Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Information security policy compliance model in organizations

Nader Sohrabi Safa [a,*], Rossouw Von Solms [a], Steven Furnell [a,b]

[a] Centre for Research in Information and Cyber Security, School of ICT, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa

[b] Centre for Security, Communications and Network Research, Plymouth University, United Kingdom

ARTICLE INFO

Article history:
Received 11 August 2015
Received in revised form 23 September 2015
Accepted 17 October 2015
Available online 3 November 2015

Keywords:
Information security
Organization policies
Users' behaviour
Involvement
Attitude

ABSTRACT

The Internet and information technology have influenced human life significantly. However, information security is still an important concern for both users and organizations. Technology cannot solely guarantee a secure environment for information; the human aspects of information security should be taken into consideration, besides the technological aspects. The lack of information security awareness, ignorance, negligence, apathy, mischief, and resistance are the root of users' mistakes. In this research, a novel model shows how complying with organizational information security policies shapes and mitigates the risk of employees' behaviour. The significant aspect of this research is derived from the conceptualization of different aspects of involvement, such as information security knowledge sharing, collaboration, intervention and experience, as well as attachment, commitment, and personal norms that are important elements in the Social Bond Theory. The results of the data analysis revealed that information security knowledge sharing, collaboration, intervention and experience all have a significant effect on employees' attitude towards compliance with organizational information security policies. However, attachment does not have a significant effect on employees' attitude towards information security policy compliance. In addition, the findings have shown that commitment and personal norms affect employees' attitude. Attitude towards compliance with information security organizational policies also has a significant effect on the behavioural intention regarding information security compliance.

1. Introduction

Web-based technologies have brought many advantages to organizations and their customers, but information security breaches are still a controversial concern. Anti-virus, anti-malware, anti-spam, anti-phishing, anti-spyware, firewall, authentication, and intrusion detection systems are all technological aspects that address information security, but they cannot guarantee a secure environment for information (Safa et al., 2015). Hackers target people, rather than computers, in order to create a breach; examples of user mistakes include inappropriate information security behaviour, such as taking a social security number as user name and password, writing passwords on sticky paper, sharing their username and password with colleagues, opening unknown emails and downloading their attachments, as well as downloading software from the Internet. Acceptable information security

* *Corresponding author.* Tel.: +27415043302, +27415049604, +441752586234.
E-mail addresses: nader.sohrabisafa@nmmu.ac.za (N. Sohrabi Safa), Rossouw.VonSolms@nmmu.ac.za (R. Von Solms), S.Furnell@plymouth.ac.uk (S. Furnell).
http://dx.doi.org/10.1016/j.cose.2015.10.006
0167-4048/

behaviour should ideally be combined with technological aspects (Furnell and Clarke, 2012). Thus, in the information security environment, applying multiple security approaches is necessary to mitigate the risk of information security breaches.

The World Wide Web is a huge and dynamic environment, within which hackers use new and different methods to achieve security breaches (Safa et al., 2014). Misleading applications, such as bogus disk defragmentation or fake anti-virus scanners, are samples of new methods that are designed to mislead users into thinking that their computer has a problem or a virus. These kinds of misleading applications usually report non-existent problems or threats, and they suggest that downloading free software that could possibly be spyware (Kim et al., 2015); knowledge sharing in these cases can mitigate the effect of these attacks in organizations.

Von Solms and Van Niekerk (2013) have investigated different aspects of cyber security, and they asserted that although information security and cyber security have a substantial overlap, these two concepts are not totally analogous. The general definition of information security comprises availability, integrity, and confidentiality. Cyber security includes additional dimensions, which extend beyond the formal boundaries of information security, including humans in their personal capacity and society at large. It can be harmed or affected; whereas this is not necessarily the case with information security, where harm is always indirect. Collaboration within organizations is necessary in order to establish a security environment for both information security and cyber security (Werlinger et al., 2009).

Information security breaches not only lead to extra costs for organizations, but they also affect their reputation significantly (Safa and Ismail, 2013). Proper information security behaviour, besides the technological aspects of information security, mitigates the risk of information security breaches in organizations. Previous studies have revealed that employees' information security awareness plays a vital role in mitigating the risk associated with their behaviour in organizations (Abawajy, 2014; Arachchilage and Love, 2014). Kritzinger and von Solms (2010) divided users into two groups – home and organizational users – and they asserted that information security awareness plays a vital role in both groups. This study has also revealed that delivery methods and enforcement components play important roles in this domain. Information security awareness can stem from employees' experience in this domain. Information security experience leads to comprehension, familiarity, as well as the ability and skill to manage incidents (Safa et al., 2015).

Previous studies have also indicated that organizations that have neglected to focus on individuals fail to achieve success in their efforts (Li et al., 2010; Stanton et al., 2005; Webb et al., 2014). Experts recommend multi-perspective approaches for protecting organizations' information assets (Herath and Rao, 2009). Although organizations invest in the technological aspects of information security and tools, the number of security incidents and breaches continues to be a significant problem due to the lack of attention to employees in organizations (Ifinedo, 2012). Amendment and improvement of employees' information security behaviour, in line with information security organizational policies and procedures (ISOP), are an effective and efficient approach (Crossler et al., 2013; Son, 2011). However, previous research has shown that although information system security policies are in place to help safeguard an organization against abuse, destruction and misuse, their employees do not comply with such documents (Vance et al., 2012). The improvement of employees' information security behaviour, in line with ISOP, is imperative for a secure environment (Woon and Kankanhalli, 2007). Ifinedo (2014) investigated employees' information security policy compliance behaviour in organizations from the theoretical lens of a social bond. Attachment to the organization, commitment to the organizational policies and plans, involvement in particular activities, such as information security, and the belief that information security behaviour is important to safeguard informational assets are the main factors in the Social Bond Theory.

In another study, Cheng et al. (2013) described the violation of information security policy in organizations. The results of the study revealed that employees with a stronger bond to their organization are less likely to deviate from policies and participate in delinquent behaviour.

This research aims to improve employees' information security behaviour in line with information security policies and procedures, based on involvement, attachment, commitment and the personal norms that stem from the Social Bond Theory (SBT). Information security knowledge sharing, collaboration, intervention and experience not only shape employees' involvement in line with information security issues, but they also serve to increase the level of information security awareness and knowledge, which is a significant aspect of this research.

In this paper, the theoretical background of the research model is illustrated in section two. Diverse parts of the conceptual framework, together with their hypotheses, are discussed in section three. A description of the research methodology, data collection and demography of the participants is illustrated in section four. The data analyses with more details and their results are covered in section five. This is followed by a discussion of these findings in section six. The conclusion, limitation and future works are presented in section seven.

2. Theoretical background

The Internet has introduced a new communication model that differs from the traditional media, regardless of the users' social, educational, political or economic orientations. However, information security breaches are still important issues among experts in this domain. In this research, compliance with ISOP is presented as an effective and efficient approach to mitigate the risk of information security breaches in organizations. Concepts in the Social Bond and Involvement Theories were applied to develop a conceptual framework that shows how commitment, attachment, involvement and personal norms can serve to change employees' attitudes towards compliance with information security policies and procedures in organizations.

In this research, information security knowledge sharing, collaboration, intervention and experience have been replaced by involvement in the SBT based on the nature and meaning of such involvement. Information security knowledge sharing, collaboration, intervention and experience are the novel

aspects of this research that have been derived from the Involvement Theory. More explanations about the theories and factors will be presented in the following sections.

2.1. *Social bond theory*

In order to better understand employees' compliance with ISOP, the SBT was applied. The SBT has attracted the attention of experts in recent years. Hirschi (1969) proposed the SBT and argued that men are intrinsically prone to deviance. The SBT describes how individuals, who have stronger social ties, engage less in deviant behaviour. This is a salient point in this theory that encourages us to use it, in order to increase the level of information security compliance with organizational policies and procedures. Deviance occurs when the social bond is weak or broken. Attachment, involvement, commitment and personal norms are the four main elements in this theory. These components are separate, but interrelated. The more an individual is bonded to an organization, the less likely he or she is to deviate from the organization's policies (Chapple et al., 2005).

Previous studies have also applied the SBT to explain the delinquency of adolescents. Their attachment to conventional significant others, their commitment to the actions of conventional goals, their involvement in conventional activities, and their belief in the validity of common value systems affect their delinquent behaviour. In this situation, they either neglect, or fail to do what the law or duty requires (Mesch, 2009; Veenstra et al., 2010). The scope of SBT applications was extended to adult criminality and organizational deviances. Lee et al. (2004) demonstrated that attachment, commitment, involvement and beliefs significantly decrease insiders' computer abuse. Cheng et al. (2013) and Ifinedo (2014) have described how the compliance of employee behaviour with information security policies and procedures lower the risk of information security breaches in organizations. In line with these studies, we adopted the social bond factors in this research. Attachment to organization, commitment to organizational policies and plans, involvement in information security, and the personal belief that complying with organizational information security policies and procedures is important to safeguard information assets, are main factors in this research model.

2.2. *Involvement theory*

The Involvement Theory discusses the level of energy, time and participation in a particular activity (Lee et al., 2004). The Involvement Theory has been applied in various domains, such as customer involvement, product involvement, student involvement, and so forth. Rocha Flores et al. (2014) argued that the lack of information security awareness or knowledge among staff can be explained by the low level of information security involvement. Involvement influences attitude and it can manifest in different forms. Information security knowledge sharing, collaboration, intervention and experience, all show the effort, participation and time that an employee spends on safeguarding information assets in the organization. In other words, information security knowledge sharing, collaboration, intervention and experience indicate different aspects of involvement. This research endeavours to investigate whether information security knowledge sharing, collaboration, intervention and experience influence employees' attitude towards complying with organizational information security policies and procedures.

3. Conceptual framework and hypotheses

In this research, we conceptualize a novel model that shows compliance with ISOP. The concepts in the Involvement Theory and the SBT were applied in the research model. The framework has two main sections. The first part discusses the different aspects of information security involvement, such as information security knowledge sharing, collaboration, intervention and experience. The second part discusses the attachment, commitment and personal norms that are the other main elements in SBT. These are further described in the sections that follow.

3.1. *Information security knowledge sharing*

Knowledge is the theoretical or practical understanding of a subject, fact, information, value, or skill achieved through education or experience. Knowledge sharing helps others to collaborate, so as to solve a problem, establish new ideas, or implement policies or procedures (Wang and Noe, 2010). Data, information and human knowledge together define organizational knowledge when shared among employees properly; they are valuable assets that can help decision-making, improve efficiency, mitigate risks and reduce costs (Lee et al., 2011).

Information security knowledge sharing is an effective approach to increase the level of awareness and it is a sign of information security involvement. Experts face similar problems in this domain and they should provide proper solutions. Preventing the duplication of developing the same solutions for similar problems by sharing knowledge leads to avoiding wasted time and money (Feledi et al., 2013). Such time and money could be better spent increasing the quality of solutions, instead of reinventing the security wheel. However, the previous study showed that the motivation for knowledge sharing among the professionals is the important challenge in this domain. Sharing previous relevant experience in the domain of information security is a valuable resource in information security awareness (Rhee et al., 2009). Tamjidyamcholo and Sapiyan Bin Baba (2014) investigated the effect of information security knowledge sharing in the virtual community and its effect in reducing risk. They also mentioned the low level of willingness of members to share knowledge with one another as an important barrier in information security knowledge sharing.

Cyber security is a complex task and users' knowledge can significantly mitigate the risk of security incidents (Ben-Asher and Gonzalez, 2015). Arachchilage and Love's (2014) investigation also revealed that users' knowledge thwarts the threat of phishing. Knowledge can be explicit and implicit. The knowledge that can be expressed in words, organized, summarized, and transferred via documents, guidelines, even video is explicit. Implicit knowledge is in the individuals' minds; it has not yet been codified in structured form, and so it is difficult to transfer (Rocha Flores et al., 2014). Information security

knowledge sharing not only increases the level of awareness, but it also shows information security involvement in organizations. Awareness has been mentioned as an important factor that affects individuals' attitude towards performing a particular behaviour (Abawajy, 2014). Based on the aforementioned explanations, we hypothesized that:

H1. Information security knowledge sharing has a positive effect on employees' attitude towards compliance with ISOP.

3.2. *Information security collaboration*

Collaboration is defined as working together in order to do a task or achieve a goal. Collaboration is synonymous with participation, association and sometimes teamwork; it is a recursive process, in which two or more persons, teams or organizations, work together to reach shared goals. Information security collaboration helps experts to collect, integrate, classify, distribute, and share information security knowledge with the other experts and employees. Communication and collaboration in responding to the information security incidents were highlighted by Ahmad et al. (2012). The organizations' incident tracking system communicates between employees and technical teams.

This collaboration is imperative in terms of documentation, and providing a timeline for activities and a set of evidence for incident handling. Collaboration can be in the shape of submitting, improving, commenting on and peer-reviewing the submitted knowledge (Feledi et al., 2013). Identifying features, in order to assess information security threats, is one of the benefits of collaboration (Mace et al., 2010). Bernard (2007) investigated information lifecycle security risk assessment to close such security gaps. The collaboration among members of an information security council has been mentioned as being the most successful policy to address the critical information risk picture. The members are typically from IT security, audit, human resources, legal, complaints, risk management, corporate security, and various other units. They report information security breaches and this collaboration can create valuable knowledge in this domain. Information security collaboration enables users to understand and extend their information about security breaches. Information security collaboration reduces the cost of knowledge capturing and processing for companies in the domain of information security. Based on the aforementioned explanations, we postulate:

H2. Information security collaboration has a positive effect on employees' attitude towards compliance with ISOP.

3.3. *Information security intervention*

Participation, dialogue, and collective reflection in groups are the methods that improve the level of awareness in the domain of information security (Albrechtsen and Hovden, 2010). Seminars, lectures, online learning and discussions, sending messages and emails, blogging, videos, and newsletters are examples of tools that could improve information security awareness and show information security involvement in organizations. These tools affect users' perception, comprehension, and prediction of cyber security at individual and organizational levels (Shaw et al., 2009).

The Internet is a huge network and it has a great potential for information security breaches. Hackers use various methods to breach the confidentiality, integrity, and availability of information. The cyber environment is a dynamic space and users' awareness should be updated frequently (Stanton et al., 2005). Relevance, timeliness, and consistency are the important characteristics of security awareness programmes. Parsons et al. (2014) investigated the effects of organizational policy awareness and intervention on the attitude and behaviour of users. The results of their research showed that intervention has a positive effect on the level of knowledge about organizational policy and that better knowledge of information security policy is associated with a better attitude towards policy. Information security intervention increases the level of awareness in the domains of Internet, emailing, social engineering, pass-wording, and incident reporting. Hence, the following hypothesis is proposed:

H3. Information security intervention has a positive effect on employees' attitude towards compliance with ISOP.

3.4. *Information security experience*

Experience is the knowledge or mastery that leads to familiarity, ability, skill and comprehension of an event or a subject through exposure to it or involvement with it. Individuals with considerable experience in a particular field gain a reputation and are known as experts. In this research, information security experience refers to familiarity with information security incidents, skills and the ability to prevent, manage, and mitigate the risk of information security events. Ashenden (2008) considered knowledge and experience, risk analysis and management, information relating to incidents and vulnerabilities, strategy and planning, process and procedures, policies and standards, methodologies and frameworks, training, audits, contract and outsourcing as different aspects of information security management. It is interesting to note that knowledge and experience are at the top of the list in this investigation. Albrechtsen (2007) studied users' experience and its role in the domain of information security. The results revealed that the lack of information security knowledge and experience is the main problem regarding the role of users in information security work. Knowledge and experience help to generate proper behaviour in the actual and dynamic environment (Internet). We therefore postulate that:

H4. Information security experience has a positive effect on employees' attitude towards compliance with ISOP.

3.5. *Attachment, commitment and personal norms*

Attachment, commitment, involvement and belief are the four main factors that were presented by Hirschi (1969) in order to describe how individuals bond with social institutions. The SBT predicts that an individual with more bonds with conventional society is less likely to deviate from those general norms and engage in delinquent behaviour. Crime occurs when the

social bond is weak or broken. This theory explains the delinquency of teenagers, particularly juveniles' attachment to others, commitment to the fulfilment of their goals, involvement in their activities, and belief in the moral validity of common values. All these affect juveniles' delinquent behaviour, such as misbehaving, drunk-driving, cigarette smoking, and drug abuse, that society considers wrong or criminal (Chapple et al., 2005; Mesch, 2009).

The Social Bond Theory has been used to describe employees' information security compliance with organizations' policies and procedures in recent years (Cheng et al., 2013; Ifinedo, 2014). The Social Bond Theory has been extended to include organizational deviance. Employees who have a stronger bond with their managers, co-workers and organizations are less likely to engage in white-collar crime. The rate of deviance would increase when the bond between employees and the organization is weak or broken. Individuals who have a stronger bond with a group would be more likely to conform to their rules.

Attachment refers to the respect and affection that an individual has with significant others. Co-workers, supervisors, jobs and organizations can be significant others. Individuals with strong attachment are less likely to engage in deviant behaviour (Cheng et al., 2013). Employees seek their supervisor's support. Therefore, they care about the recognition provided by these people. Supervisors evaluate their performance and affect their promotion; attachment to a supervisor and following his/her advice has a positive effect on employees' behaviour (Zhai et al., 2013). Therefore, we propose the following hypothesis:

H5. Attachment has a positive effect on employees' attitude towards compliance with ISOP.

People are the main issue in the human aspects of information security due to their direct contact with information. Their responsibility and commitment to safeguard information assets play a vital role in this domain (AlHogail, 2015). Commitment refers to the aspiration of acquiring a high status job. Personal achievement and reputation are important to committed individuals (Cheng et al., 2013). They spend more time and energy in order to achieve success in their careers. Committed persons would not take the risk of breaking rules that could thereby jeopardize or destroy their career aspirations (Lee et al., 2004). Consequently, employees with more commitment to the organization are less likely to deviate from the security policies. Hence, the following hypothesis is proposed:

H6. Commitment has a positive effect on employees' attitude towards compliance with ISOP.

Personal norms refer to the employees' values and views on information security compliance with organizational policies. Lee et al. (2004) investigated the role of personal norms in the formation of acceptable computer behaviour. A review of the literature revealed that personal norms affect individuals' attitude towards engaging in organizational information security misbehaviour (Lee and Kozar, 2005; Ng et al., 2009). It is conjectured that individuals with favourable personal values and norms have a positive attitude towards complying with information security policies in organizations. Therefore, we propose the following hypothesis:

H7. Personal norms have a positive effect on employees' attitudes towards compliance with ISOP.

Attitude refers to the individual's positive or negative feeling towards engaging in specific behaviour. Attitude towards objects could manifest in a place, person, event, or thing that individuals perceive (Hepler, 2015). Attitude originates from an individual's past and present. An attitude is an evaluation of objects, people, activities, events and ideas, changing from very positive to very negative. In the domain of information security, an employee's attitude towards complying with organizational information security policies leads to actual compliance with the policies (Siponen et al., 2014). We conjecture that a positive attitude towards organizational information security policies has a positive effect on compliance with these policies, yielding a final hypothesis as follows:

H8. Employees' attitude towards compliance with ISOP has a positive effect on ISOP compliance behavioural intentions.

Fig. 1 shows the formation of ISOP compliance behaviour intention in a concise form.

4. Research methodology

This research aims to present a conceptual framework that shows how information security policy compliance arises in organizations. The effective factors were extracted from a review of the literature. The SBT and the concept of involvement helped us to construct a novel conceptual framework that shows how employees comply with organizational information security

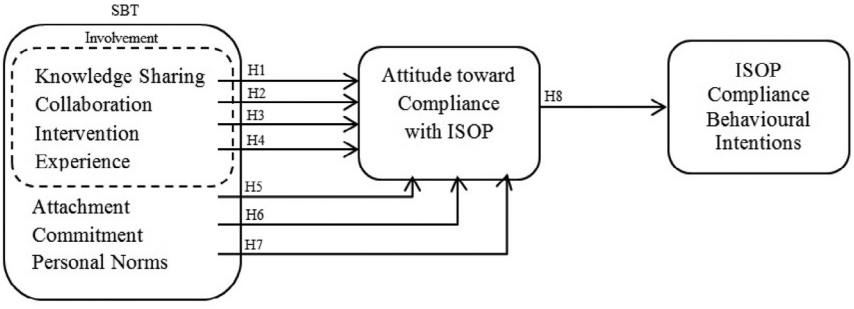

Fig. 1 – Information security compliance with organizational policies model.

policies. The data were collected by means of a Likert scale and questionnaires. The items for each construct are adopted from previous studies and each question relates to an item (Cheng et al., 2013; Ifinedo, 2014; Tamjidyamcholo et al., 2014; Witherspoon et al., 2013). IBM Amos 20 was used for the data analysis. More explanation will be presented in the next section.

4.1. *Data collection*

The data were collected from the employees of four different companies who had established proper information security policies in order to safeguard their information assets in Malaysia from the beginning of February to the end of April 2015. All the participants had access to the Internet and worked with a web system in different departments. The preliminary version of the questionnaire was pilot-tested in order to investigate whether all the participants understood the questions in a similar way, and whether they interpreted questions in the same manner. We described the purpose of this research with them and requested them to answer the questionnaire in the presence of one of the researchers to provide some feedback regarding wording, applicability and comprehension of the instruments. Their consent was important for us. We explained to them that the data would only be used confidentially for academic purposes. After they had given their consent, we presented the questionnaire to them. Pilot testing with 52 questionnaires revealed that the participants understood and interpreted the questions correctly. The final version of the questionnaire included 42 questions, in which every factor was measured by several items.

Besides the traditional data collection (by questionnaire), we used the electronic version of the questionnaire and sent the link of the questionnaire to the email of some participants in order to speed up the data gathering. Their responses were collected automatically in the data set. Using these kinds of facilities, the respondents could answer the questionnaires at any time and place, and the data collection is more user-friendly for the researchers.

4.2. *Demography*

Two approaches were used for the data collection. The data were collected by paper-based questionnaires and via an electronic version. A total of 416 questionnaires were emailed to participants, using the facilities in Google, yielding a total of 302 responses. Six questionnaires were not considered as useable data due to inconsistent responses, and thus 296 questionnaires were saved in the main dataset for further analysis. In addition, 174 questionnaires (hard copies) were personally distributed to the participants. To decrease the number of incomplete questionnaires, the participants' responses were reviewed immediately after completion and we asked them to complete the neglected questions. Despite our efforts to have completed questionnaires, eight of them were rejected in this part due to their incompleteness. Finally, 462 questionnaires were considered for the data analysis. Table 1 shows the demographics of the participants in a concise form.

More information about participants' gender and education is presented in Table 2.

Table 1 – Participants' demographics.

Variables		Frequency	Per cent
Gender	Male	252	54.5
	Female	210	45.5
Age (years)	21–30	98	21.2
	31–40	132	28.6
	41–50	118	25.5
	51 and above	114	24.7
Education	Diploma	88	19.0
	Bachelor	224	48.6
	Master	142	30.7
	PhD	8	1.7
Position	Top manager personnel	12	2.5
	Mid-level personnel	126	27.3
	Junior staff	324	70.2
Number of participants	Retail/wholesale	111	24.1
	TelComs/IT	107	23.2
	Education	85	18.3
	Government	159	34.4

5. Results

Structural equation modelling (SEM) is acknowledged as a suitable approach for this kind of research (Hair et al., 2010). SEM uses various types of models to depict the relationships among observed variables in order to provide a quantitative test of a theoretical model hypothesized by the researcher. Basic models include regression, path, and confirmatory factor analyses. The research model in this study stems from a literature review in this domain and two fundamental theories – the Social Bond Theory and the Involvement Theory. Therefore, regression, path and confirmatory factor analysis that exist in SEM are acceptable for this research (Schumacker and Lomax, 2010). Knowledge sharing, collaboration, intervention, experience, attachment, commitment and personal norms are the latent (unobservable) variables in the model. These unobservable variables are measured by several items. These latent variables can be modelled by using a measurement model and a structural model.

Table 2 – Participants' information.

Organizational activity	Participants					
	Male	Female	Diploma	Bachelor's degree	Master's degree	PhD
Retail/wholesale	62	49	38	58	38	-
TelComs/IT	65	42	14	62	48	2
Education	40	45	12	56	32	5
Government	85	74	24	48	24	1

The measurement model is based on the relationships between the observed and the latent variables, while the structural model specifies the relationships among the unobserved variables (Gaur, 2009). The measurement model and the structural model are two important parts of the data analysis in this research.

5.1. *Measurement model*

Structural equation modelling is the most appropriate approach to address the relationships between independent, mediating and dependent variables (Arbuckle, 2007). SEM tests the overall data fit to the conceptual model, and it examines the relationships among the variables. SEM comprises the measurement model and the structural regression model. In the measurement model, each latent variable is measured by several observed variables or items, while the measurement structure regression model explores the relationships among the latent variables. The isolation of observational error in the measurement of the latent variables is an important advantage of SEM.

Standard skewness and kurtosis were applied to test the normal distribution of the data. The results of these tests were between –2 and +2, which shows the normal distribution of the data (Hair et al., 2010). Confirmatory factor analysis (CFA) is a multivariate statistical procedure to examine whether the measured variables are in line with our understanding of the nature of factors. CFA was applied since the model was developed from a review of the literature and the theories.

Factor loading of the measurement variables was calculated to test the convergent validity. Factor loading exceeding 0.5 demonstrates acceptable convergent validity. The items with factor loading of less than 0.5 were dropped from the model. ISKS6 in the information security knowledge sharing and ISC5 in information security collaboration were omitted from the model due to a lower factor loading in the respective constructs. The correlations between items and a factor are measured by using Cronbach's alpha. Cronbach's alpha shows internal consistency. Cronbach's alpha for all the constructs exceeded 0.7, which shows an acceptable level of internal consistency (Habibpor and Safari, 2008). Table 3 shows the measurement scale in a concise form.

We explored the correlations between all the pairs of constructs in order to probe the discriminant validity of the constructs. The correlations between all the pairs of constructs were below the recommended threshold value of 0.9, and the variances of all the constructs were above 0.5. In addition, the square root of the variance extracted was greater than the correlation of the constructs. Therefore, the discriminant validity of the constructs in the model was established. Table 4 shows the correlation matrices and their discriminant validities.

5.2. *Testing the structural model*

SEM was applied to explore the relationships among the independent, mediating, moderating and dependent variables. SEM presents reliable measurements when estimating the relationships among variables and examining the overall data fit to the research model. The maximum likelihood method in IBM Amos version 20 was applied in order to estimate the model's parameters.

The global fit measure and comparative fit measures were applied to test the fit indices. The chi-square test (χ^2) with degrees of freedom is generally used as the global model fit criterion. Chi-square/df indicates the extent to which the data can cover the hypothesis. A small chi-square/df equal to or less than 2 shows that the data and the model fit each other. The hypothesized model may be rejected due to a large sample size. The chi-square statistic is sensitive to sample size. Fortunately, our sample size was adequate for this test. The goodness of fit (GFI) measures show the fit between the actual data and the data that were predicted from the conceptual model. GFI with a degree of freedom presents another measure, which is the adjusted goodness of fit index (AGFI).

The comparative fit index (CFI) compares the data against the null model. A CFI with a value greater than 0.9 is an acceptable measure (Bagozzi and Yi, 2011). The incremental fit index (IFI) is a useful complementary measure that evaluates the model by considering the degree of freedom and the discrepancy. An IFI value close to 1 indicates a very good fit. The minimum discrepancy of the model with the data was tested by the normed fit index (NFI). A model with NFI equal to 1 shows that the model and the data perfectly cover each other. The root mean square of approximation (RMSEA) answers the question of "How well does the model fit the covariance matrix of the population?," and it addresses the error approximation. The measure of RMSEA with a value of less than 0.08 is considered good (Hair et al., 2010). The GFI, AGFI and RMSEA values indicate that the hypothesized model provides a good fit with the data. Table 5 shows the model fit indices.

The findings of the statistical tests are presented in Table 6. The results show that the path from information security knowledge sharing ($\beta = 0.722$, $p = 0.012$), information security collaboration ($\beta = 0.687$, $p = 0.004$), intervention ($\beta = 0.703$, $p = 0.041$), information security experience ($\beta = 0.806$, $p = 0.011$) towards attitude on compliance with ISOP was significant. However, the attachment does not have a significant effect on the attitude towards compliance with ISOP; therefore, hypothesis H5 is rejected. The results also revealed that commitment ($\beta = 0.614$, $p = 0.022$) and personal norms ($\beta = 0.571$, $p = 0.031$) have significant effects on attitude towards compliance with ISOP. Finally, the outcomes show the strong relationship between attitude towards compliance with ISOP and ISOP compliance behaviour intention ($\beta = 0.817$, $p = 0.002$).

6. Discussion

The significant aspect of this research is derived from the inclusion of the factors in the Social Bond Theory, on the one hand, and the concept of involvement, on the other hand. Information security knowledge sharing, collaboration, intervention and experience not only show users' involvement but also increase their information security awareness. Information security awareness plays a vital role in mitigating the risk of information security breaches (Akhunzada et al., 2015; Caputo et al., 2014). To the best of our knowledge, this is one of the first studies that discusses compliance with ISOP, based on the concept of information security involvement. This

Table 3 – The constructs, items, and their descriptive statistics.

Construct		Items	Mean	S.D.	Loading	Composite reliability
Information security knowledge sharing	ISKS1	I frequently share my information security knowledge in my working place in order to decrease information security risk.	4.36	.98	.765	.724
	ISKS2	I participate in information security knowledge sharing in order to keep myself up to date.	4.22	.89	.592	
	ISKS3	I think information security knowledge sharing helps me to understand the usefulness of information security policies in my organization.	4.44	.95	.635	
	ISKS4	I think information security knowledge sharing is an effective approach to mitigate the risk of information security breaches.	4.62	.99	.722	
	ISKS5	I think information security knowledge sharing is a valuable practice in organizations.	3.99	.82	.698	
	ISKS6	Information security knowledge sharing encourages me to follow information security policies and procedures.	3.82	1.02	Dropped	
Information security collaboration	ISC1	I feel collaboration with the information security team is reasonable.	4.36	.86	.598	.751
	ISC2	My collaboration with information security experts influences my attitude towards compliance with organization policies.	4.62	.78	.689	
	ISC3	I think my collaboration with information security experts mitigates information security incidents in my organization.	4.26	.88	.722	
	ISC4	I think my collaboration with information security experts leads to a proper response to information security breaches.	3.98	.99	.734	
	ISC5	I gain new information security knowledge in collaboration with experts.	3.42	.98	Dropped	
Information security intervention	ISI1	Information security training programmes increased my information security awareness.	4.12	1.01	.628	.804
	ISI2	Different information security training courses affected my attitude towards compliance with information security policies.	4.33	.96	.586	
	ISI3	Different information security training methods affected my attitude towards compliance with information security policies.	3.96	.84	.724	
	ISI4	I think the training programme is consistent with my organization's information security policies.	4.09	.78	.698	
Information security experience	ISE1	My information security experience changes my attitude towards compliance with organizational information security policies.	4.36	.83	.762	.784
	ISE2	My information security experience encourages me to comply with information security policies.	4.24	.92	.746	
	ISE3	My information security experience creates valuable knowledge for me.	4.39	1.04	.686	
	ISE4	I believe my information security experience causes a proper response to information security incidents.	4.45	1.06	.732	
Attachment	ATT1	My organization's concerns about information security incidents are important for me.	4.62	.95	.746	.767
	ATT2	I communicate with my colleagues about the importance of organizational information security policies.	4.12	.88	.676	
	ATT3	My colleagues' opinions and views about organizational information security policies are important to me.	4.06	.1.03	.694	
	ATT4	I always follow information security policies in order to have a secure environment in my organization.	4.61	.91	.586	
Commitment	COM1	I am committed to safeguarding organizational information assets.	4.01	.78	.688	.829
	COM2	I invest my energy and efforts to make organizational information security policies a success.	4.12	.98	.721	
	COM3	I am committed to promoting my organizational information security policies.	3.69	1.09	.692	
	COM4	I always keep myself updated based on new organizational information security policies.	4.07	.86	.722	

(*continued on next page*)

Table 3(*continued*)

Construct		Items	Mean	S.D.	Loading	Composite reliability
Personal norms	PN1	It is unacceptable to ignore my organization's information policies guidelines and measures.	4.62	.99	.702	.862
	PN2	Not following the organization's information security policies is not a trivial offence.	4.14	.83	.742	
	PN3	It is unacceptable not to follow guidelines and procedures in my organization's information security policies.	4.28	1.05	.522	
	PN4	Following information security organizational policies is a serious matter.	4.32	.86	.789	
Attitude towards compliance with ISOP	ACI1	Following ISOP is necessary.	4.40	.96	.699	.756
	ACI2	Following ISOP is beneficial.	4.14	.89	.742	
	ACI3	Following ISOP mitigates the risk of security breaches.	4.39	.91	.712	
	ACI4	Following ISOP is a good idea.	4.38	1.11	.564	
ISOP compliance behavioural intentions	ICBI1	I am certain I will adhere to ISOP.	4.16	.89	.706	.805
	ICBI2	It is my intention to continue to comply with ISOP.	4.08	.95	.689	
	ICBI3	I will comply with ISOP to protect information assets.	4.26	1.06	.521	
	ICBI4	I am likely to follow ISOP in the future.	4.14	.94	.712	
	ICBI5	I will follow ISOP whenever possible.	4.16	.96	.716	

The items with less than 0.5 factor loading were dropped from the model.
ISOP, information security organizational policies and procedures; S.D., standard deviation.

Table 4 – Correlation matrices and discriminant validity.

		Mean	SD	1	2	3	4	5	6	7	8	9
1	ISKS	4.24	0.98	0.826								
2	ISC	4.13	1.12	0.298	0.785							
3	ISI	4.12	0.92	0.311	0.302	0.779						
4	ISE	4.36	1.01	0.513	0.368	0.421	0.727					
5	ATT	4.35	0.85	0.189	0.231	0.179	0.356	0.712				
6	COM	3.97	1.03	0.168	0.256	0.292	0.276	0.280	0.852			
7	PN	4.34	0.96	0.243	0.512	0.189	0.222	0.149	0.362	0.728		
8	ACI	4.33	0.89	0.502	0.461	0.491	0.331	0.404	0.359	0.381	0.711	
9	ICBI	4.14	1.23	0.312	0.361	0.271	0.169	0.179	0.264	0.272	0.251	0.703

integrative conceptualization offers a new perspective to better understand ISOP compliance behavioural intentions. We believe that it supplements the previous research that was published by using a theoretical lens.

The results of the data analysis revealed that information security knowledge sharing has strong effects on one's attitude towards compliance with ISOP. Information security knowledge sharing furthers information security knowledge and awareness that affect the attitude towards ISOP compliance. This finding is in line with the results of the studies conducted by Rocha Flores et al. (2014) and Tamjidyamcholo et al. (2014). The findings showed significant and positive relationships between information security collaboration in organizations with a positive attitude towards compliance with ISOP. The plausible explanation for this finding exists in the collaboration process. Protecting information assets is the shared goal in information security collaboration. This collaboration implicitly increases the awareness and the experience, which both affect individuals' attitude towards compliance with ISOP (Vroom and von Solms, 2004).

Intervention, or, on the other hand, different training methods, also heighten employees' knowledge about information security, and this knowledge affects individuals' attitudes towards information security compliance with ISOP (Albrechtsen and Hovden, 2010; Parsons et al., 2014). Information security experience has been presented as another aspect of information security involvement in this research. The knowledge that comes from information security experience is deeper and more tangible for employees, and it has a significant effect on their attitude towards compliance with ISOP (Rhee et al., 2009). Contrary to our prediction, the results did not support H5; the impact of attachment on attitude towards ISOP compliance was not statistically significant. One conceivable explanation for this finding might be the perceived individual benefit and self-interest for such discord (Casper and Harris, 2008).

Table 5 – Fit indices of the model.

Fit indices	Model value	Acceptable standard
χ^2	1003.28	-
χ^2/Df	1.89	<2
GFI	0.936	>0.9
AGFI	0.961	>0.9
CFI	0.912	>0.9
IFI	0.919	>0.9
NFI	0.928	>0.9
RMSEA	0.062	<0.08

Table 6 – Results of the hypotheses tests.

Path			Standardized estimate	S.E.	*p* Value	Results
ISKS	→	ACI	0.722	0.097	0.012	Support
ISC	→	ACI	0.687	0.121	0.004	Support
ISI	→	ACI	0.703	0.086	0.041	Support
ISE	→	ACI	0.806	0.101	0.011	Support
ATT	→	ACI	0.554	0.082	0.316	Not supported
COM	→	ACI	0.614	0.189	0.022	Support
PN	→	ACI	0.571	0.221	0.031	Support
ACI	→	ICBI	0.817	0.134	0.002	Support

We postulated that employees' commitment influences their attitude towards ISOP compliance, based on a review of the literature. Committed persons would not take the risk of jeopardizing their role in organizations. Fortunately, the results of the statistical analysis showed a significant relationship between commitment and individuals' attitude towards compliance with ISOP. This finding is in line with the results of a study from Ifinedo (2014). The last effective factor in the framework that influences employees' attitude towards compliance with ISOP is personal norms. Personal norms refer to individuals' beliefs towards compliance with ISOP. The outcomes also showed a significant relationship between personal norms and attitude towards compliance with ISOP. This finding was confirmed by the studies of Van Niekerk and Von Solms (2010). Finally, the results of the statistical tests showed that attitude towards compliance with ISOP has a significant relationship with the related behavioural intention. This finding confirms the results of earlier studies (Ifinedo, 2014; Siponen et al., 2014).

7. Conclusion, limitations and future work

The Internet has become a conduit for services, applications, information content and opportunities for individuals and organizations. However, anecdotal and empirical evidence implies that the number and severity of information security breaches is growing. Compliance with organizational information security policies and procedures has been presented as an effective approach to mitigate information security breaches in organizations (Ifinedo, 2014; Vance et al., 2012). This research seeks to augment and diversify research on information security organizational policy compliance via the social bond and the involvement theories. Factors, such as involvement, commitment and beliefs, influence employees' attitude towards compliance with organizational information security policies and procedures. However, attachment did not affect the employees' attitude towards compliance with organizational information security policies and procedures. Information security knowledge sharing, collaboration in information security activities, intervention and experience together comprise the salient aspects of information security involvement.

Information security knowledge sharing in organizations not only increases the awareness among employees, but it also shows the importance of complying with organizational information security policies and procedures. Management can facilitate information security knowledge sharing by motivating their staff via intrinsic and extrinsic motivations. Extrinsic motivation is influenced from outside the individual. Different forms of rewards commonly represent extrinsic motivations (Lai and Chen, 2014). Intrinsic motivation is derived from an interest or satisfaction in conducting the task that is not based on desire for reward, or from any external pressure. Intrinsic motivations are predominantly influenced by pleasure and satisfaction (Shibchurn and Yan, 2015). This pleasure can come from curiosity satisfaction (Wang and Hou, 2015) or from self-worth (KwangWook and Ravichandran, 2011). These motivational factors can shed light for management to improve information security knowledge sharing in organizations.

The results also revealed that information security collaboration influences employees' attitude towards complying with organizational information security policies. Collaboration refers to working together in order to achieve a goal; this goal could be establishing a secure environment for information assets. Management can improve information security collaboration by providing organizational support to these kinds of activities. Organizational support refers to the extent to which the organization acknowledges and values the employees' contribution and cares about their well-being (Shropshire et al., 2015). This could be a guideline for management to improve information security collaboration in their respective organizations.

This study suggests that management can increase ISOP compliance by encouraging their employees to share knowledge and collaborate in the domain of information security. Providing adequate training also has a significant effect on employees' compliance with ISOP. Training courses, formal presentations, posters, workshops, emails, webpages, meetings, pens, and games can all form part of different training approaches. Proper information security training heightens the information security awareness, which is a key factor in information security assurance. Another outcome of this research is related to information security experience that has a significant effect on individuals' attitude towards ISOP compliance. Information security experience is the knowledge or mastery required to safeguard information assets that stem from empirical activities over time. This experience leads to a deep understanding of issues, and it changes attitudes towards compliance with ISOP.

In the context of this study, the outcomes showed a lack of support for the impact of attachment on attitudes towards compliance with ISOP. We mentioned employees' interest and benefit for this discord. Nevertheless, whenever possible, management should encourage and promote organizational bonding with respect to information security concerns. Regular group

meetings on such matters may be one means of doing so. Adherence to social norms and values requires an extensive socialization process in any organization. When such a socialization is achieved, favourable outcomes for compliance with ISOP may ensue.

Commitment to the organizational goals, rules and regulations comprises commitment to safeguard informational assets. The results of statistical analysis support the effect of commitment on attitudes towards compliance with ISOP. This can also be a guideline for the management of organizations. Personal norms refer to the employees' beliefs, values and views. Personal norms can have a significant effect on the subjective norms in organizations, a fact which should be taken into consideration by management.

There were limitations to this study. The samples in this study were collected from companies that have established suitable information security policies in Malaysia. One of the limitations is the paucity of organizations that have established information security policies in order to mitigate the risk of information breaches in their institutions. It is a hard task to obtain permission from organizations for surveys and data collections in the domain of information security; however, the generalization of findings can be improved with a bigger sample size and more companies for investigation. The data collection was conducted in Malaysia. This could be extended to other countries as well. Another important limitation stems from the inability to control double responses by participants that fill out the electronic questionnaire. Such concerns could be addressed by controlling the respondents' IP address. In this way, we can detect participants with two or more responses.

This research provides a testable research conceptualization that other researchers could further develop. This study can continue with investigations on the differences in compliance with organizational information security policies and the procedures based on gender, age (teen, youth, adults, etc.), level of education, job style, and so forth. Organizational culture, trust, interpersonal and team characteristics, motivational factors, and incentives could also be investigated in this domain. One possible area of interest might be to apply the constructs in this study and use the other perspectives in order to extend the literature to develop comprehensive and integrative models for assessing ISOP compliance in organizations. Awareness plays a vital role in mitigating the risk of information security breaches. Organizational learning perspectives might well be an interesting and effective subject for further research in complying with ISOP.

REFERENCES

Abawajy J. User preference of cyber security awareness delivery methods. Behav Inf Technol 2014;33(3):236–47. doi:10.1080/0144929X.2012.708787.

Ahmad A, Hadgkiss J, Ruighaver AB. Incident response teams – Challenges in supporting the organisational security function. Comput Secur 2012;31(5):643–52. doi:10.1016/j.cose.2012.04.001.

Akhunzada A, Sookhak M, Anuar NB, Gani A, Ahmed E, Shiraz M, et al. Man-At-The-End attacks: analysis, taxonomy, human aspects, motivation and future directions. J Netw Comput Appl 2015;48(0):44–57. http://dx.doi.org/10.1016/j.jnca.2014.10.009.

Albrechtsen E. A qualitative study of users' view on information security. Comput Secur 2007;26(4):276–89. http://dx.doi.org/10.1016/j.cose.2006.11.004.

Albrechtsen E, Hovden J. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Comput Secur 2010;29(4):432–45. http://dx.doi.org/10.1016/j.cose.2009.12.005.

AlHogail A. Design and validation of information security culture framework. Comput Human Behav 2015;49(0):567–75. http://dx.doi.org/10.1016/j.chb.2015.03.054.

Arachchilage NAG, Love S. Security awareness of computer users: a phishing threat avoidance perspective. Comput Human Behav 2014;38(0):304–12. http://dx.doi.org/10.1016/j.chb.2014.05.046.

Arbuckle JL. Amos 16.0 user's guide. Chicago (IL): SPSS, Inc; 2007.

Ashenden D. Information security management: a human challenge? Inform Secur Tech Rep 2008;13(4):195–201. http://dx.doi.org/10.1016/j.istr.2008.10.006.

Bagozzi RP, Yi Y. Specification, evaluation, and interpretation of structural equation models. J Acad Market Sci 2011;40:8–34. doi:10.1007/s11747-011-0278-x.

Ben-Asher N, Gonzalez C. Effects of cyber security knowledge on attack detection. Comput Human Behav 2015;48(0):51–61. http://dx.doi.org/10.1016/j.chb.2015.01.039.

Bernard R. Information lifecycle security risk assessment: a tool for closing security gaps. Comput Secur 2007;26(1):26–30. http://dx.doi.org/10.1016/j.cose.2006.12.005.

Caputo DD, Pfleeger SL, Freeman JD, Johnson ME. Going spear phishing: exploring embedded training and awareness. IEEE Secur Priv 2014;12(1):28–38. doi:10.1109/MSP.2013.106.

Casper WJ, Harris CM. Work-life benefits and organizational attachment: self-interest utility and signaling theory models. J Vocat Behav 2008;72(1):95–109. http://dx.doi.org/10.1016/j.jvb.2007.10.015.

Chapple CL, McQuillan JA, Berdahl TA. Gender, social bonds, and delinquency: a comparison of boys' and girls' models. Soc Sci Res 2005;34(2):357–83. http://dx.doi.org/10.1016/j.ssresearch.2004.04.003.

Cheng L, Li Y, Li W, Holm E, Zhai Q. Understanding the violation of IS security policy in organizations: an integrated model based on social control and deterrence theory. Comput Secur 2013;39(Pt B):447–59. http://dx.doi.org/10.1016/j.cose.2013.09.009.

Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville R. Future directions for behavioral information security research. Comput Secur 2013;32(0):90–101. http://dx.doi.org/10.1016/j.cose.2012.09.010.

Feledi D, Fenz S, Lechner L. Toward web-based information security knowledge sharing. Inform Secur Tech Rep 2013;17(4):199–209. http://dx.doi.org/10.1016/j.istr.2013.03.004.

Furnell S, Clarke N. Power to the people? The evolving recognition of human aspects of security. Comput Secur 2012;31(8):983–8. http://dx.doi.org/10.1016/j.cose.2012.08.004.

Gaur A. Statistical methods for practice and research. SAGE; 2009.

Habibpor K, Safari R. 2008. *Comprehensive guide for using SPSS software and data analysis*.

Hair JF, Black WC, Babin BJ, Anderson RE, editors. Multivariate data analysis. 7th ed. 2010.

Hepler J. A good thing isn't always a good thing: dispositional attitudes predict non-normative judgments. Pers Individ Dif 2015;75(0):59–63. http://dx.doi.org/10.1016/j.paid.2014.11.016.

Herath T, Rao HR. Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. Decis Support Syst 2009;47(2):154–65. http://dx.doi.org/10.1016/j.dss.2009.02.005.

Hirschi T. Causes of delinquency. University of California Press; 1969.
Ifinedo P. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput Secur 2012;31(1):83–95. http://dx.doi.org/10.1016/j.cose.2011.10.007.
Ifinedo P. Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. Inf Manage 2014;51(1):69–79. http://dx.doi.org/10.1016/j.im.2013.10.001.
Kim DW, Yan P, Zhang J. Detecting fake anti-virus software distribution webpages. Comput Secur 2015;49(0):95–106. http://dx.doi.org/10.1016/j.cose.2014.11.008.
Kritzinger E, von Solms SH. Cyber security for home users: a new way of protection through awareness enforcement. Comput Secur 2010;29(8):840–7. http://dx.doi.org/10.1016/j.cose.2010.08.001.
KwangWook G, Ravichandran T. 2011, 4-7 Jan.). *Accessing External Knowledge: Intention of Knowledge Exchange in Virtual Community of Practice*. Paper presented at the System Sciences (HICSS), 2011 44th Hawaii International Conference on.
Lai H-M, Chen TT. Knowledge sharing in interest online communities: a comparison of posters and lurkers. Comput Human Behav 2014;35(0):295–306. http://dx.doi.org/10.1016/j.chb.2014.02.004.
Lee G, Lee WJ, Sanford C. A motivational approach to information providing: a resource exchange perspective. Comput Human Behav 2011;27(1):440–8. http://dx.doi.org/10.1016/j.chb.2010.09.006.
Lee SM, Lee S-G, Yoo S. An integrative model of computer abuse based on social control and general deterrence theories. Inf Manage 2004;41(6):707–18. http://dx.doi.org/10.1016/j.im.2003.08.008.
Lee Y, Kozar KA. Investigating factors affecting the adoption of anti-spyware systems. Commun ACM 2005;48(8):72–7. doi:10.1145/1076211.1076243.
Li H, Zhang J, Sarathy R. Understanding compliance with internet use policy from the perspective of rational choice theory. Decis Support Syst 2010;48(4):635–45. http://dx.doi.org/10.1016/j.dss.2009.12.005.
Mace JC, Parkin S, Moorsel AV. 2010. A Collaborative Ontology Development Tool for Information Security Managers. Proceedings of the 4th Symposium on Computer Human Interaction for the Management of Information Technology.
Mesch GS. Social bonds and internet pornographic exposure among adolescents. J Adolesc 2009;32(3):601–18. http://dx.doi.org/10.1016/j.adolescence.2008.06.004.
Ng B-Y, Kankanhalli A, Xu Y. Studying users' computer security behavior: a health belief perspective. Decis Support Syst 2009;46(4):815–25. http://dx.doi.org/10.1016/j.dss.2008.11.010.
Parsons K, McCormac A, Butavicius M, Pattinson M, Jerram C. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Comput Secur 2014;42:165–76. http://dx.doi.org/10.1016/j.cose.2013.12.003.
Rhee H-S, Kim C, Ryu YU. Self-efficacy in information security: its influence on end users' information security practice behavior. Comput Secur 2009;28(8):816–26. http://dx.doi.org/10.1016/j.cose.2009.05.008.
Rocha Flores W, Antonsen E, Ekstedt M. Information security knowledge sharing in organizations: investigating the effect of behavioral information security governance and national culture. Comput Secur 2014;43(0):90–110. http://dx.doi.org/10.1016/j.cose.2014.03.004.
Safa NS, Ismail MA. A customer loyalty formation model in electronic commerce. Econ Model 2013;35(0):559–64. http://dx.doi.org/10.1016/j.econmod.2013.08.011.
Safa NS, Ghani NA, Ismail MA. An artificial neural network classification approach for improving accuracy of customer identification in e-commerce. Malays J Comput Sci 2014;27(3):171–85.
Safa NS, Sookhak M, Von Solms R, Furnell S, Ghani NA, Herawan T. Information security conscious care behaviour formation in organizations. Comput Secur 2015;53(0):65–78. http://dx.doi.org/10.1016/j.cose.2015.05.012.
Schumacker RE, Lomax RG. A beginner's guide to structural equation modeling. 3rd ed. New York: Taylor & Francis Group; 2010.
Shaw RS, Chen CC, Harris AL, Huang H-J. The impact of information richness on information security awareness training effectiveness. Comput Educ 2009;52(1):92–100. http://dx.doi.org/10.1016/j.compedu.2008.06.011.
Shibchurn J, Yan X. Information disclosure on social networking sites: an intrinsic–extrinsic motivation perspective. Comput Human Behav 2015;44(0):103–17. http://dx.doi.org/10.1016/j.chb.2014.10.059.
Shropshire J, Warkentin M, Sharma S. Personality, attitudes, and intentions: predicting initial adoption of information security behavior. Comput Secur 2015;49(0):177–91. http://dx.doi.org/10.1016/j.cose.2015.01.002.
Siponen M, Adam Mahmood M, Pahnila S. Employees' adherence to information security policies: an exploratory field study. Inf Manage 2014;51(2):217–24. http://dx.doi.org/10.1016/j.im.2013.08.006.
Son J-Y. Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. Inf Manage 2011;48(7):296–302. http://dx.doi.org/10.1016/j.im.2011.07.002.
Stanton JM, Stam KR, Mastrangelo P, Jolton J. Analysis of end user security behaviors. Comput Secur 2005;24(2):124–33. http://dx.doi.org/10.1016/j.cose.2004.07.001.
Tamjidyamcholo A, Sapiyan Bin Baba M. Evaluation model for knowledge sharing in information security professional virtual community. Comput Secur 2014;http://dx.doi.org/10.1016/j.cose.2014.02.010.
Tamjidyamcholo A, Bin Baba MS, Shuib NLM, Rohani VA. Evaluation model for knowledge sharing in information security professional virtual community. Comput Secur 2014;43(0):19–34. http://dx.doi.org/10.1016/j.cose.2014.02.010.
Van Niekerk JF, Von Solms R. Information security culture: a management perspective. Comput Secur 2010;29(4):476–86. http://dx.doi.org/10.1016/j.cose.2009.10.005.
Vance A, Siponen M, Pahnila S. Motivating IS security compliance: insights from habit and protection motivation theory. Inf Manage 2012;49(3–4):190–8. http://dx.doi.org/10.1016/j.im.2012.04.002.
Veenstra R, Lindenberg S, Tinga F, Orme J. Truancy in late elementary and early secondary education: the influence of social bonds and self-control – the TRAILS study. Int J Behav Dev 2010;302–10. doi:10.1177/0165025409347987.
Von Solms R, Van Niekerk J. From information security to cyber security. Comput Secur 2013;38(0):97–102. http://dx.doi.org/10.1016/j.cose.2013.04.004.
Vroom C, von Solms R. Towards information security behavioural compliance. Comput Secur 2004;23(3):191–8. http://dx.doi.org/10.1016/j.cose.2004.01.012.
Wang S, Noe RA. Knowledge sharing: a review and directions for future research. Hum Resour Manage Rev 2010;20(2):115–31. http://dx.doi.org/10.1016/j.hrmr.2009.10.001.
Wang W-T, Hou Y-P. Motivations of employees' knowledge sharing behaviors: a self-determination perspective. Information and Organization 2015;25(1):1–26. http://dx.doi.org/10.1016/j.infoandorg.2014.11.001.
Webb J, Ahmad A, Maynard SB, Shanks G. A situation awareness model for information security risk management. Comput

Secur 2014;44(0):1–15. http://dx.doi.org/10.1016/j.cose.2014.04.005.
Werlinger R, Hawkey K, Botta D, Beznosov K. Security practitioners in context: their activities and interactions with other stakeholders within organizations. Int J Hum Comput Stud 2009;67(7):584–606. http://dx.doi.org/10.1016/j.ijhcs.2009.03.002.
Witherspoon CL, Bergner J, Cockrell C, Stone DN. Antecedents of organizational knowledge sharing: a meta-analysis and critique. J Knowl Manag 2013;17(2):250–77. doi:10.1108/13673271311315204.
Woon IMY, Kankanhalli A. Investigation of IS professionals' intention to practise secure development of applications. Int J Hum Comput Stud 2007;65(1):29–41. http://dx.doi.org/10.1016/j.ijhcs.2006.08.003.
Zhai Q, Lindorff M, Cooper B. Workplace Guanxi: its dispositional antecedents and mediating role in the affectivity–job satisfaction relationship. J Bus Ethics 2013;117(3):541–51. doi:10.1007/s10551-012-1544-7.

Steven Furnell is a professor of Information Systems Security and leads the Centre for Security, Communications and Network Research at Plymouth University, United Kingdom. He is also an Adjunct Professor with Edith Cowan University in Western Australia. His research interests include usability of security and privacy technologies, security management and culture, and technologies for user authentication and intrusion detection. Furnell is the BCS representative to Technical Committee 11 (security and privacy) within the International Federation for Information Processing, and is a member of related working groups on security management, security education, and human aspects of security.

Rossouw Von Solms is a professor and director of the Centre for Research in Information and Cyber Security, School of ICT, Nelson Mandela Metropolitan University (NMMU), Port Elizabeth, South Africa. He supervises many PhD and postdoctoral students in the field of Information Security and IT Governance. Rossouw has published and presented in excess of one hundred and fifty academic papers in journals and conferences, both internationally and nationally. Most of these papers were published and presented in the field of Information Security.

Nader Sohrabi Safa is a postdoctoral fellow in the Centre for Research in Information and Cyber Security, School of ICT, Nelson Mandela Metropolitan University (NMMU), Port Elizabeth, South Africa. He received his PhD degree in Information Systems in 2014 from the Faculty of Computer Science and Information Technology, University of Malaya. His research interest is in the domain of human interaction with systems and human aspects of information security. He received his bachelor's degree in Software Engineering in 1999 and master's degree in Industrial Engineering-System Productivity and Management in 2005.