationship between human, technology and strategy controls. Their data were derived from information security culture assessment (ISCA), based on a case study of an international financial institution at four intervals over a period of eight years, across 12 countries. Their study was centered on the effects of security-awareness training, and they recommended further research to be conducted on employees who comply to information security policy and others who do not, as well as extending the research across national and cultural boundaries.

Herath and Rao (2009a) argued the need for organizations to deploy different approaches to enhance data security. Ifinedo (2012) added that many organizations are heavily investing in technology-based measures, but these often do not yield positive results due to the lack of attention allotted to employee behavior. Crossler *et al.* (2013) concluded that a combination of technology-based solutions and employee security behavior plays a major role in information security management, and this calls for a strategic approach to model a solution to unify technology, human, cultural and organizational factors.

2.2 Technology role in information security

Numerous studies have investigated cyber-attack prevention. According to Li *et al.* (2009), limited countermeasures are available to prevent cyber-attacks. Mirkovic and Reiher (2005) proposed the source-end defense points. Chen and Hwang (2006) also proposed the core-end defense techniques, while Wang *et al.* (2007) proposed the casualty end protection, and Seo *et al.* (2013) proposed the versatile probabilistic filter planning. All the above countermeasures have been developed to prevent flood attacks, but none were aimed at employees. Other traditional techniques such as cryptography and firewalls have also been proposed as distinct options to avoid intruders and maintain data confidentiality, integrity and authentication (CIA) (Wright *et al.*, 2004).

According to Singh *et al.* (2013), technology is not capable of providing a dependable answer for hierarchical information security needs and challenges. Werlinger *et al.* (2009) recommended that, to overcome the constantly challenging issues of information security management, it is important that in combination with a technical approach, employee and organizational factors should also be addressed. In their recommendation, the technical approaches are initiating, planning, acquisition of new innovations, budgetary designations and purchasing innovative hardware and software. Human factors include skilled staff recruitment, hiring, information security management training and employee motivation. Organizational factors include staff compliance with organization rules and regulations, frequent information security management training, rigid managerial direction and presence of compliance departments. Hence, we hypothesis in this study that technology

and human factors are interrelated and need to be addressed efficiently for the successful deployment of information security management (Werlinger *et al.*, 2009; Abawajy, 2014; Arachchilage and Love, 2014; Kritzinger and von Solms, 2010).

2.3 The financial impact on information security

According to Safa and Ismail (2013), information security breaches cause financial costs for organizations and affect organization reputation. In addition to adopting technology-based solutions, appropriate data security conduct can mitigate the risk of information security breaches in an organization. Abawajy (2014) determined the important role of security compliance awareness among employees, such as conduct and behavior, during a study on security risk mitigation. This research was subsequently supported by findings generated by Arachchilage and Love (2014). However, both researchers neglected human ability, culture, information security management, technology and how all these variables interrelate and need to be addressed efficiently in an organization. Kritzinger and von Solms (2010) held a workshop where they divided users into home and organizational environments to confirm the important role that both groups play in security awareness. They further confirmed the efficacy of the methods used and the strong impact of policy enforcement. However, Kritzinger and von Solms (2010) based their study on private and public behavior, but neglected culture, familiarity, management, technology and how all these factors interrelate and work together. Safa *et al.* (2015) found that knowledge of information security (information security) is linked to better understanding, familiarity and capacity to manage and overcome crises.

2.4 Misuse of information security knowledge sharing

The misuse of information security resources has been recognized in numerous studies as a significant problem, often identified during information security mitigations. This supports the hypothesis found in other studies that assessed employee behavior, that workers often take part in inappropriate behaviors increase security risks. These findings caused many organizations to concentrate on placing impediments and preventative systems such as sanctions on employees for the misuse of computers. Straub and Nance (1990) explored how to detect computer abuse and how to sanction employees. They advised organizations to sanction employees severely to prevent other employees from conducting the same or similar activities. Willison (2006) studied the impacts of employee misbehavior and subsequent risks for information security by using rational decision and crime preventive methodologies to explore the relationship between the culprit and the context. According to Willison, organizations need to concentrate on the inappropriate behavior of employees in various levels and enforce preventive measures to decrease employee behaviors that increase information security risks.

A study by Lee and Lee (2002) focused on the deterrence hypothesis along with social speculations to clarify the impact of information security management, information security programs and organizational factors. Lee and Lee (2002) analyzed both insider and outsider information security abuse by evaluating organizational factors and the causes of the security abuse. They determined that the improvement of social networks via organizational factors could eliminate the misuse of information systems in an organization. However, Lee and Lee based their work on how social relationships and traditional counter-measures impact the decision process employees that misuse computers by using the general deterrence theory (GDT) for guidelines (e.g. as in the work of Straub and Nance, 1990). The GDT is a basis for security awareness, security training and education and minimizes cost

(Beccaria, 1963); however, it comes with some limitations and needs to be enhanced and revised. GDT also neglects the interrelationship between technology and humans.

2.5 Information security management standards

Siponen and Vartiainen (2004) analyzed BS7799, PCI BS, ISO/IEC17799: 2000, GASPP/GAISP and the SSE-CMM to determine and compare how international information security management guidelines play a key role in managing and confirming the organizational information security. They realized that those listed guidelines were too generalized and neglected the verification of the difference in information security requirements in various organizations. Furthermore, these guidelines were not meant for international information security standards because of their general practices in nature. Owing to these shortcomings, they recommended that information security management guidelines should be seen as "a library of material for information security management for specialists" (Siponen and Vartiainen, 2004). An empirical study was conducted by Kotulic and Clark (2004) in the sector of security risk management (SRM) where they proposed a conceptual model to enhance SRM on organizational level. However, their model was not able to detect and specify information systems security. According to Baskerville (1993), computer misuse (i.e. use for purposes other than that intended by the company, such as recreational activities) is the main cause of information security risk, and they recommended that information security experts and IT managers should implement systems that will detect information security abuse and specify information systems security.

Despite the fact that the vast majority of the data security literature focuses on sanctions and technology-based solutions, little data are available on the roles management boards, employee information security training and collaboration play in information security management. The current study will not only evaluate technology and the responses of individual employees but will also target individual managers because they are responsible for the proper implementation of security compliance. Our study further analyzes organizational culture, collaboration, employee familiarity with security management, managing director skills, governance, leadership, records management, information access, communication, compliance, technology and how all these factors interrelate and work together. The expectation is that security compliance needs to be initiated from the top level down to the lowest level in every organization.

In our work, the factors in our research are both dependent and independent factors. These factors are interrelated and the complex design reflects that a number of independent factors may work together to determine the level of the dependent factor. For example, we investigate the cause of the issues that an organization faces during policy compliance deployment (the dependent variable). Here we hypothesize that our SPSS findings such as lack of security training-awareness, lack of management directives, absence of compliance policy, lack of security interest and failure of hardware (five independent factors) may work separately or in conjunction with each other in determining the condition of the dependent factors. The identification of independent and dependent factor relies on the particular research question and conceptual underpinning of our work. Here, the two labels "dependent" and "independent" can be used in a specific design differently from ours. That is to say, there is nothing inherent in a factor itself that makes it independent or dependent; a factor that is independent in our design may in another work be used as the dependent factor or the effect of estimation.

3. Method

Uneducated employees and/or unethical employee behavior are the causes of information security risk (Abawajy, 2014; Arce, 2003). It is clear that security risk cannot just be eliminated solely via security awareness without effective implementation and enforcement of compliances by organization management boards. In this study, we first analyzed levels of employee information security awareness regarding information security risk via their observational and behavioral viewpoints. We were also aware that employee awareness of information security does not guarantee that they will be compliant; therefore, we extended the scope of the study to analyze top management board individuals' information security awareness, and we proposed an effective information security policy compliance guideline.

We developed a conceptual framework, illustrated in Figure 1, using the simple build tool (SBT), to explain how employees comply with information security policies.

Before developing the instrument for the survey, we first identified and developed effective measurements built upon the existing literature, prepared our survey questionnaires according to past studies, and analyzed our findings based on previous qualitative analyses. We were able to collect data by using a cross-sectional questionnaire and a Likert scale as in the work of Ifinedo and Olsen (2014) and Witherspoon *et al.* (2013).

All surveyed questions shown in Appendix are related to an item illustrated in Table I. Data analysis was conducted with SPSS as described in the SPSS Analysis diagram in Figure 2.

3.1 Data collection

In Germany, we approached different organizations that ranged in both size and how they approach information security management. We then divided the three participating organizations into cases: Case 1, a private bank with over 1,500 employees; Case 2, an automobile manufacturer; and Case 3, a FinTech startup company with 125 employees. Participants were requested to answer different questions, including demographic information including age, gender, and position. We focused on data from the senior directors, functional managers, IT specialists and personnel in all three organizations. All participants had internet access and use the internet in various departments.

A preliminary workshop for a pilot test explained the questions to the participants and ensured that each participant understood the purpose of the research study. Each question was explained in various ways to ensure that all questions were understood in the same manner by all participants. After this phase, participants were asked to answer the cross-

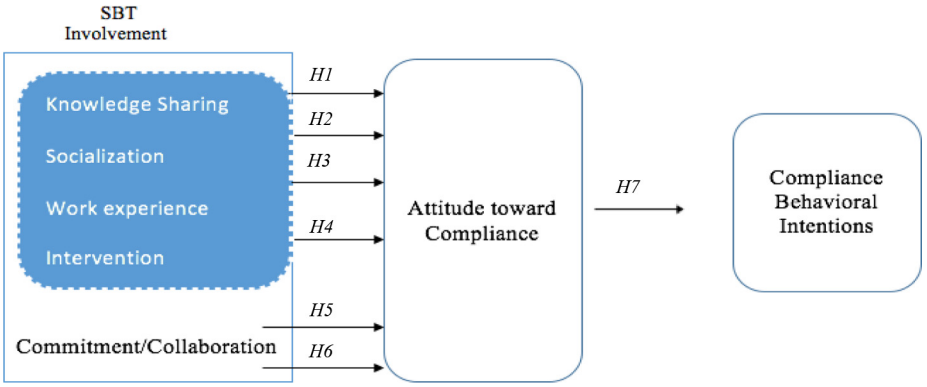

Figure 1.
A conceptual framework

Question related items	Description
Knowledge and information management (KIM)	Q1-Q30 are related to how the employees value and use information in the company. For example, if they are aware of KIM and who is responsible for their organization KIM as well as how their organizations have assessed and identified critical information
Records management	Q31-Q38 are related to how organizations keep records, share information, destroy and dispose created information. Furthermore, they are also related to the responsibility of record management and their storage, the sustainability of digital records, retention procedures, disposal policies and how data are transferred
Information access	Q39-Q44 are related to how these organizations secure data and re-use data, how they meet freedom of information (FOI) requests and if they are aware of their technical environment that enhances their information
Compliance/governance and leadership	Q45-Q62 are related to change management programs that are held in the organization. Subsequently, change management programs and clarified procedures that enable them to examine completeness, availability and usability of data asset after any change. The questions are also related to information security training, induction programs, staff responsibilities, change management, policies and guidance. We also wanted to be informed on governance and leadership in these organizations such as: any naming conventions that are mandatory to abide by as well as their strategic management, business objectives, resourcing, risk management and management supports and control
Culture	Q63-Q69 are based on both individual and organizational culture. Furthermore, these questions are also related to employees' commitment, knowledge sharing, collaboration, communication and understanding. For example, how effective is the sharing of knowledge enhances KIM networks, communities and if there are several strategies that have been adopted to enhance internal communication and collaboration in these organizations

Table I.
Questionnaire and related items

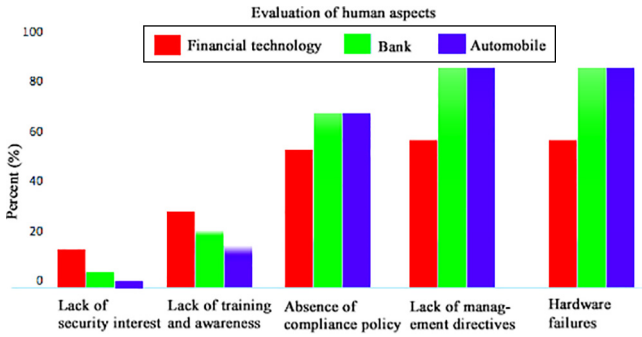

Figure 2.
SSPS analyzer

sectional questionnaire survey composed of closed-ended questions. These questions were intended to gather and measure quantitative data on a diversity of interests.

We applied the Microsoft© Access Management Matrix that helped us to determine what data would be needed for this study, and from whom to collect these data, by listing all management levels vertically and department levels horizontally. Owing to data policy, an agreement was written and signed by the researchers stating that the collected data would

be used for only this study and would not be shared with any third party. After they agreed to the terms and conditions, we presented them with the questionnaires. The pilot testing during the initial phase assured that all participants understood the questions. The pilot test consisted of 70 questions, compared to the 50 questions in the final version shown in the Appendix. Time spent on social media sites via using company computers and networks was questioned as well. The role of employees in information security breaches and their adherence to security policies were also asked. A comment field was added in the form for participants to share their experiences, worries and the reasons that drive them not to abide by information security policies.

We extended the standard data collection and sped up collection by sending a link of the website form via a mass mail to all other participants. The top personnel were asked how they view their roles in information security management and infrastructure development. They were also asked how they manage their security policy, how they see the role of human factors in information technology, and how they train their personnel on information security risks. The surveys took an estimated 45 min to complete. All answers were saved in a MySQL database.

3.2 Demographics

The reason for this research was to explore information security management, explore the human aspect in organizations and propose a compliance guideline for organizations. We mailed a total of 955 questionnaires to participants using mass mail software, and received 633 completed responses. These data were saved in a database for further analyses. We also printed 100 copies and distributed them to other participants, so that our answered questionnaires totaled 733, which enabled us to analyze the data.

3.3 Results

We used a structural equation model (SEM) as was conducted in Hair *et al.* (2010) because of the simplicity and accuracy of this type of model. SEM has various methodologies that enabled the depiction of relationships among variables. It also provided a quantitative sample of our proposed model (Tables II and III). Furthermore, because our work in this study was based on past literature reviews, involvement theories and social hypotheses, we used the three fundamental methodologies of SEM: confirmatory factor analysis, regression analysis and path analysis, similar to the work of Schumacker and Lomax (2010). Certain variables that could not be observed, such as collaboration, job contentment, employee devotion, work experience, socialization, creativity, knowledge sharing via SNS, commitment and others, were measured by few items. These variables were considered as latent variables which were then modelled using both the structural and measurement models within SEM.

Following the work of Gaur (2009), our measurement model focused on the relationship that exists between the variables we observed and those we classified as latent, while our structural model focused on the latent variables.

4. Findings and analysis

In all three organizations in our study, we found that the main issues that trigger security incidents and that hinder the accomplishment and enhancement of information security compliance were based on different factors. For example, we found that employee behavior is the most common obstacle associated with information security compliance (e.g. password sharing, password written down on a piece of paper, using shortcuts, visiting unauthorized websites, downloading unapproved internet programs from the internet,

Variables	Total (%)
Gender	
Male	60
Female	40
Age	
18-30 years	20
31-40 years	35
41-50 years	40
50 + years	5
Position	
Senior directors	15
Functional directors	20
IT specialists	15
Personnel	50
Participants from each CASE	
CASE 1 – Bank	60
CASE 2 – Automobile	25
CASE 3 – FINTECH startup	10

Table II.
Demographic of participants

Level of education	Academic	Group Administrative	Students	Total
Elementary school				
Number	0	15	0	
%	0.0	1.14	0.0	
Secondary school				
Number	0	33	0	
%	0.0	2.5	0.0	
High school				
Number	2	211	0	
%	0.15	16.05	0.0	
Associate programs				
Number	3	27	776	
%	0.23	2.05	59.1	
HND				
Number	2	19	0	
%	0.15	1.4	0.0	
Bachelor				
Number	59	21	0	
%	4.5	1.6	0.0	
Masters				
Number	37	5	0	
%	2.81	0.4	0.0	
PhD				
Number	95	9	0	
%	7.2	0.7	0.0	
Total				
Number	198	340	776	1314
%	15.06	25.87	59.1	

Table III.
Demographics of respondents based on educational level

opening unapproved email attachments, disregarding important security strategies, lack of knowledge, poor information security training, keeping relevant information to themselves, lack of commitment, lack of security awareness, security infringement(s) not reported, culprit(s) not punished, weak security-related guidelines and lack of security compliance regulations). On the organizational level, we found that employees do not comply with organization rules and regulations due to lack of organization handbooks with clear rules and regulations, as well as lack of information security training, lack of managerial direction and absence of compliance departments. On the technical level, we found that both the automobile and the bank institutes were still using legacy technology devices and traditional information security management standards that do not meet their needs.

Furthermore, we realized that in all the organizations, employees were reluctant to share knowledge or collaborate in the context of information security. The FinTech organization lacked the following: effective information security training courses, workshops, security notices, monthly mass-mails in the context of information security, company social network webpage and general company procedures. All these findings answer *RQ1* and *RQ2* as illustrated in Table IV.

To determine if our conceptual framework and findings describe employee information security activities that occur over the span of managing day-to-day activities, we used the SPSS statistical software to develop an in-depth visual evaluation of the findings. This visual evaluation enabled us to detect patterns and relationships that exist with employee

Organizations	Causes	Hindrance
Bank	Poor or ill management, employee errors, and noncompliance	Due to poor security "know-how" and "know-why". Lack of security awareness and training respectively. Poor administrative directives and/or roles
	Access violation: malicious and/or viral software	Poor organizational structure. Lack of knowledge on whom to contact as well as the absence of clear definitions of security process and roles. Lack of collaboration, communication and commitment
	Not complying with organization rules and regulations	Lack of security compliance regulations and lack of security policy compliance training
Automobile	Poor or ill management, employee errors, and noncompliance	Due to poor security "know-how" and "know-why". Lack of security awareness and training respectively. Poor administrative directives and roles. Lack of collaboration, communication and commitment
	Access violation: malicious and/or viral software	Poor organizational structure. Lack of knowledge on whom to contact as well as the absence of clear definitions of security process and roles
	Not complying with organization rules and regulations	Lack of security compliance regulations and lack of security policy compliance training
	Sharing passwords and engaging in private social networks and/or emails	Lack of security awareness; security infringement(s) not reported and culprit(s) not punished
FinTech startup	Poor or ill management, employee errors, and noncompliance	Due to poor security "know-how" and "know-why". Lack of security awareness and training respectively. Poor administrative directives and roles
	Access violation: malicious and/or viral software	Poor organizational structure. Lack of knowledge on whom to contact as well as the absence of clear definitions of security process and roles. Lack of commitment
	Hardware failure(s)	Budget constraint(s)

Table IV.
Causes of security incidents and hindrance

information security-related conduct in the three organizations. The SPSS analysis produced the results that satisfied our main research aim.

As shown in Figures 2 and 3, the primary driver of security risk is not only employee error but also lack of information security training and unskilled management boards. The head of the IT manager at the bank stated that human errors are the main issues of the bank, e.g. employees downloading unauthorized software that many contain viral and/or malicious data and/or programs. The data protection unit manager also stated that lack of information security training has become a problem that need to be addressed. He added that the heads of the organization consider security training as a waste of investment. The head of the management board added that most security training costs large sums of money, yet have not delivered results or improvements.

We also identified that both the automobile company and the FinTech startup had difficulties with administrative errors and security managers. Most of their security managers are bachelor degree-holding individuals that have no or low experience in real-world information security management. The FinTech company also had budget constraints that hindered them from implementing strategic security mechanisms and/or a process to enhance or protect organizational data.Other attributes such as budget constraints, operation, organizing, budgeting, time-frame, managing and reporting procedures and cost of security training and outcomes were all part of our findings.

Our literature review and results indicate various aspects of administering information security management in different contexts. We focused on human aspects in information security management, technical factors, organization policies, employee security awareness training, technologies adopted, employees' collaboration and commitment to the organization, activities of the management boards and how security is viewed in their business domain. From this we cannot simply conclude that information security awareness will keep data safe without training the employees on this subject. Training the employees on information security management can enable employees to know why security is important; however, lack of compliance in this context will not make this training effective at reducing security breaches. Various studies have focused on both security awareness and security training, but none has been able to solve the security issues that these organizations currently face.

We present a comprehensive information security management plan based on the NFC that ensures the transfer of knowledge regarding information security and potential threats to organization data assets. According to Hagen *et al.* (2008), increasing

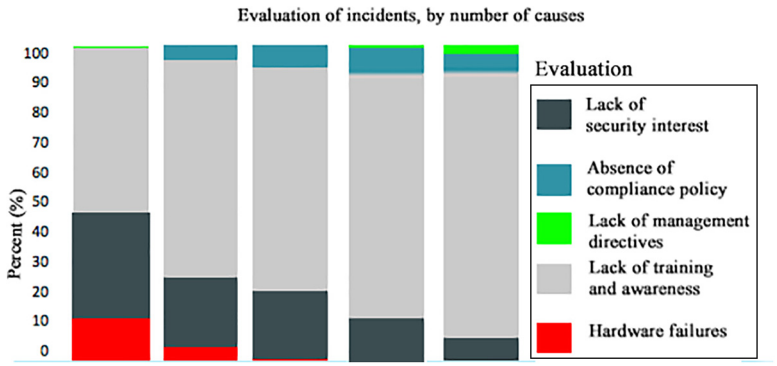

Figure 3.
Stacked chart

knowledge in security awareness is more effective at increasing policy compliance than other information security management measures. Albrechtsen and Hovden (2010) added that information security training directs and enhances employee behavior toward policy compliance. Siponen *et al.* (2014) argued that without employees complying with security policies, security awareness training will not be an adequate solution. It is therefore clear, that employees need to be trained on policy compliance. Ma *et al.* (2009) highlighted this, and further studied the essential role that compliance training has on information security management. Rubenstein and Francis (2008) studied how policy compliance can prevent access policy violations. Parsons *et al.* (2014) studied how compliance training has had various positive effects on numerous organizations.

5. Study limitations

We encountered limitations during this study. Some of the data collected were from organizations that were externally regulated. The FinTech external regulator initially disapproved the project due to risk management (i.e. not realizing finance and risk alignment benefits). The external regulators believed that the FinTech organization lacked the capability needed to execute compliance policies successfully in the real world. It was a tedious task to acquire authorization from these regulators for surveys and data collection in the area of information security. In any case, the data we collected were enhanced with a greater sample size by including the other organizations.

Owing to information security management unawareness of employees, some of the staff members at the bank resisted the survey (Joshi, 2005). These staff members did not comprehend the importance of our research because of changing and new challenges in IT security risk that have arisen in recent years (Kim and Pan, 2006). This could have been solved via another workshop to explain the reason behind this survey.

Another critical problem in our study came from the failure to control for duplicated responses by employees that took part in the online survey. Such issues could be mitigated in the future by ensuring that each person enters his or her email address as well as recording the employee MAC or IP addresses. With this approach, we could have identified employees with multiple responses or prevent duplication from occurring.

6. Compliance guidelines and decision-making

Globalization and emerging markets have increased the complexity of information sharing. This complexity has also increased security risks, which has become a large issue in many organizations' information security management. Recent studies have depicted how organizations are deploying technology solutions and other strategies to eliminate these risks. From our findings, none of these approaches yielded positive results, while some organizations are not even aware of the importance of data security. On the other hand, modern organizations rely on information to make decisions that are used to carry out organizational activities. In this section, we answer *RQ3* by proposing a principle that will enhance the development and implementation of information security management policies in an organization. This will also help eliminate various issues with respect to information security management and help to enhance productivity in an organization.

There are numerous ISRM standards but not limited to the ISO27000 series (ISO27001, ISO27002), SAS70, SOC2 and PCI DSS. In this work, we propose a new principle called the NFC that can be configured to meet individual organizational needs. The proposed principle will indicate the necessities for the implementation of operational and information security enhancements. It also puts more emphasis on the measurement and evaluation of

organization ISMI performance and outsourcing. We can relate our principle to the ISO27001:2013 and supersedes the ISO27001:2005 (Bresin, 2014; Mackie, 2013; Herbert, 2014). The NFC prescribes an administration model to empower organizations in planning and vigilance in:

- How information systems are understood and how those systems identify critical events.
- What security counter measures have been deployed for information protection.
- How valuable data assets have been identified and how they are protected.
- What process the organization has used to identify applicable legal, regulatory, and other obligations.

Specific guidelines are not provided by NFC; however, it enables organizations to manage information security in an organized way by providing a principle to enhance the management of security measures, potential risks, uncertainty, unpredictable incidents and compliance.

At this phase of our study, we cannot conclude that the standard ISO27001 and ISO 27002 will fit organizations that are eager to identify or detect potential risk. This is due to the fact that, using the ISO27001 standard checklist would be excessively specific and would decrease flexibility in processing information security management tasks in this study. The ISO27001 is presumably the most well-known of all the ISO standards owing to the essential tools it provides to enhance security of information. For example, one of the greatest myths about ISO27001 is that it is centered around IT; however, we cannot agree to this because IT cannot secure information alone. In the context of security, human resource management, physical security, legal protection, organizational issues and how they are interrelated are required to secure information as in the context of the NFC principle. Therefore, this study proposes the NFC to support the general procedure of information security management by taking not only IT into consideration but also human resource management, physical security, legal protection, organizational issues and how they are all interrelated to secure information. We propose that an organization following the NFC principle or framework can effectively measure their risk and deploy robust security measures based on their needs. As in the case of the ISO27001, an organization can select from the 114 controls, which will provide instruction on what an organization needs to accomplish, yet does not provide the information on how this should be accomplished. Moreover, these 114 controls can be misleading, as the implementation guidance prescribes various actual controls in the details. This is the purpose of the ISO27002, which provides more details on implementation. However, an organization cannot use only the ISO27002 because it does not provide any information about which controls should be implemented, how to measure them, or how to assign them to the right people. The ISO27002 is an advisory document and not a formal specification like the ISO27001.

6.1 Our proposed principle

The NFC principle is defined as a strategic diagram that shows the potential factors that prevent the successful development and implementation of an information security management strategy. This principle is mainly a process used to design, to identify and to mitigate potential factors causing an overall hindrance in security-related policy compliance within an organization. Every potential factor that generates any hindrance is a cause of variation that should be addressed.

In Table IV, we defined several incidents that hinder information security management in organizations through our data collection and findings. In this section, we propose a principle that enhances the interrelationship between technology and human factors in an organization for the deployment of successful information security management (Werlinger *et al.*, 2009; Abawajy, 2014; Arachchilage and Love, 2014; Kritzinger and von Solms, 2010). In this work, we derived five causes and hindrances after analyzing the data using SPSS, as depicted in Figures 2 and 3. These causes and hindrances are:

- lack of security interest;
- lack of security awareness training;
- lack of management directives;
- absence of compliance policy; and
- hardware failures.

We then propose the NFC principle to solve those issues, rather than using any general standard guidelines that has been proposed in the literature thus far. The NFC principle should enable us to come up with a moderate procedure for successful development and implementation of an information security management strategy based on organizational needs. In this work, the comprehensive nature of the NFC principle should enable us to enhance the interrelationship of technology and human factors highlighted above, and to close the knowledge gaps that still exist for the deployment of a successful information security management strategy. Figure 4 introduces our NFC principle with the five causes and hindrances we derived from the SPSS analysis. These causes and hindrances are grouped into attributes and categorized as potential key factors. The key factors are held together by the central point of the NFC that consists of all the prerequisites that are essentially needed for the development and implementation of the ISRM. In our work, we developed a conceptual framework, illustrated in Figure 1, using the SBT to explain how employees comply with information security policies. Here, the variables that were not observed, such as job contentment, employee devotion, work experience, socialization, creativity, knowledge sharing via SNS and commitment are considered as our latent variables as shown in Figure 6. Other prerequisites include, but are not limited to, collaboration, cultural, confidentiality, integrity, moral agreements, certified leaders and communication. Therefore, our prerequisites (including our latent variables) are the blueprint in the development and implementation of ISRM in the concept of the NFC. These prerequisites are the shaft on which the NFC oscillates. The key factors are joined together by a dynamic compliance process standard that involves:

- awareness of the compliance regulation;
- controlling integration; and
- closing gaps.

Both the key factors and the central point *prerequisites* are enclosed in the control integration and close gaps dynamic. The rotation starts at the 9 o'clock, 12 o'clock, 3 o'clock, 5 o'clock and 7 o'clock positions. The entire process repeats itself after each life cycle during a time span, and it needs to be adjusted frequently.

6.1.1 Why the nine-five-circle. The NFC is a portable, simple and improved starting point when compared to other principles and frameworks, such as the standard ISO27001 and ISO27002, which come with different distinct features. For example, the ISO 27002 does not make a distinction between controls applicable to a particular organization and those which are not, while the ISO27001 prescribes a risk assessment

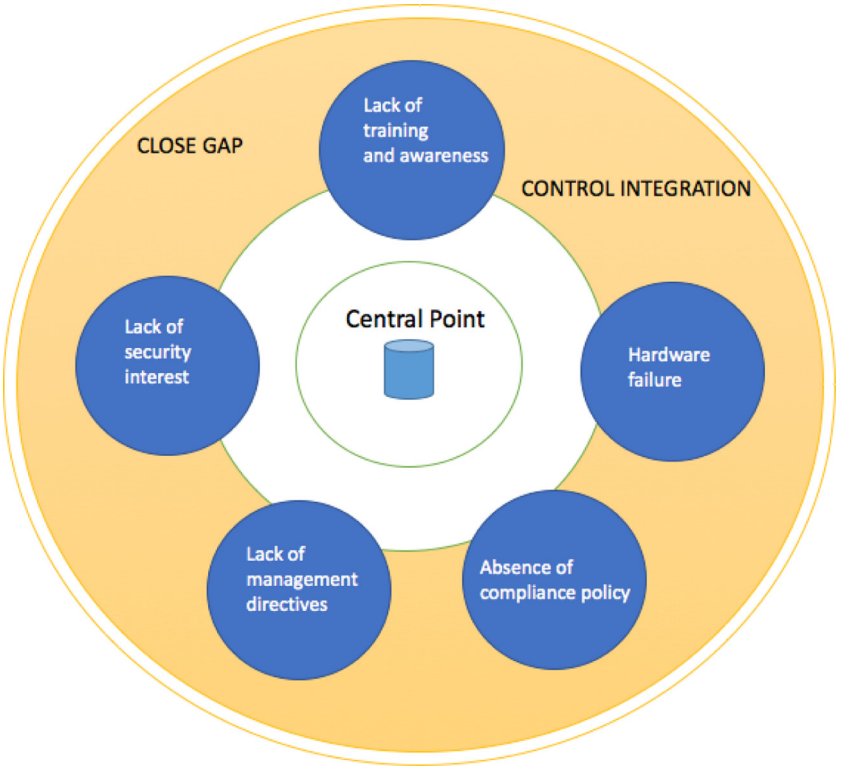

Figure 4.
NFC principle with SPSS evaluation results

to be performed to identify for each control whether it is required to decrease the risks, and if it is, to what extent it should be applied. Here, we can see that both standards are different, but lack the positive attributes of both tools when combined. This is where the NFC comes in, taking usability in to consideration and using a single standard that makes it simple and portable for practical use. The NFC also focuses on design, identification and mitigation of potential factors causing an overall hindrance to security-related policy compliance within an organization. Every potential factor that generates any hindrance is a cause of variation that should be addressed in the NFC context, unlike the ISO27000 where standards are designed for certain focus. For example, the ISO27001 is for building an information security foundation in an organization, the ISO27002 is for the control implementation, and the ISO27005 is for carrying out risk assessment and risk treatment. The NFC combines all these with a dynamic compliance process standard that involves:

- awareness of the compliance regulation;
- controlling integration; and
- closing gaps.

Both the key factors and the central point prerequisites are enclosed in the control integration and close gaps dynamic. The NFC also enhances the interrelationship between technology and human factors and these are not seen in the context of ISO27000. In this paper, Figure 4

introduces our NFC principle with the five causes and hindrances we derived from the SPSS analysis.

6.2 Applying the nine-five-circle in this study

As shown in Figure 4 and Table V, the five key factors (lack of security interest, lack of information security training and awareness, lack of management directives, absence of compliance policy and hardware failures) are all joined with the central point. Security training and awareness have been separated on our SPSS results in Figures 2 and 3 because employees might be aware of security issues but without training, they might make costly errors in regard to information security. Therefore, security awareness training should be implemented to reduce or eliminate costly errors among employees in the context of information security. Here, the security awareness training includes, but is not limited to, workshop training sessions, security programs, security awareness websites or emailed information. All these procedures are capable of enhancing employee understanding of organizational security policy, process and best practices.

Starting from the 9 o'clock position, we have placed our first key, lack of security interest, followed by lack of security awareness training and awareness, lack of management directives, absence of compliance policy and hardware failures. In the NFC, it is essential to address the SPSS analysis results efficiently based on how critical each key factor is assessed, and how they affect other key factors by taking the needs of the organization into account within each life cycle.

To ensure that an organization's compliance is established and followed, the NFC principle provides a dynamic compliance process. Here, organizations need to consider that compliance is not a product, but a continuous process that needs to be adjusted frequently to meet administrative constraints and needs. Frequent reassessment will enhance organization activities – especially in the context of security issues, due to the rapid advancement of Information Technology (IT) and increases in its associated risks. Therefore, our proposed principle comes with a dynamic compliance process standard that involves:

- awareness of the compliance regulation;
- controlling integration; and
- closing gaps.

6.2.1 Awareness of compliance regulation. The first step in NFC is to identify the type of governance that will fit in the business domain and then to list any related controls. In this work, we address the five security issues that face the three organizations. As discussed earlier on, the NFC can be scoped to meet individual organization needs; however, for the sake of time, we will address all the three case studies as one example. The first phase in the NFC principle is to identify metrics that consist of operation, organizing, budgeting, time-frame, managing and reporting procedures. These will enable the management board to use

Table V.
SPSS Evaluation table

SPSS Results	Fintech (%)	Bank (%)	Automobile (%)
Lack of security interest	10	2	1
Lack of security awareness training	30	21	20
Absence of compliance policy;	52	66	65
Lack of management directives	59	82	80
Hardware failures	55	1	2

that information effectively in the business units, in accordance with regulations and to provide strategic outcomes. From our analysis and findings, the proposed metric consists of the following:

- *End to end*: All members should understand how their efforts contribute to the results. All members need to have a broad understanding of input and output procedures and the effectiveness of the drivers.
- *Balance*: Here we propose that organizations should incorporate the measurement of their viability and productivity. The utilization of the scorecards will enable organizations to quantify progression status as well as the adequacy of educational programs, occasionally on an alternate cadence than the execution reporting.

Lack of security concern is driven by lack of security awareness training initiatives, and both are due to the absence of policy compliance which is due to lack of management directives and collaboration. Hardware failure could also be seen in this study as being caused by both human and technology factors. Hence it is clear from our SPSS analysis that these factors are interrelated and need to be addressed efficiently for the successful development of ISRM. Furthermore, each of our findings is a critical factor that needs to be addressed efficiently.

6.2.1.1 Lack of security interest, lack of security awareness training and hardware. In this study, the three key factors (variables) are related and need to be address first. Here, the organization should develop a formal security awareness team that will be responsible for the development and implementation of a security awareness program. It is also vital that during this phase, each organization has a skilled team, either internally or externally, to maintain this program and all associated hardware. In the NFC, the process of getting the right people is termed as assembling the security awareness team. The next step in this phase of the NFC is to determine roles for the security awareness program. This is vital in the NFC principle since it enables each organization to train its personnel based on their job functions. This training is extendable, based on subject and area of expertise. Other areas can be joined or removed during this process. The goal here is to develop various levels of in-depth training to enable the organizations to convey the correct training to the perfect individuals at the right time. This approach will enhance each organization's security compliance and the consistency of NFC. Thus, NFC can be applied as a singular approach, or holistic approach, or tiered approach, depending on the organization's prerequisites. One critical point in the phase of selecting the right people in the NFC is to group individuals by their job functions. In this work, we have identified three roles, such as "all employees", "top personnel" and the "management team". The next phase of the NFC is to apply a tool that can enhance ISRM. It is vital that the proposed programs and hardware are solid for all the groups. In the context of the group "all employees" the proposed program should aim to enable this group to recognize security threats and embrace security as an enhancement tool which is aimed to increase their security interests, and for them to feel comfortable to report those employees creating security risks. The "top personnel" group should concentrate on the employee's commitment to follow security protocols for accessing delicate information and perceive the related dangers if access is abused. The "management" group should comprehend the organization's approach to security and security requirements well enough to examine and strengthen the message to all personnel, encourage personnel security awareness, and perceive and address security-related issues when they arise. As a recommended tool, a "bolt-on tool" can be adopted in this work to enable leaders to have a picture of service-level agreement (SLA) performances and have an in-depth view to analyze main causes. The next phase is to develop a fundamental security awareness level for all

personnel based on the security awareness program. We recommend security awareness to be transferred either via emails, posters and computer-based training without any restriction in any form. Here we recommend that such security programs should be delivered with regards to the organization culture. This step in the NFC is seen as the development of minimum security awareness. We depict the depth of security awareness training as seen in Figure 5 and illustrate how this stage of the NFC can increase the depth of security awareness and enhance security interest through solid security awareness programs. This process needs to be repeated frequently because in time, the interest of these top managers and other workers deteriorates and causes such projects also to deteriorate. Furthermore, a classification policy might work during a period of time, but when technology changes, both organizations people change. This means old policies will be made obsolete and one cannot comply with an obsolete document.

Up to this stage in our paper, it is clear that the NFC supersedes both the ISO27001 and the ISO27002 because both standards need to be combined to achieve what the NFC can accomplish. The ISO27002 provides more details on implementation, but one cannot use it alone as stated in section 6 in this paper because it does not provide any information on which controls need to be implemented, how to measure them and how to assign them to the right people. The combination of the two ISO27000 standards can increase the complexity in the ISRM for companies that are eager to enhance security in a flexible environment. Some organizations can even abuse the ISO27001 adaptability and concentrate just on the minimum controls with a specific end goal to pass the certification. However, this abuse of the certification process is beyond the scope of this study.

As discussed earlier on, the NFC can be scoped to match an individual organization's needs. Thus, the training that is held during this phase can be further broken down to map each organizational requirement. For instance, because the percentage of security interest is higher in the FinTech sector than the rest, the FinTech organization could decide on which roles may not need security training in this phase. This enables each organization to determine the content of training that is needed. Because technological and human factors are interrelated and work together in the NFC principle, a communication channel is needed to deliver security awareness throughout the organization. This is seen as a suitable manner to deliver significant resources to the right people that fit the organization's interests and culture. As discussed earlier, this form of delivery is not restricted to any communication gateways (hardware and software), but rather, what fits the organization. This flexibility of delivery enhances how employees receive information. However, we recommend that each

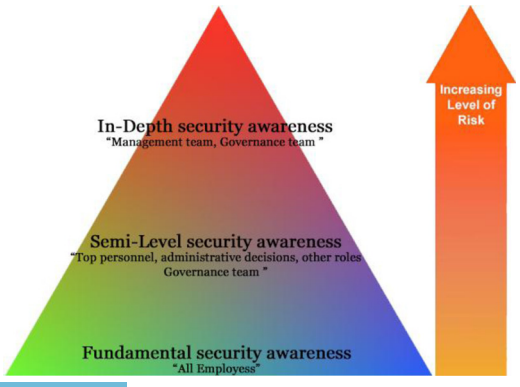

Figure 5.
Increasing security interest through a depth security awareness training program

organization limit its delivery channels so as to enable individuals to remember how information is delivered to them. The communication channel should be made clear to all newly hired personnel and be updated for existing personnel. It is also important in the NFC that both the training content and the communication channel used correspond to each group receiving that particular training. As shown in Figure 6, security awareness needs to be consolidated with other prerequisites located at the central point of the NFC, such as collaboration, culture, confidentiality, integrity, moral agreements, certified skilled leaders, communication and commitment. Furthermore, because employees react to change in a critical manner, these prerequisites enhance the transparency of the proposed security program and any change that might occur. To guarantee that each group is informed at any point in time when there is a need to occupy a security awareness position, we recommend the organizations add this procedure in their recruiting and re-classifications so that general security awareness training objectives will be actively encouraged without dependence on an individual authoritative unit. Collaboration is characterized as working together with a specific end goal to accomplish an objective. Collaboration comes with participation, commitment, and teamwork. It is seen as a procedure in which at least two people, groups or organizations, cooperate to achieve shared objectives. The collaboration in information security management enables experts to gather, coordinate, group, disseminate, and share information security know-how with other experts and co-workers. Ahmad *et al.* (2012) highlighted on the impact of collaboration and communication in the context of information security management. According to Feledi *et al.* (2013), collaboration involves documentation and scheduling events and can be seen as proposing or submitting, reviewing, commenting and improving knowledge. The organization should also have the right tools to monitor and detect staff activities. For example, accessing violations such as malicious and/or viral software, monitoring unauthorized websites, a tool to monitor and approve the downloading of internet programs and email attachments. Furthermore, other

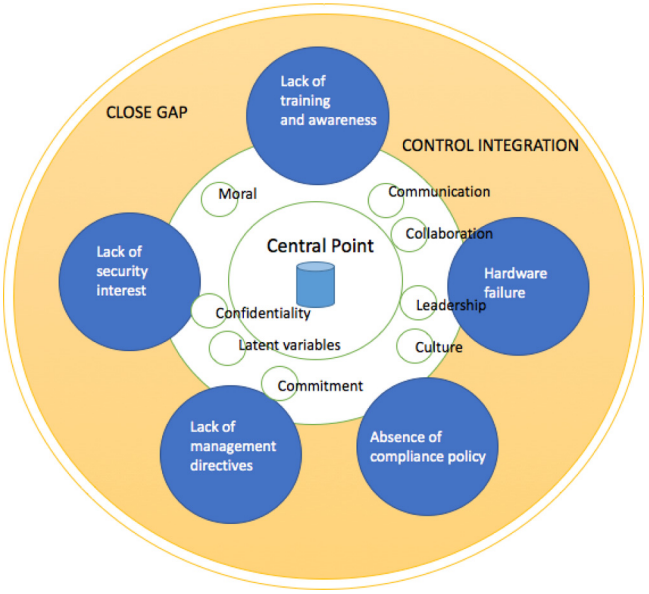

Figure 6.
Communication channels for security awareness training program

tools to enable productive procedures need to be considered. An example is to enable the organization to assemble, and enhance awareness in performance.

6.2.1.2 Lack of management directives. Management leadership and support activity are considered the most critical factors for the security awareness program, and we urge organizations to encourage all personnel to participate and abide by security awareness principles during the life cycle of the NFC. The compliance project should be assigned to a certified leader who has essential abilities. There are several certifications that organizations could look for when deciding on a competent leader such as the CISM, CISSP Lead ISO27001 certificate or the CISA.Here, governing bodies should challenge and question standards at any time, and a responsibility assessment metric should be established to enable an operational team to establish joint decisions frequently. A suitable security awareness method should be established to enforce the security awareness program on the employees. Security metrics should also be added where appropriate, to measure both management and staff performance. The governance team should be proactive and react to any situation by monitoring and measuring progress with deliveries. This is vital for organizations that consolidate procedures and policy and operate globally. All resolved obstructions should be surveyed by the leaders and they should subsequently adjust various procedure plans into a single cognizant fund plan. Mandates should be established to address the punishment of culprits, security-related guidelines and lack of security compliance regulations. We recommend organizations renew the entire process frequently, as compliance is not a product, but a continuous process that needs to be adjusted frequently to meet administrative constraints and needs. Frequent assessment will enhance organization activities, especially, in the context of security issues due to the rapid speed of IT and its associated risks.

6.2.2 Control integration. The integration phase is where both the control activities and governance targets are defined and institutionalized. Here, the extent to which all the critical factors and latent factors interrelate as well as their main effects are measured. The NFC has the ability to represent unobserved factors or variables in these relationships and account for measurement error in the compliance process. To acquire dependable and predictable result of ISRM development and implementation in the NFC principle, the whole procedure should be controlled and measured persistently. To archive that, the complexities of the procedure in terms of different latent variables and interrelated variables need to be separated, comprehended and re-integrated into a point of view to empower complete understanding of the process. The critical issues affecting developing and implementing ISRM need to be identified understood and controlled during the integration. Here procedures such as organizational risk, control targets, testing process, hardware and software tools are all encompassed. This phase enables auditing, identification of non-compliant components and definition of the sources of relationships in governance based on organization risk (Reding *et al.*, 2013). At this level, we can see that the NFC is not prescriptive, but it provides organizations with information and tools to make decisions based on their needs – what needs to be done and how to accomplish it. It is also a principle that enables organizations to decide on appropriate protections and to take measurements.

6.2.3 Closing gaps. The absence of compliance in an organization is an indication of poor security measures, causing security risks. Organizations that lack compliance should make sure that decision-making includes mechanisms that will enable them to make dynamic decisions and select mitigating strategies. Lack of information security policy compliance can trigger defective security systems and endanger the business domain. Organizations need to weigh the costs and the risks during mitigation. An advisory board should be set that will advise the IT team regarding the controls needed. Hence, our proposed principle

supports our hypothesis in this study that technology and human factors are interrelated and work together for the successful deployment and implementation of information security management in an organization.

7. Implications for research, practice and/or society

Our main objective in this study was to address the lack of research evidence on what mobilizes and influences information security management development and implementation. We have fulfilled this objective by surveying, collecting and analyzing data and giving an account of the attributes that hinder information security management. Accordingly, a major practical contribution of the present research is the empirical data it provides that enables us to have a bigger picture and precise information about the real issues that cause information security management shortcomings. Assessing an organization's valuable information will highlight the activities of the CEO, IT managers, top-level personnel, policymakers, consultants and trainers to design initiatives, apparatuses and actions in view of what strategy needs to be adopted to implement information security management, what they need to do and where they are now in terms of security-related issues, as opposed to what they think they ought to do. For instance, policymakers could observe that more often than not, top personnel will not read policies specifically and are probably going to pass them to their immediate staff members. This will enable them to reformat their policies accordingly. We believe that, various organizations could derive comparative implications through some of our findings.

Additionally, we believe that our research is especially convenient for several organizations to become more open to challenge and scrutiny. In the event that an organization is having inaccurate idea of their business domain security issues, they may be driven to the idea of applying our NFC principle. This might enable them to develop audit trails of proof in the context of their information systems before making decisions, as opposed to applying standard guidelines which may result in excluding the essential attributes rather than providing them with more prominence attributes, such as, how the employees react to policies, collaboration, communication and commitment. For example, the ISO27001 standard comes with the importance of statement of applicability (SoA), while the ISO9001 comes with the central document that characterizes how an organization should execute a large part of their information security. This documentation is underrated in the context of NFC because most organizations implementing the ISO27001 invest more time writing this document than they expected. While this type of information could constitute a critical source of knowledge, the risk is that it is disregarded and not valued enough of the fact that it does not fit the customary formal idea of what constitutes information security management development and have no use in real life.

Furthermore, another essential implication of our study derives from our findings. Our findings indicate a particular set of information sources, capacities, decision strategies, staff and organization attitudes toward security-related issues that can help to close the gap between technology and humans in the context of information security management. Although analyzing the data we collected with a view to distinguishing and systematizing employee skills, behavior, collaboration, commitment, security interest, skilled management directives, technically and frequent security-related issues training goes beyond the remit of this study. We have made contacts with other major firms to explore how this can be accomplished cooperatively in the near future.

Our study is focused on how to nurture and enhance organizations to develop and implement a rigid security policy compliance. Our discoveries recommend in actuality that using flexible tools that can be scoped to meet individual organizational needs have positive effects in the implementation of information security management policies within an organization. Accordingly, our research proposes that organizations should forsake the oversimplified generalized guidelines that neglect the verification of the difference in information security requirements in various organizations. Instead, they should focus on the issue of how to sustain and enhance their organization's compliance through a dynamic compliance process that involves: awareness of the compliance regulation, controlling integration and closing gaps.

In this sense, despite the fact that our study has limitations concerning the development of a diagnostic tool, it is obviously the main procedure for the measurements of a framework to assess information security compliance policies in the organizations we surveyed. Furthermore, such measurements, which we derived from the SPSS in Figures 2 and 3 subsequently from our NFC in Figure 6 above, recommend that these organizations should reflects on the following questions:

Q1. What sort of a leadership should be in charge of the Information security management policies?

Q2. What is the nature of their organization and current information management?

Q3. What is the nature of their organization security policies at present (e.g. commitment, collaboration, employees' knowledge sharing, humans, technology and how all these factors interrelate and work together?

Q4. What individual information security principles do they have a tendency to adopt (for example; a principle that can enhance both internal and external environment of the organization information security policies as well as policy compliance operation and strategic)?

Q5. They also have to assess if they do have the right framework set up (both humans and technology, e.g. employees commitment, collaboration and skilled leadership) to permit them to establish a rigid policy compliance.

The principle we have graphically demonstrated in Figure 6 can be flexible adopted into any organization and can facilitate vital procedures of developing and implementing rigid information security management policies on the demand of each company over time. The NFC principle likewise recommends that organizations ought to abandon the possibility of general standard ISRM tools that refuse to address the issue of information security management knowledge mobilization in their business domain and focus on tools that can be adjusted to meet the demand of their organization, which in turn, will provide individual and sensitive approaches and solutions in the context of information security management.

7.1 Implications for future research

Our study was based on exploratory and interpretive nature and raises various opportunities for future research, both regarding hypothesis development and idea validation. More research will in reality be important to refine and advance expounds our discoveries. We do believe that we have generated new findings and useful factors due to the in-depth sampling we obtained from the three organizations we surveyed. However, very little can be said of the nature of data that will be derived from a larger population of bigger

firms. Thus, our study could in this manner be extended to analyze a bigger set of statistical data. Furthermore, other research can be carried out to refine and validate our concepts and constructs based on our five key factors derived from the SPSS analyzer. The principle we proposed in this study can also be used to create various hypotheses for future empirical testing using a more extensive sample and quantitative research strategies.

Finally, as this study limitation is discussed on Section 8, it is therefore essential for further work to be carried out so as to analyze and examine the practices of information security management policies compliance at major firms to explore how this can be accomplished cooperatively in the near future as opposed to the three organizations we surveyed in this study. Additionally, research can in this manner highlight how policy compliance can be conducted across boundaries, such as policy compliance circulation, sharing and exchange within a firm with several branches in nationwide or across different countries.

8. Conclusion and limitations

Information breaches could be successfully mitigated if security policy compliance is taken seriously in an organization (Ifinedo and Olsen, 2014; Vance *et al.*, 2013). The arguments of the information security literature and the results from our survey on information security policy compliance via leadership decisions, employee commitment, collaboration and communication have been the main focus of this work. Certain variables such as knowledge sharing, socialization, work experience, skilled leadership management and intervention can direct employee behaviors toward compliance with information security policies and processes. Sharing information knowledge in an organization enhances both security awareness and the essence of organization security policy compliance and their processes. Leaders in the organization should encourage the importance of knowledge sharing via information security management training, and motivate employees through intrinsic and extrinsic manners for information security risk abatement. Lai and Chen (2014) concur that organization leaders can reward their staff via extrinsic motivation. There is no reward associated with intrinsic motivation because this type of motivation is based on the interest of the employees. Shibchurn and Yan (2015) also added that intrinsic motivations are influenced via satisfaction, and that pleasure is influenced via curiosity.

Based on the results from our three surveys and findings, we have proposed a principle of information security compliance practices based on our proposed NFC principle that enhances information security management by identifying human conduct and IT security-related issues regarding the aspect of information security management. Furthermore, the NFC principle has enabled us to close the gap between technology and humans in this study by proving that the factors in our finding are interrelated and work together, rather than on their own. Therefore, our work presented information security standards and best practices that could be used in most business domains. Additionally, we examined special components and factors that organizations need to be considered when making a decision based on standards.

Despite the fact that our methodology does not convey a new measure, it contributes to a more reliable, good practice of information security measures that help to educate leaders and secure the participation of employees in the context of information security management. The principle quality of our guideline is employees' behavior complexity and related activities. We determined how information security collaboration enhances employee's conduct in the context of complying with policies. Furthermore, we found

collaboration as a cooperative approach where different groups of employees work jointly towards the same goal. Leaders can encourage this collaboration via authoritative support and encouragement based on how these leaders reward employees and on how employee well-being matters to the organization (Shropshire *et al.*, 2015).

This study proposes that leaders can encourage security compliance effectiveness by urging employees to share knowledge and collaborate in the context of information security. Sufficient information security management training also has an effect on employee compliance with policies by providing effective information security training courses, frequent workshops, security awareness events, notices, monthly mass-mails, webpages and frequent meetings. Furthermore, outside events can also enhance information security training procedure in the context of policy compliance process.

Security awareness training employees in the context of information security management in the right approach sheds light on information security awareness and adds to the key factors to the success of information security management in an organization. Another key factor in this research was selecting the right method to support policy compliance implementation. The last key factor is related to the effect of leadership on employee behavior towards policy compliance. Information security "know-how" and "know-why" creates topical mastery for securing information resources in an organization. This engenders a profound understanding of the problems that are associated with poor information security management and throws more lights on policy compliance.

Additionally, we encourage organizations to adopt more encompassing procedures to deal with information security management such as: the interest of leader management. HR management, implementation and execution of information security policy, information security training, awakening employee security awareness and group-based decision-making.

We cannot conclude that information security awareness will keep data safe without information security training. Moreover, information security training can enable employees to know why security is important, but this alone will not solve the issues in information security management. This indicates that, without compliance being rigidly established and directed by organization leaders, security-awareness training will not be effective on how humans see information security. Therefore, our work proposes an organization to consider what alternatives there are to enable them to internally and externally communicate security issues with employees. Also, leaders should be trained to manage and direct employees to comply with any policies that governs the organization. We also propose that organizations facing budget constraints and/or time limitations to apply the NFC principle.

References

Abawajy, J. (2014), "User preference of cyber security awareness delivery methods", *Behaviour & Information Technology*, Vol. 33 No. 3, pp. 237-248, doi: 10.1080/0144929X.2012.708787.

Ahmad, A., Hadgkiss, J. and Ruighaver, A.B. (2012), "Incident response teams – challenges in supporting the organisational security function", *Computers & Security*, Vol. 31 No. 5, pp. 643-652, doi: 10.1016/j.cose.2012.04.001.

Ahmad, A., Maynard, S.B. and Park, S. (2012), "Information security strategies: towards an organizational multi-strategy perspective", *Intelligent Manufacturing*, Vol. 25 No. 2, pp. 357-370, available at: http://link.springer.com/10.1007/s10845-012-0683-0

Albrechtsen, E. and Hovden, J. (2010), "Improving information security awareness and behaviour through dialogue, participation and collective reflection: an intervention study", *Computers & Security*, Vol. 29 No. 4, pp. 432-445.

Arachchilage, N.A.G. and Love, S. (2014), "Security awareness of computer users: a phishing threat avoidance perspective", *Computers in Human Behavior*, Vol. 38, pp. 304-312, doi: 10.1016/j.chb.2014.05.046.

Arce, I. (2003), "The weakest link revisited", *IEEE Security & Privacy Magazine*, Vol. 1 No. 2, pp. 72-76.

Baskerville, R. (1993), "Information systems security design methods: implications for information systems development", *Computing Surveys*, Vol. 25 No. 4, pp. 375-414.

Beccaria, C. (1963), *On Crime and Punishments*, Bobbs Merril, Indianapolis, IN.

Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A. and Boss, R.W. (2009), "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 151-164, available at: www.palgrave-journals.com/doifinder/10.1057/ejis.2009.8 (accessed 16 June 2016).

Breslin, P. (2014), *Security Updates: The Upcoming Revision of ISO/IEC 27001*, DNV Business Assurance, available at: http://enewsletter.ntu.edu.sg/itconnect/2011-03/Pages/ISO27001-ISM.aspx?AspxAutoDetectCookieSupport=1 (accessed 20 May 2016).

Cavusoglu, H., Cavusoglu, H., Son, J.-Y. and Benbasat, I. (2009), "Information security control resources in organizations: a multidimensional view and their key drivers", working paper, Sauder School of Business, University of British Columbia.

Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004a), "A model for evaluating IT security investments", *Communications of the ACM*, Vol. 47 No. 7, pp. 87-92.

Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004b), "The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers", *International Journal of Electronic Commerce*, Vol. 9 No. 1, pp. 69-104.

Chang, S.E. and Ho, C.B. (2006), "Organizational factors to the effectiveness of implementing information security management", *Industrial Management & Data Systems*, Vol. 106 No. 3, pp. 345-361, available at: www.emeraldinsight.com/10.1108/02635570610653498 (accessed 8 July 2016).

Chen, Y. and Hwang, K. (2006), "Collaborative detection and filtering of shrew DDoS attacks using spectral analysis", *Journal of Parallel and Distributed Computing*, Vol. 66 No. 9, pp. 1137-1151.

Chen, Y., Nazareth, D.L. and Wen, K.-W. (2010), "Research in information security: a literature review using a multidimensional framework", *Proceedings of the Thirty-Ninth Annual Western Decision Sciences Institute Conference (WDSI 2010), Lake Tahoe, NV*, pp. 3681-3687.

Compston, H. (2009), *Policy Networks and Policy Change: Putting Policy Network Theory to the Test*, Palgrave Macmillan, Basingstoke.

Cronan, T.P., Foltz, C.B. and Jones, T.W. (2006), "Piracy, computer crime, and information security misuse at the university", *Communications of the ACM*, Vol. 49 No. 6, pp. 84-90.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R. (2013), "Future directions for behavioral information security research", *Computers & Security*, Vol. 32, pp. 90-101, doi: 10.1016/j.cose.2012.09.010.

Da Veiga, A. and Martins, N. (2016), "Improving the information security culture through monitoring and implementation actions illustrated through a case study", *Computers & Security*, Vol. 49, pp. 162-176.

Dhillon, G. and Backhouse, J. (2001), "Current directions in information security research: toward socio-organizational perspectives", *Information Systems Journal*, Vol. 11 No. 2, pp. 127-153.

Feledi, D., Fenz, S. and Lechner, L. (2013), "Toward web-based information security knowledge sharing", *Information Security Technical Report*, Vol. 17 No. 4, pp. 199-209, doi: 10.1016/j.istr.2013.03.004.

Gaur, A. (2009), *Statistical Methods for Practice and Research*, SAGE.

Guo, K.H. (2013), "Security-related behavior in using information systems in the workplace: a review and synthesis", *Computers & Security*, Vol. 32 No. 1, pp. 242-251, available at: http://linkinghub.elsevier.com/retrieve/pii/S0167404812001666

Guo, K.H. and Yuan, Y. (2012), "The effects of multilevel sanctions on information security violations: a mediating model", *Information and Management*, Vol. 49 No. 6, pp. 320-326.

Hagen, J.M., Albrechtsen, E. and Hovden, J. (2008), "Implementation and effectiveness of organizational information security measures", *Information Management & Computer Security*, Vol. 16 No. 4, pp. 377-397.

Hair, J.F., Black, W.C., Babin, B.J. and Anderson, R.E. (Eds) (2010), *Multivariate Data Analysis*, Pearson.

Harrington, S.J. (1996), "The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions", *MIS Quarterly*, Vol. 20, pp. 257-278.

Harrison, K. and White, G. (2010), "An empirical study on the effectiveness of common security measures", *Proceedings of 43rd Hawaii International Conference Systems Science, Koloa, HI*, pp. 1-9, available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5428509 (accessed 24 June 2016).

Herath, T. and Rao, H.R. (2009a), "Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness", *Decision Support Systems*, Vol. 47 No. 2, pp. 154-165, available at: http://linkinghub.elsevier.com/retrieve/pii/S0167923609000530 (accessed 13 May 2016).

Herath, T. and Rao, H.G. (2009b), "Protection motivation and deterrence: a framework for security policy compliance in organisations", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 106-125.

Herbert, C. (2014), *More Changes Ahead*, ISO 27001: 2005 Information Security Management Standard, available at: www.isoqsltd.com/ahead-iso-270012005-information-security-management-standard/ (accessed 17 May 2016).

Hovav, A. and D'Arcy, J. (2012), "Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the U.S. and South Korea", *Information Management*, Vol. 49 No. 2, pp. 99-110.

Hsu, C.W. (2009), "Frame misalignment: interpreting the implementation of information systems security certification in an organization", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 140-150, available at: www.palgrave-journals.com/doifinder/10.1057/ejis.2009.7 (accessed 3 July 2016).

Hu, Q., Hart, P.J. and Cooke, D. (2007), "The role of external and internal influences on information systems security: a neo- institutional perspective", *Journal of Strategic Information Systems*, Vol. 16 No. 2, pp. 153-172, available at: http://linkinghub.elsevier.com/retrieve/pii/S0963868707000212

Ifinedo, P. (2012), "Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory", *Computers & Security*, Vol. 31 No. 1, pp. 83-95, doi: 10.1016/j.cose.2011.10.007.

Ifinedo, P. and Olsen, D. (2014), "An empirical research on the impacts of organisational decisions' locus, tasks structure rules, knowledge, and IT function's value on ERP system success", *International Journal of Production Research*, Vol. 53 No. 8, doi: 10.1080/00207543.2014.991047. available at: http://faculty.cbu.ca/pifinedo/IJPRDR.pdf

Jaeger, J. (2013), "Human error, not hackers, cause most data breaches", *Compliance Week*, Vol. 10 No. 110, pp. 56-57.

Jansson, K. and von Solms, R. (2013), "Phishing for phishing awareness", *Behaviour & Information Technology*, Vol. 32 No. 6, pp. 584-593.

Joshi, K. (2005), "Understanding user resistance and acceptance during the implementation of an order management system: a case study using the equity implementation model", *Journal of Information Technology Case and Application Research*, Vol. 7 No. 1, pp. 6-20.

Kankan-Halli, A., Teo, H.-H., Tan, B.C. and Wei, K.-K. (2003), "An integrative study of information systems security effectiveness", *International Journal of Information Management*, Vol. 23 No. 2, pp. 139-154.

Kim, H.W. and Pan, S.L. (2006), "Towards a process model of information systems implementation: the case of customer relationship management (CRM)", *ACM Sigmis Database*, Vol. 37 No. 1, pp. 59-76.

Kotulic, A. and Guynes-Clark, J. (2004), "Why there aren't more information security research studies", *Information and Management*, Vol. 41 No. 1, pp. 597-607.

Kritzinger, E. and von Solms, S.H. (2010), "Cyber security for home users: a new way of protection through awareness enforcement", *Computers & Security*, Vol. 29 No. 8, pp. 840-847, doi: 10.1016/j.cose.2010.08.001.

Lai, H.M. and Chen, T.T. (2014), "Knowledge sharing in interest online communities: a comparison of posters and lurkers", *Computers in Human Behavior*, Vol. 35 No. 6, pp. 295-306.

Lee, J. and Lee, Y. (2002), "A holistic model of computer abuse within organizations", *Information Management & Computer Security*, Vol. 10 Nos 2/3, pp. 57-63.

Lee, Y. and Kozar, K.A. (2008), "An empirical investigation of anti-spyware software adoption: a multitheoretical perspective", *Information Management*, Vol. 45 No. 2, pp. 109-119.

Li, H., Zhang, J. and Sarathy, R. (2010), "Understanding compliance with internet use policy from the perspective of rational choice theory", *Decision Support Systems*, Vol. 48 No. 4, pp. 635-645, doi: 10.1016/j.dss.2009.12.005.

Li, J., Li, N., Wang, X.F. and Yu, T. (2009), "Denial of service li attacks and defences in decentralised trust management", *International Journal of Information Security*, Vol. 8 No. 2, pp. 89.

Lim, V.K.G. and Teo, T.S.H. (2005), "Prevalence, perceived seriousness, justification and regulation of cyberloafing in Singapore: an exploratory study", *Information & Management*, Vol. 42 No. 8, pp. 1081-1093.

Loster, P.C. (2005), "Managing e-business risk to mitigate loss", *Financial Executive*, Vol. 21 No. 5, pp. 43-45.

McFadzean, E., Ezingeard, J.-N. and Birchall, D. (2006), "Anchoring information security governance research: sociological groundings and future directions", *International Journal of Information Security*, Vol. 2 No. 3, pp. 3-48.

Ma, Q., Schmidt, M.B. and Pearson, J.M. (2009), "An integrated framework for information security management", *Review of Business*, Vol. 30 No. 1, pp. 58-69.

Mackie, R. (2013), *ISO 27001:2013 – Understanding the New Standard*, The Pragmatic Auditor (accessed 27 June 2016).

Mirkovic, J. and Reiher, P. (2005), "D-WARD: a source-end defense against flooding denial-of-service attacks", *IEEE Transactions on Dependable and Secure Computing*, Vol. 2 No. 3, pp. 216-232.

Pahnila, S., Siponen, M. and Mahmood, A. (2007), "Employees' behavior towards is security policy compliance", *Proceedings of the 40th Hawaii International Conference on System Sciences, Los Alamitos, CA*, IEEE Computer Society Press, pp. 156-166.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014), "Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)", *Computers & Security*, Vol. 42, pp. 165-176.

PricewaterhouseCoopers (2008), "Employee behaviour key to improving information security, new survey finds", 23 June, available at: www.ukmediacentre.pwc.com/content/detail.aspx?releaseid=2672&newsareaid=2

Puhakainen, P. and Siponen, M. (2010), "Improving employees' compliance through information systems security training: an action research study", *MIS Quarterly*, Vol. 34 No. 4, pp. 757-778.

Reding, K.F., Sobel, P.J., Anderson, U.L., Head, M.J., Ramamoorti, S., Salamasick, M. and Riddle, C. (2013), *Internal Auditing: Assurance & Advisory Services*, The IIA Research Foundation.

Richardson, R. (2011), *15th Annual 2010/2011 Computer Crime and Security Survey*, Computer Security Institute, New York, NY.

Rubenstein, S. and Francis, T. (2008), "Are your medical records at risk?", *Wall Street Journal*, Vol. 251 No. 100, pp. D1-D2.

Safa, N.S. and Ismail, M.A. (2013), "A customer loyalty formation model in electronic commerce", *Economic Modelling*, Vol. 35, pp. 559-564, doi: 10.1016/j.econmod.2013.08.011.d.

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A. and Herawan, T. (2015), "Information security conscious care behaviour formation in organizations", *Computers & Security*, Vol. 53, pp. 65-78, doi: 10.1016/j.cose.2015.05.012.

Schultz, E.E., Proctor, R.W., Lien, M.-C. and Salvendy, G. (2001), "Usability and security an appraisal of usability issues in information security methods", *Computers & Security*, Vol. 20 No. 7, pp. 620-634.

Schumacker, R.E. and Lomax, R.G. (2010), *A Beginner's Guide to Structural Equation Modeling*, 3rd ed., Taylor & Francis Group, New York, NY.

Seo, D., Lee, H. and Perrig, A. (2013), "APFS: adaptive probabilistic filter scheduling against distributed denial-of-service attacks", *Computers & Security*, Vol. 39, pp. 366-385.

Shibchurn, J. and Yan, X. (2015), "Information disclosure on social networking sites: an intrinsic-extrinsic motivation perspective", *Computers in Human Behavior*, Vol. 44, pp. 103-117, doi: 10.1016/j.chb.2014.10.059.

Shropshire, J., Warkentin, M. and Sharma, S. (2015), "Personality, attitudes, and intentions: predicting initial adoption of information security behavior", *Computer & Security*, Vol. 49, pp. 177-191.

Siau, K.F., Nah, F.-H. and Teng, L. (2002), "Acceptable internet use policy", *CACM*, Vol. 45, pp. 75-79.

Simmonds, A., Sandilands, P. and Ekert, L.V. (2004), "An ontology for network security attacks", in Manandhar, S., Austin, J., Desai, U., Oyanagi, Y. and Talukder, A. (Eds), *Applied Computing*, Springer, Berlin, pp. 317-323.

Singh, A.N., Picot, A., Kranz, J., Gupta, M.P. and Ojha, A. (2013), "Information security management (ISM) practices: lessons from select cases from India and Germany", *Global Journal of Flexible Systems Management*, Vol. 14 No. 4, pp. 225-239.

Siponen, M.T. (2005), "An analysis of the traditional information security approaches: implications for research and practice", *European Journal of Information Systems*, Vol. 14 No. 3, pp. 303-315.

Siponen, M. and Vartiainen, T. (2004), "Unauthorized copying of software and levels of moral development: a literature analysis and its implications for research and practice", *Information Systems Journal*, Vol. 14 No. 4, pp. 387-407.

Siponen, M., Mahmood, M.A. and Pahnila, S. (2014), "Employees' adherence to information security policies: an exploratory field study", *Information & Management*, Vol. 51 No. 2, pp. 217-224.

Smith, S., Winchester, D., Bunker, D. and Jamieson, R. (2010), "Circuits of power: a study of mandated compliance to an information systems security de jure standard in a government organization", *MIS Quarterly*, Vol. 34 No. 3, pp. 463-486.

Son, J.-Y. (2011), "Out of fear or desire? toward a better understanding of employees' motivation to follow information security policies", *Information Management*, Vol. 48 No. 7, pp. 296-302.

Soo Hoo, K.J. (2000), "How much is enough: a risk management approach to computer security", working paper, Center for International Security and Cooperation, Stanford University, available at: http://cisac.stanford.edu/publications/how_much_is_enough__a_riskmanagement_approach_to_computer_security/.

Straub, D.W. and Nance, W.D. (1990), "Discovering and disciplining computer abuse in organizations: a field study", *MIS Quarterly*, Vol. 14 No. 1, pp. 45-60.

Sunyaev, A., Kaletsch, A., Mauro, C. and Krcmar, H. (2009), "Security analysis of the German electronic health card's peripheral parts", *ICEIS – Proceedings of the 11th International Conference on Enterprise Information Systems, ISAS*, pp. 19-26.

Trcek, D., Trobec, R., Pavesic, N. and Tasic, J.F. (2007), "Information systems security and human behaviour", *Behaviour & Information Technology*, Vol. 26 No. 2, pp. 113-118.

Vance, A., Lowry, P.B. and Eggett, D. (2013), "Using accountability to reduce access policy violations in information systems", *Journal of Management Information Systems*, Vol. 29 No. 4, pp. 263-290.

Vivo, M.D., Vivo, G.O.D. and Isern, G. (1998), "Internet security attacks at the basic levels", *ACM SIGOPS - Operating Systems Review*, Vol. 32, pp. 4-15.

Wang, H., Jin, C. and Shin, K.G. (2007), "Defense against spoofed IP traffic using hop-count filtering", *IEEE/ACM Transactions on Networking*, Vol. 15 No. 1, pp. 40-53.

Webb, J., Ahmad, A., Maynard, S.B. and Shanks, G. (2014), "A situation awareness model for information security risk management", *Computers & Security*, Vol. 44, pp. 1-15, doi: 10.1016/j.cose.2014.04.005.

Werlinger, R., Hawkey, K. and Beznosov, K. (2009), "An integrated view of human, organizational, and technological challenges of IT security management", *Information Management & Computer Security*, Vol. 17 No. 1, pp. 4-19, available at: www.emeraldinsight.com/10.1108/09685220910944722 (accessed 13 June 2016).

Werlinger, R., Hawkey, K., Botta, D. and Beznosov, K. (2009), "Security practitioners in context: their activities and interactions with other stakeholders within organizations", *International Journal of Human-Computer Studies*, Vol. 67 No. 7, pp. 584-606, doi: 10.1016/j.ijhcs.2009.03.002.

Willison, R. (2006), "Understanding the perpetration of employee computer crime in the organisational context", *Information and Organization*, Vol. 16 No. 4, pp. 304-324.

Witherspoon, C.L., Bergner, J., Cockrell, C. and Stone, D.N. (2013), "Antecedents of organizational knowledge sharing: a meta-analysis and critique", *Journal of Knowledge Management*, Vol. 17 No. 2, pp. 250-277, doi: 10.1108/13673271311315204.

Wright, B.R.E., Caspi, A., Moffitt, T.E. and Paternoster, R. (2004), "Does the perceived risk of punishment deter criminally prone individuals? Rational choice, self-control, and crime", *Journal of Research in Crime and Delinquency*, Vol. 41 No. 2, pp. 180-213.

Yeniman, Y., Ebru Akalp, G., Aytac, S. and Bayram, N. (2011), "Factors influencing information security management in small-and medium-sized enterprises: a case study from turkey", *International Journal of Information Management*, Vol. 31 No. 4, pp. 360-365.

Zhang, J., Reithel, B.J. and Li, H. (2009), "Impact of perceived technical protection on security behaviors", *Information Management & Computer Security*, Vol. 17 No. 4, pp. 330-340.

Further reading

Breslin, P. (2014), *Security Updates: The Upcoming Revision of ISO/IEC 27001*, DNV Business Assurance (accessed 27 January 2015).

Hsu, C.W., Lee, J.-N. and Straub, D.W. (2012), "Institutional influences on information systems security innovations", *Information Systems Research*, Vol. 23 No. 3, pp. 918-939, available at: http://isr.journal.informs.org/cgi/doi/10.1287/isre.1110.0393

McFadzean, E., Ezingeard, J.-N. and Birchall, D. (2011), "Information assurance and corporate strategy: a Delphi study of choices, challenges, and developments for the future", *Information Systems Management*, Vol. 28 No. 2, pp. 102-129, doi: 10.1080/10580530.2011.562127.available at: www.tandfonline.com/doi/abs/ (accessed 15 June 2016).

Appendix

Survey Questionnaire:

IT Security Services created a survey to help establish a baseline for an Information Security Awareness Program. The questions have been posted below along with additional information.

There are 70 questions in this survey

[1] Please fill the following? *

[]Gender:
[]Age:
[]Occupation:
[]Position:
[]Years of Experience:
[]Salary:

[2] Is it true that an anti-virus program installed on your computer prevents it from being infected, as the anti-virus program will block all viruses, worms and Trojans?

Please write your answer here:

[3] How can you identify an e-mail scam and what do you understand by the that?

Please write your answer here:

[4] Is it advisable to use personal devices, such as your mobile phone, tablets or personal computer, to store or transfer sensitive information from your organization?

Please write your answer here:

[5] According to your organization policies, Cloud services, other than Google Drive, are used to store organizational data?

Please write your answer here:

[6] You believe that the responsibility of protecting your organization's devices and information rests solely on Information Technology Services.*

Please write your answer here:

[7] I have nothing to worry since company computer or information has no value to hackers; they do not target me.

Please write your answer here:

[8] Is your work computer configured to be automatically updated or you have no time for updating due to all the pop ups? *

Please write your answer here:

[9] Do you take a lot of cautions when you open an attachment in e-mail? *

Please choose **only one** of the following:

- ○Yes
- ○No

[10] Do you share your password with co-workers or your boss? *

Please choose **only one** of the following:

- ○Yes
- ○No

(*continued*)

[11] Do you use the same passwords for your company accounts as you do for your personal accounts at home, such as Facebook, Twitter, iTunes, or your personal e-mail accounts? *

Please choose **only one** of the following:

- ○Yes
- ○No

[12] Will you log into company's accounts, including e-mail, using public computers, such as computers from a public library, cyber café or hotel lobby? *

Please choose **only one** of the following:

- ○Yes
- ○No

[13] Is your organization meeting its own expectation with regards to information management? *

Please choose the appropriate response for each item:

	Yes	Uncertain	No
Yes	○	○	○
No	○	○	○
I Don't Know	○	○	○

[14] Is your organization aware of Knowledge and Information Management (KIM)? *

Please choose **only one** of the following:

- ○Yes
- ○No

[15] Is there any strategy that has been successfully been integrated in to the corporate strategy of your organization? *

Please choose **only one** of the following:

- ○Yes
- ○No

[16] Are there performance measurement for KIM in your organization?

Please choose **only one** of the following:

- ○Yes
- ○No

[17] If you answered yes to question B001, have they been reported to the board of directors in the last 3 years?

Please choose **only one** of the following:

- ○Yes
- ○No

[18] Who is responsible for your Organization KIM? *

Please choose **only one** of the following:

- ○Executive
- ○Senior Manager
- ○Technology Manager
- ○Department Manager
- ○No idea
- ○I Don't Know
- ○Other

[19] How do managers see and understand the critical factor of KIM in your organization? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

(*continued*)

[20] Is your organization documenting how information asset is being utilized? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[21] Has your organization assessed and identified critical information? *

Please choose the appropriate response for each item:

	Yes	Uncertain	No
Yes	○	○	○
No	○	○	○
I Don't Know	○	○	○

[22] If so, is the organization critical information part of the business continuity plan of the organization? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[23] Has your organization determined the cost and resources need for KIM? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[24] Can your organization demonstrate KIM function cost as percentage of the total expenditure? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[25] Has your organization identified risk to its information assets? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[26] Is there a constant review of the organization KIM function in the last 3 years from the internal audit? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[27] Do senior managers capturing digital continuity and review them? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

(*continued*)

[28] Is your organization aware of information needed? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[29] Is your organization aware of information needed by the users and when needed? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[30] Are there any naming conventions that are mandatory to abide by? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[31] Are there any means of monitoring misfiling and non-filing? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[32] Are there any means and how and when information created is destroyed? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[33] Select the range of percentage that information managements are included in new projects *

Please choose the appropriate response for each item:

None	○
Less than 10%	○
10% - 49%	○
49% - 59%	○
59% - 69%	○
69% - 79%	○
79% - 89%	○
89% - 99%	○
100%	○

[34] Has your organization secured its knowledge and Information? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[35] Is there any coherent information and records management systems in your organization? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

(*continued*)

[36] Is data frequently stored on corporate server instead of personal devices? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[37] Does your organization have a transparent overall view of paper records? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[38] Does your organization have a direct access control in place for digital information? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[39] Does your organization promptly withdraw and block access to information from users who should no longer have access to information? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[40] Does your organization have guidelines with regards to what information need to be kept and where? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[41] Is your organization aware of its business prerequisites for storing digital records? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[42] Is your organization aware of its technical environment that enhances its information? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[43] Does your organization know the period to retain information? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

(*continued*)

[44] Are legislation prerequisites and impacts identified? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[45] Does the organization meet FOI request? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[46] Does the organization share information across business sectors? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[47] Is this shared for commercial gain? *

Please choose **only one** of the following:

- ○Yes
- ○No

[48] Do data management managers have the required skills? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[49] Do workers have the right information management systems skills? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[50] Do managers go for professional development training? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[51] Do KIM leaders having the right skills?
*Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[52] Is there any change management program? *

Please choose **only one** of the following:

- ○Yes
- ○No

[53] If there is change management programs, is KIM part of it? *

Please choose **only one** of the following:

- ○Yes
- ○No

(*continued*)

[54] Has your organization clarified procedures to examine completeness, availability and usability of data assets after change? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[55] Does your organization include training in their organization induction programs? *

Please choose **only one** of the following:

- ○Yes
- ○No

[56] Do you think the training in the organization induction programs enhances KIM? *

Please choose **only one** of the following:

- ○Yes
- ○No

[57] Is the organization having records management policy? *

Please choose **only one** of the following:

- ○Yes
- ○No

[58] Is information management part of this policy? *

Please choose **only one** of the following:

- ○Yes
- ○No

[59] Is there a policy or strategy governing digital records storage over a period of time and within a technical change? *

Please choose **only one** of the following:

- ○Yes
- ○No

[60] Are stakeholders part of the policy or strategy governing digital records storage development and implementation? *

Please choose **only one** of the following:

- ○Yes
- ○No

[61] Do staff at all level have easy access to information management policies and guidance within the organization? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[62] Do managers proactively transfer the essentials of good information management to staff at all level? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[63] Do staff at all level see the benefit of this transparency? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

(*continued*)

[64] Do staff at all level understand the essentials of KIM? *

Please choose **only one** of the following:

- ○Yes
- ○No

[65] Is there any knowledge transfer mechanism to ensure knowledge are shared and captured? *

Please choose **only one** of the following:

- ○Yes
- ○No

[66] Do all staff value, recognize and understood corporate knowledge? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[67] Is the usage of KIM apparatus and methods available to users? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[68] Is there any strategical system adopted to enhance internal communication and work collaboration? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[69] Do the sharing of good practices enhanced by the existence of KIM networks and communities? *

Please choose **only one** of the following:

- ○I Don't know
- ○Partially
- ○Totally
- ○Average
- ○Not Applicable
- ○Not Much

[70] Thank you for taking part in this survey. We would like to know how easy or difficult it was for you to complete this questionnaire *

Please choose **only one** of the following:

- ○Easy
- ○Very Easy
- ○Too much Questions
- ○Neither Easy nor Difficult
- ○Fair
- ○Difficult
- ○Very Difficult
- ○Time Consuming
- ○Other

11-06-2016 – 00:00

Submit your survey.
Thank you for completing this survey.