COMPUTERS & SECURITY 53 (2015) 65–78

Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Information security conscious care behaviour formation in organizations

Nader Sohrabi Safa [a,*], Mehdi Sookhak [a,1], Rossouw Von Solms [b,2], Steven Furnell [c,3], Norjihan Abdul Ghani [a,4], Tutut Herawan [a,5]

[a] Department of Information Science, Faculty of Computer Science & Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia

[b] Centre for Research in Information and Cyber Security, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa

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

ARTICLE INFO

Article history:
Received 29 November 2014
Received in revised form
25 April 2015
Accepted 25 May 2015
Available online 3 June 2015

Keywords:
Information security
Conscious care behaviour
Awareness
Risk
Organization policy

ABSTRACT

Today, the Internet can be considered to be a basic commodity, similar to electricity, without which many businesses simply cannot operate. However, information security for both private and business aspects is important. Experts believe that technology cannot solely guarantee a secure environment for information. Users' behaviour should be considered as an important factor in this domain. The Internet is a huge network with great potential for information security breaches. Hackers use different methods to change confidentiality, integrity, and the availability of information in line with their benefits, while users intentionally or through negligence are a great threat for information security. Sharing their account information, downloading any software from the Internet, writing passwords on sticky paper, and using social security numbers as a username or password are examples of their mistakes. Users' negligence, ignorance, lack of awareness, mischievous, apathy and resistance are usually the reasons for security breaches. Users' poor information security behaviour is the main problem in this domain and the presented model endeavours to reduce the risk of users' behaviour in this realm. The results of structural equation modelling (SEM) showed that Information Security Awareness, Information Security Organization Policy, Information Security Experience and Involvement, Attitude towards information security, Subjective Norms, Threat Appraisal, and Information Security Self-efficacy have a positive effect on users' behaviour. However, Perceived Behavioural Control does not affect their behaviour significantly. The Protection Motivation Theory and Theory of Planned Behaviour were applied as the backbone of the research model.

* *Corresponding author*. Tel.: +60 102402372.
E-mail addresses: sohrabisafa@yahoo.com (N.S. Safa), m.sookhak@ieee.org (M. Sookhak), Rossouw.VonSolms@nmmu.ac.za (R. Von Solms), S.Furnell@plymouth.ac.uk (S. Furnell), norjihan@um.edu.my (N.A. Ghani), tutut@um.edu.my (T. Herawan).
[1] Tel.: +60 177614849.
[2] Tel.: +27 415049604.
[3] Tel.: +44 1752586234.
[4] Tel.: +60 125432935.
[5] Tel.: +60 142723760.

http://dx.doi.org/10.1016/j.cose.2015.05.012
0167-4048/

1. Introduction

Advances in web-based oriented technologies and services are taking place with significant speed around the world. However, information security is still a prevalent issue among experts as well as users. Companies and their e-Customers are concerned about cyber-attacks, and, consequently, are keen to minimize information security risk (Safa and Ismail, 2013). The Internet is a vast network and has great potential for threats. Online attackers use new and different methods for achieving security breaches. Recently, hackers have developed a fake website and asked users to download free antivirus software from their website. Many users downloaded the antivirus software from these fake websites and lost their private information (Kim et al., 2015). Technology and the threat environment change frequently, and are dynamic due to their nature. For instance, the Internet of Things (IoT) shows the vast number of new applications on the Internet that connects devices, systems, services and even smart objects, and covers a variety of protocols, domains, and applications. These changes make it difficult to anticipate and quantify the information security risk (Pfleeger and Caputo, 2012). Conscious care behaviour is an effective approach to counter creative attacks. Conscious care behaviour means that users think about the consequences of their actions in terms of information security when they work with a system, particularly on the Internet. Information security awareness, knowledge and experience play vital roles in this domain. Rhee et al. (2009) asserted that information security risk management encompasses two aspects: 1) security software and features, such as pop-up blocking function, anti-spyware, and anti-virus software; 2) security conscious care behaviour related to computer and Internet usage.

Experts believe that the technology aspects of information security cannot solely guarantee a secure environment and that human information security behaviour should be taken into consideration (Furnell and Clarke, 2012). The importance of human factors in the domain of information security cannot be understated. Information security management should consider users and their perceptions as important factors to provide a secure environment. In other words, users are the centre of the security concept. Mitigating and preventing cyber security risks need to be implemented in several stages, and behavioural science plays an important role in the stages of the design, development and maintenance of web systems (Padayachee, 2012). Users consider security as an obstacle when there is no appropriate response to their cyber incidents. They may be faced with difficulties in security implementation, and misinterpret, mistrust or override the security (Cox, 2012). Users' attitudes and their resistance behaviour change when they face a mandatory password change. Researchers have realized that such changes are intentionally delayed and are considered an unnecessary interruption. They know that a password breach can have severe consequences, but do not change their attitude towards the implementation of a security policy (Stanton et al., 2005). Users, intentionally or through negligence, are an important threat to information security, in which careless information security behaviour is the main problem. This research aims to change users' behaviour to conscious care behaviour in the domain of information security.

The remainder of this paper is organised as follows. Section two presents two fundamental theories, the Theory of Planned Behaviour (TPB) and the Protection Motivation Theory (PMT), as the background of this research. Different parts of the model and hypotheses are then discussed in section three. The research methodology describes the stages of problem solving and is presented in section four. Data analysis and the results of the measurement model and structural model are discussed in section five. The contribution and implementation of the research are presented in section six, and, finally, overall conclusions and thoughts towards future work can be found in section seven.

2. Theoretical background

Human behaviour can change based on one's attitude, which is a salient point that we applied to change information security behaviour to conscious care behaviour. Behaviour is driven by behavioural intention where the behavioural intention is a function of an individual's attitude towards the behaviour (Ajzen and Madden, 1986). The Theory of Planned Behaviour (TPB) and Protection Motivation Theory (PMT) are the backbone of the research model and explain how the users' behaviour can change to conscious care behaviour.

2.1. *Theory of planned behaviour*

Ajzen (1991) proposed the Theory of Planned Behaviour (TPB) to explain the influence of attitude, subjective norms, and perceived behavioural control upon individual behaviour. The TPB has been widely applied in diverse studies to predict individuals' behaviour. Attitude refers to the users' positive or negative feeling towards a particular behaviour, and is defined as a learned tendency to evaluate things in a particular way. The evaluation can be positive or negative about an object, issue, people or events (Leonard et al., 2004). Once the evaluation changes, attitude, and, consequently, behaviour change. Attitude can also be implicit or explicit. In explicit attitude, we are consciously aware, which influences our beliefs and behaviour. In contrast, implicit attitude unconsciously affects our behaviour and beliefs (Albrechtsen and Hovden, 2010). Human knowledge has a direct effect on one's attitude. This effect comes from our direct personal experience or the result of our observations. Different training methods also change our attitude towards certain issues (Abawajy, 2014). Information security awareness of risks influences the attitude towards behaviour in the users (Bryce and Fraser, 2014; Dinev and Hu, 2007). Ifinedo (2014) showed that attitude, subjective norms, and perceived behavioural control influence users' intention to comply with information security organization policies.

In this research, the presented model shows that information security awareness influences the attitude towards having a careful manner in terms of information security behaviour. Subjective norms lead to social pressure on individuals to perform or not perform a behaviour and refer to the users' perception of what people important to them think.

Their supervisor, head of department, managers are important people to whom information security policies are important due to the importance of information assets to an organization. That is why we conjecture that information security organizational policies affect subjective norms towards conscious care behaviour. Perceived behavioural control refers to the individual's perceived ease or difficulty in performing a special behaviour. Users' experience and involvement influence users' perception that having a careful manner is not a difficult task in the domain of information security. Fig. 1 shows the effect of the aforementioned factors on individuals' behaviour based on the Theory of Planned Behaviour.

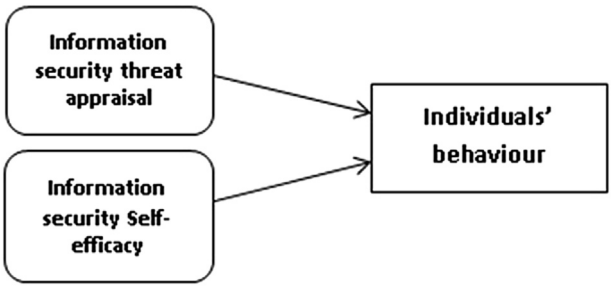

Fig. 2 – The effect of factors based on Protection Motivation Theory.

2.2. *Protection Motivation Theory*

The Protection Motivation Theory (PMT) is one of the most powerful explanatory theories for predicting users' intention to engage in protective actions (Anderson and Agarwal, 2010). Information about the threats plays an important role in the cognition of risk. PMT has been applied in different studies. Rogers (1983) applied this theory to better understand fear appeals and how individuals cope with them. The cognitive processing and expectancy-value theories are fundamental parts of this theory. Threat appraisal and coping appraisal are two main parts of this theory. Threat appraisal relates to users' assessment of the level of risk that results from having a careless manner in terms of information security. This risk can threaten availability, integrity, and confidentiality of information. The perceived vulnerability and severity of the risk are two important sections of threat appraisal. Coping appraisal refers to the users' ability to cope with the risk or threat (Woon and Kankanhalli, 2007). Self-efficacy refers to users' abilities and capabilities to cope with or perform the recommended behaviour. In the context of this study, it refers to user behaviour in such a manner that the risk of information security breach is minimized. Ifinedo (2014); Lee and Larsen (2009); Woon and Kankanhalli (2007) applied PMT in order to show how compliance with information security organizational policy reduced the risk of users' behaviour. We used this theory to show that if users think about the consequences of their manner in terms of information security before taking any action and consider the level of damage and cost that might be incurred, they will behave carefully. Fig. 2 shows the effect of information security threat appraisal and self-efficacy on individuals' behaviour based on the Protection Motivation Theory.

3. Research model and hypotheses

This research aims to mitigate the risk of information security breaches by emphasizing the human aspects of information security. We developed a new multi-theory based model that explains how information security conscious care behaviour (ISCCB) forms among information security and technology employees. Conscious care behaviour has been acknowledged to be an effective approach to reduce the risk of information security incidents in organizations (Rhee et al., 2009). Information security awareness (Furnell and Clarke, 2012), organizational information security policies (Siponen et al., 2014), and individuals' experience and involvement (Albrechtsen, 2007) are three main factors in this research. The Theory of Planned Behaviour and Protection Motivation Theory are two fundamental theories that have been used to justify the effect of the above-mentioned factors on information security conscious care behaviour. Further explanation about the different parts of the model is presented in the following sections.

3.1. *Information security awareness (ISA)*

Awareness is a key factor in information security assurance. Suitable information security training is required to improve users' awareness that leads to secure behaviour. Training courses, workshops, formal presentations, Internet pages,

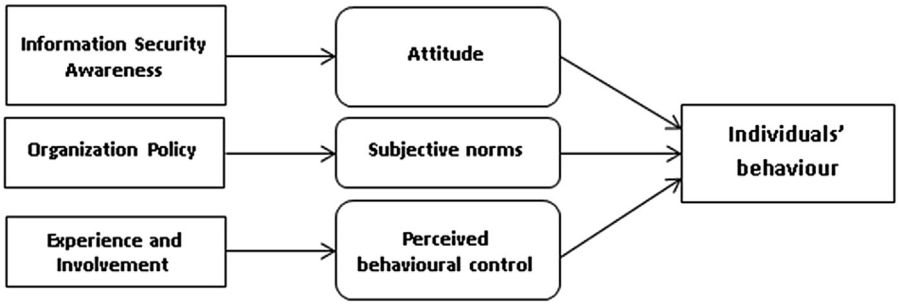

Fig. 1 – The effect of factors based on the Theory of Planned Behaviour.

e-mails, screen savers, posters, pens, games and meetings are among the ways that experts can improve the knowledge of users' information security (Albrechtsen and Hovden, 2010). Information security awareness discusses the security awareness programme that leads to security positive behaviour as a key factor. Information security is defined as the perception of the importance of information security by users or members, their responsibilities, the level of information security appropriate to the organization and their acts (Kruger and Kearney, 2006). The combination of procedural and technical controls is imperative in the management of information security to reduce the risk, and people are central to this process. Controls can be abused or circumvented by users that ignore security procedures or policies. Everybody should understand and engage in secure behaviour to have a secure environment. Changing the perception or culture of users to a positive information security culture is not easy or straightforward (Son, 2011). Risk and threat frequently change; information security awareness is a dynamic process, and, consequently, awareness programmes should be updated. To keep customers updated, awareness programmes should be an integral part of organizational culture. Relevant and consistent programmes are the key to success in information security awareness. Information security awareness, and keeping up to date in terms of the methods that attackers may use, plays an important role in reducing the risk of information security breaches (Allam et al., 2014). Information security knowledge sharing, intervention (different training methods) and collaboration are three factors that heighten the users' awareness and affect users' attitude and their behaviour (Abawajy, 2014; Feledi et al., 2013; Tamjidyamcholo et al., 2014). This research aims to show that information security awareness changes the users' attitude towards performing information security conscious care behaviour.

H1: Information security awareness has a positive effect on attitude towards performing ISCCB.

3.2. *Information Security Organization Policy (ISOP)*

Information security is extremely important in most organizations in terms of business and individual data. Although most organizations use technology and spend money on anti-spyware, anti-virus, anti-malware and other technology tools, it is well known that technology tools alone are not sufficient (Ashenden, 2008; Chu and Chau, 2014; Herath and Rao, 2009). Users should care about their manner in terms of information security (Da Veiga and Eloff, 2010). Users' information security behaviour is a new challenge for organizations. Experts have divided users to home and organization groups. Kritzinger and von Solms (2010) believe that information security awareness support by firms and enforcement component reduce the risk of information security breaches in organizations. Herath and Rao (2009) investigated the role of penalties, pressure and the perceived effectiveness of employee action in information security organization policies. Intrinsic and extrinsic motivations affect employees' behaviour towards compliance with organization security policies. The results of their study showed that the pressures exerted by subjective norms and peer behaviour influence employees' information security behaviour. Penalties also have a significant effect on security behaviour. Furnell and Thomson (2009) investigated information security culture and mentioned that corporate culture is an important aspect of organization and has a positive effect on information security. The shared tacit assumptions of employees, as well as their corresponding beliefs and values, play an important role in the information security behaviour of the organization when they are in line with the organization's security policies. Information security policies and procedures should be clear and understandable for staff. Promoting good user behaviour and constraining bad user behaviour can be an effective policy in the organizations (Stanton et al., 2005). Subjective norms reflect the impact the opinions of significant others have on individuals' decisions. In an organization, there is pressure on employees to follow the information security policies that are supported by management, heads of department, and even co-workers (significant others) (Cheng et al., 2013), because information is considered an important asset that should be safeguarded by employees. This pressure affects employees' information security behaviour in organizations.

H2: Organizational policies have a positive effect on subjective norms towards performing ISCCB.

3.3. *Information security experience and involvement (ISEI)*

Involvement shows how much thought, time, energy and other resources are devoted to the main issue by users. Researchers have mentioned the involvement concept in various behaviour models. Involvement explains the relationship between two entities based on different variables. The level of involvement that impacts on the users' decision can be low, medium or high (Huang et al., 2010). Involvement has been considered to be an important factor in different research domains. Frías et al. (2008) studied the factors that influence customers' motivation or image formation regarding product. The results of their research revealed that there is a significant difference between the high and medium involvement groups in terms of their behaviour. The outcomes also explained how the level of involvement has a significant moderate effect on the customers' perception. Park and Lee (2008) discussed consumer behaviour intention based on their involvement with products, in which customers' involvement was explored based on customers' goal directedness. Participants with a high level of involvement read and process the information of products more carefully while customers with low involvement do not. These are samples of involvement in the different areas. Involvement has been acknowledged in different researches to be an important factor that influences user perception and the intention to make a decision for a particular purpose. Information security involvement means information security participation and engagement. Ifinedo (2014) investigated individuals' involvement in the organizational activities and policies in the domain of information security. The results showed that information security involvement positively affects users'

attitudes towards information security policy compliance. Perceived behavioural control refers to the perceived ease or difficulty in performing a behaviour (Woon and Kankanhalli, 2007). Perceived behavioural control is defined as the employee's beliefs regarding the efficacy and resources needed to facilitate behaviour. We also adopt this concept in the information security domain. Information security involvement is defined as the time, effort and energy that users spend to ensure a secure information environment. Their information security experience and involvement affect employees' beliefs about the ease of performing conscious care behaviour. The hypothesis presented below is based on the aforementioned factors:

H3: Users' experience and involvement have a positive effect on perceived behavioural control towards performing ISCCB.

3.4. Attitude, subjective norms and perceived behavioural control

Attitude is an important factor that influences individual's emotion and behaviour. Attitude is a favourable or unfavourable expression towards an object. The object can be an event, person, thing, place, idea, or activity. Positive or negative evaluation forms attitude. The attitude varies from extremely negative to extremely positive. Attitude is a main item in the TPB. The TPB explains the relationship between beliefs and behaviour. Ajzen (1991) improved the Theory of Reasoned Action (TRA) by adding perceived behavioural control. TPB has been applied to explain the relation among beliefs, attitude, behavioural intentions, and, finally, behaviour in a wide range of research. Based on the TRA, if somebody evaluates a behaviour positively (attitude), and if he or she thinks other important persons want them to perform it (subjective norms), this leads to motivation and they are more likely to do it. However, there are arguments against the relationship between behavioural intention and actual behaviour, inasmuch as behavioural intention does not always lead to actual behaviour. This means that behavioural intention cannot be an exclusive item of behaviour when a person's control over the behaviour is incomplete. Ajzen added perceived behavioural control and extended the TRA to explain non-volitional behaviour. Ifinedo (2014) asserted that information security awareness has a significant effect on individuals' attitude towards information security. Subjective norms refer to the perceived social pressure to perform (or not perform) the behaviour in question. It reflects the impact the opinions of significant others have on an individual's decisions. In an information security setting, employees feel the pressure to meet their significant others (such as the immediate supervisors and co-workers) and organization's expectations and policies (Cheng et al., 2013). Therefore, subjective norms can be affected by information security organizational policies. Perceived behavioural control refers to the perception of ease or difficulty in performing a task or behaviour. Albrechtsen (2007) mentioned users' information security experience and involvement as an important factor that affects their perceptions about performing information security behaviour. Based on the aforementioned factors we considered these hypotheses in this research:

H4: Attitude towards information security has a positive effect on performing ISCCB.
H5: Subjective norms have a positive effect on performing ISCCB.
H6: Perceived behavioural control has a positive effect on performing ISCCB.

3.5. Threat appraisal

Threat refers to the possibility and severity of danger. It can be the probability of losing something of value. Value can be social status, financial wealth, physical health, emotional wellbeing and business or private information. Threat relates to intentional interaction with uncertainty. Risk perception is the person's judgement about the severity of the risk. Threat involves the exposure of private information and is not just bound to a possible financial or even identity loss. Customers trust less and have more concern when they find it difficult to control the unauthorized distribution or misuse of their business or private information, which leads to the perception of uncertainty and hesitation to disclose personal information (Liao et al., 2011).

The Protection Motivation Theory (PMT) is one of the most powerful explanatory theories for predicting users' intention to engage in protective actions (Anderson and Agarwal, 2010). Threat and coping appraisal are two main parts of this theory. Threat appraisal is the user's assessment about the level of danger posed by a threatening event. Threat appraisal contains perceived vulnerability and perceived severity. The coping appraisal refers to the users' assessment of his or her ability to cope with and avert the potential loss or damage of information arising from the threat. Self-efficacy, response-efficacy, and response cost affect coping appraisals (Ifinedo, 2012).

In recent research, threat appraisal has been considered to be an important factor that affects individuals' perception and changes their behaviour towards compliance with information security policies in the organization (Lee and Larsen, 2009; Siponen et al., 2014). In this research, threat appraisal is considered to be an important factor that influences customers' perception about information security towards ISCCB.

H7: Threat appraisal has a positive effect on performing ISCCB.

3.6. Information security self-efficacy (ISSe)

Self-efficacy (SE) is a form of self-evaluation, which is a proximal determination of human behaviour. SE refers to an individual's belief in their ability to organize action based on motivation and cognitive resources (Beas and Salanova, 2006). Users with a high level of SE possess a high level of SE about the successful implementation of a task. SE affects the measure of effort, self-regulation, persistence or initiation of coping efforts in the face of problems (Hasan, 2003). Computer

self-efficacy (CSe) refers to the user's judgement of their capability to use computers to achieve a particular purpose. CSe relates to users' computing behaviour, such as adaptation of information, software learning, contributing to system development and ethical computer usage (Potosky, 2002). Experts emphasize that the domain specificity of SE should be considered in order to increase the predictability of SE in performance. Task self-efficacy refers to the efficacy belief in performing computer tasks within the general domain of computing.

Coping appraisal is one of the important elements of the Protection Motivation Theory that refers to the individual's capability and ability to implement secure behaviour in the domain of information security. In this research, the general definition of CSe was adapted to the information security context. Protection of system, information, store and transmit information is in the concept of information security. Therefore, a belief in the ability to protect information and system from unauthorized disclosure, loss, modification, destruction, and lack of availability refers to self-efficacy in information security. In this study, information security self-efficacy is considered to be an important factor that leads to security conscious care behaviour.

H8: Information security self-efficacy has a positive effect on performing ISCCB.

Fig. 3 shows the research model in a concise form.

4. Research methodology

This research aims to mitigate the risk of information security incidents based on individuals' behaviour. The root of the problem is poor information security behaviour. The lack of awareness, negligence, carelessness, inability and non-involvement are the symptoms of the main problem (Albrechtsen and Hovden, 2010; Furnell et al., 2012; Shaw et al., 2009). Framing the problem allows it to be structured in the proper context, and to identify the resources and potential solutions that may need to be employed (Safa et al., 2014). A systematic problem solving approach was applied in this research. This approach avoids mere intuitive judgement, and ensures that the researchers consider all aspects of the issue to solve the problem.

Information security conscious care behaviour is an effective approach to reduce the risk of information security breaches. When a user is faced with a suspicious email that asks him/her to change his/her username or password, user awareness and knowledge about phishing sends the first alarm to his/her mind. The user starts to think about the consequences of changing the username and password through the email. Based on organizational information security policy, employees should not reply to this kind of email, because any change of username and password should be conducted through the official website. In an organization where all staff respect the information security policy, subjective norms can be a positive factor in ensuring secure information security behaviour. In addition, a user's previous information security experience and involvement warn him/her to be careful about behaviour that could lead to a security breach. In this regard, this research aims to examine whether:

- information security awareness changes users' attitudes;
- organization policy in the domain of information security influences subjective norms;
- information security experience and involvement affects users in performing information security conscious care behaviour; and
- assessment of information security threat and information security self-efficacy have a positive effect on information security conscious care behaviour.

Qualitative and quantitative approaches have been applied in this research. In the first step, the effective factors have been collected from a literature review in this domain. Interviews with experts as well as applying the Delphi method improved the results of the previous steps, and, finally, the research model was developed.

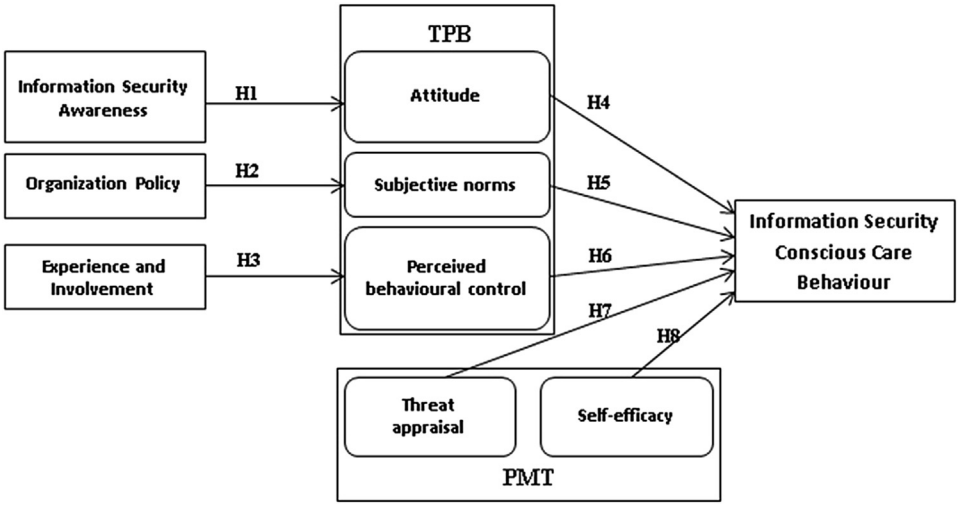

Fig. 3 – Formation of information security conscious care behaviour.

Confirmatory factor analysis was applied to test whether the measurement model is consistent with our understanding of the nature of that factor or construct. In other words, to test whether the data fit the hypothesized measurement model. The hypothesized model in this research is based on two fundamental theories (TPB and PMT).

Due to the probability of existence of multi relationships among the independent, dependent, mediating, and variables, structural equation modelling (SEM) is considered to be the most appropriate method to explore the research model (Zweig and Webster, 2003). Because SEM examines the overall data fit to the hypothesized model, SEM was applied in this research. The measurement model and structural model were assessed by IBM Amos 20 using the maximum likelihood method. To assess the fit of the model, Chi-square with degrees of freedom, the goodness of fit index (GFI), the comparative fit index (CFI), the adjusted goodness of fit index (AGFI), and root mean square error of approximation (RMSEA) were applied (Hair et al., 2010).

4.1. *Data collection*

This research focuses on two groups of participants: Information Security Experts and Information Technology Professionals in Malaysian organizations due to their familiarity with the research subject. A person with extensive knowledge in the domain of information security based on research, education, experience and occupation is an expert in this research. A preliminary version of the questionnaire was pilot-tested. The participants reviewed the questionnaire in the presence of the main author and provided feedback regarding wording, understandability, and applicability of the instrument. The original questionnaire was based on a seven-point Likert scale. However, participants in the pilot test indicated that a five-point scale would be more comfortable to answer, since they tended to avoid the extreme points.

The participants were asked to complete the questionnaires based on their experience and knowledge. We explained the aim of the research to them and informed them that the data would be kept confidential and only used for academic purposes. After expression of their consent, we presented the questionnaire to them. Pilot testing with 32 questionnaires showed that the participants understood and interpreted the questions correctly and consistently. The final version of the questionnaire included forty-three questions, in which, every construct was measured by several items. Although, the main subject of this research is novel, the presented model has some common constructs with other resent studies (Hartono et al., 2014; Ifinedo, 2014; Siponen et al., 2014; Tamjidyamcholo et al., 2014). The items and questions were adopted from these studies. The coverage of items in the final version is as shown in Table 1.

In the next step, two hundred and twenty questionnaires, based on a five-point Likert scale (1-strongly disagree to 5-strongly agree), were used to measure every construct by the items. To decrease the number of incomplete questionnaires, the participants' responses were reviewed immediately after completion and they were asked to reply to the neglected questions. Nevertheless, eight questionnaires (4%) were discarded due to incomplete answers or because the same response was given to all items. The facilities in Google Drive were also used to create a questionnaire form and were emailed to some of the participants. Their responses were collected automatically in Google Drive. In this method, participants can reply to the questionnaire at any time and the place and data collection is more comfortable for researchers. In order to speed up data gathering, parallel to the electronic data gathering, data were also collected using a paper-based survey.

Table 1 – Distribution of constructs and survey items.

Construct	No. of related items
Information security awareness	5
Information security organizational policy	4
Information security experience and involvement	6
Attitude toward performing information security conscious care behaviour	6
Subjective norms	4
Perceived behavioural control	4
Threat appraisal	5
Information security self-efficacy	4
Information security conscious care behaviour	5

4.2. *Demography*

Finally, two hundred and twelve questionnaires remained for data analysis, of which, 51.4% were from male respondents and 48.6% were from female respondents. The gender was relatively equal. Approximately 46.2% of participants were experts in information security and 53.8% were information technology professionals (e.g. roles, such as systems analyst, designer, developer, and so on). Telecommunication and information technology, finance and insurance, retail, healthcare, education, and hotel are the domains of the participants' jobs. The participants' data show diversity in terms of experience, education, age, and gender. Table 2 shows the demography of the participants in a concise form.

5. Results

The variables of interest are usually latent (unobservable) variables, such as Information Security Awareness, Self-efficacy, Risk Perception, Experience and Involvement, and Organization Policy. These unobservable variables can be modelled using a measurement model and structural model. The measurement model shows the relationship between the observed indicators and the latent variables while the structural equation model specifies the relationships amongst the unobserved variables (Chang and Chen, 2008). The measurement model and structural model are two important parts of the data analysis.

5.1. *Measurement model*

To explore the multiple relationships between the dependent, mediating, and independent variables, structural equation

Table 2 – Participants' demography.

Demography	Category	Frequency	Per cent
Gender	Male	109	51.4
	Female	103	48.6
Focus Group	Information security Experts	98	46.2
	Information technology Experts	114	53.8
Industry	Telecom/IT	86	40.57
	Finance/Insurance	48	22.64
	Retail	36	16.98
	Healthcare	25	11.79
	Education	11	5.19
	Hotel	6	2.83
Availability of formal security policies	Yes	158	74.5
	No	48	22.6
	I don't know	6	2.9
Work experience	1–5	98	46.2
	5–10	65	30.7
	More than 10 year	49	23.1
Education	PhD	32	15
	Master	70	33.1
	Bachelor	110	51.9
Age	20–29	45	21.2
	30–39	68	32.1
	40–49	52	24.5
	50 above	47	22.2

modelling (SEM) is the most suitable approach to address the research question. This is because SEM tests the overall data fit to the hypothesized model and estimates the relationships among the variables. SEM is a combination of the measurement model and structural regression model. The measurement model defines latent variables using several observed variables. The structural regression model links latent variables together. The advantage of using SEM is the isolation of observational error from the measurement of latent variables. In the first step, the normality of data distribution was tested using the standard skewness and kurtosis tests. The results were between −2 and +2, which shows normal distribution (Gaur and Gaur, 2006). Confirmatory factor analysis (CFA) is a multivariate statistical procedure to test whether the measured variables are consistent with a researcher's understanding of the nature of the factor or construct. In this kind of study, the research model is usually developed based on previous research and fundamental theories in the respective domain. The CFA approach was used since the model was developed based on the theoretical background and literature review.

To assess the convergent validity, the factor loading of the measurement variables were calculated. Hair and Anderson (2010) contended that factor loadings greater than 0.5 show acceptable convergent validity. Hence, the items with factor loadings less than 0.5 were dropped from the model. ISA5 in the information security awareness construct, ISEI4 in the information security experience and involvement, and ATT5 in the attitude construct were omitted due to a lower factor loading on the mentioned constructs. Internal consistency shows the correlations among the items that measure a construct. Cronbach's Alpha is a measure of internal consistency. Internal consistency for every construct was tested by calculating Cronbach's Alpha. All the measures of Cronbach's Alpha exceeded the threshold of 0.7, which shows the composite reliability of the constructs (Hair et al., 2010). Table 3 provides a summary of the measurement scale in a concise form.

The discriminant validity of the items was tested by calculating the correlations between all pairs of constructs. The correlations between all pairs of constructs were less than 0.9, which shows the discriminant validity of the constructs (Siponen et al., 2014). Table 4 shows the results for discriminant validity.

5.2. *Testing the structural model*

Structural Equation Modelling (SEM) was applied to address the relationships among the independent, dependent, moderating, and mediating variables. SEM examines the overall data fit to the conceptual model and considers reliable measurement when estimating the relationships among variables. The maximum likelihood method in IBM Amos version 20 was applied to estimate the model's parameters. This approach shows how much the data matches the model based on different measures.

Two different fit characteristics were applied to explore the fit indices: the global fit measures and comparative fit measures. The Chi-square test (χ^2) with degrees of freedom is commonly used as the global model fit criteria. Chi-Square and Chi-square/df also indicates the extent to which the data are compatible with the hypothesis. Data with a better fit with the model show a small Chi-Square value and a Chi-square/df ratio of 2 or less. The Chi-square statistic is sensitive to sample size. The hypothesized model may be rejected due to a large sample size. Fortunately, the sample size (212 samples) is adequate for this test. The Goodness of Fit (GFI) measures the fit between the observed or actual data (covariance or correlation) matrix and that predicted from the proposed model. The Adjusted Goodness of Fit Index (AGFI) is

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

Construct		Items	Mean	Std Dev	CFA Loading	Composite reliability
Information Security Awareness (ISA)	ISA1	I am aware of potential security threat.	4.21	0.751	0.651	0.784
	ISA2	I have sufficient knowledge about the cost of information security breaches.	4.11	0.794	0.582	
	ISA3	I understand the risk of information security incidents.	3.95	0.797	0.685	
	ISA4	I keep myself updated in terms of information security awareness.	3.56	0.802	0.695	
	ISA5	I share information security knowledge to increase my awareness.	4.21	0.695	Dropped	
Information Security Organization Policy (ISOP)	ISOP1	Information security policies and procedures are important in my organization.	4.25	0.859	0.710	0.804
	ISOP2	Information security policies and procedures affect my behaviour.	4.31	0.795	0.527	
	ISOP3	Information security policies and procedures have attracted my attention.	4.11	0.864	0.742	
	ISOP4	Behaviour in line with organizational information security policies and procedures is of value in my organization.	3.79	0.793	0.774	
Information Security Experience and Involvement (ISEI)	ISEI1	My experience increases my ability to have a safe behaviour in terms of information security.	4.05	0.761	0.756	0.751
	ISEI2	I am involved with information security and I care about my behaviour in my job.	4.03	0.719	0.805	
	ISEI3	My experience helps me to recognize and assess information security threats.	3.93	0.861	0.851	
	ISEI4	I can sense the level of information security threat due to my experience in this domain.	3.58	0.762	Dropped	
	ISEI5	My experience helps me to perform information security conscious care behaviour.	3.84	0.805	0.806	
	ISEI6	I have suitable capability in order to manage information security risk due to my experience.	4.22	0.812	0.855	
Attitude (ATT)	ATT1	Information security conscious care behaviour is necessary.	3.91	0.705	0.721	0.829
	ATT2	Information security conscious care behaviour is beneficial.	4.07	0.874	0.601	
	ATT3	Practicing information security conscious care behaviour is useful.	3.67	0.816	0.772	
	ATT4	I have a positive view about changing users' information security behaviour to conscious care.	4.41	0.924	0.823	
	ATT5	My attitude towards information security conscious care behaviour is favourable.	4.01	0.953	Dropped	
	ATT6	I believe that information security conscious care behaviour is valuable in an organization.	3.98	0.764	0.718	
Subjective Norms (SN)	SN1	Information security policies in my organization are important for my colleagues.	3.92	0.949	0.685	0.767
	SN2	My colleagues' information security behaviour influences my behaviour.	3.65	0.915	0.754	
	SN3	Information security culture in my organization influences my behaviour.	4.41	0.848	0.799	
	SN4	My boss's information security behaviour influences my behaviour.	3.68	0.868	0.683	

(*continued on next page*)

Table 3 – (*continued*)

Construct		Items	Mean	Std Dev	CFA Loading	Composite reliability
Perceived Behavioural Control (PBC)	PBC1	I believe that information security conscious care behaviour is not a difficult practice.	4.18	0.759	0.851	0.862
	PBC2	I believe that my experiences help me to have a careful behaviour about information security.	3.86	0.858	0.762	
	PBC3	Following information security policies and procedures is easy for me.	3.74	0.708	0.676	
	PBC4	Information security conscious care behaviour is an achievable practice.	4.13	0.894	0.901	
Threat Appraisal (TA)	TA1	I know the probability of security breach increases if I do not consider information security policies.	3.65	0.816	0.864	0.720
	TA2	I could fall victim to different kinds of attack if I do not follow information security policies.	3.87	0.880	0.812	
	TA3	The security of my data will be weak if I do not consider information security policies.	4.17	0.922	0.609	
	TA4	Hackers attack with different methods and I should be careful in this dynamic environment.	4.13	0.739	0.714	
	TA5	To reduce the risk I do not open unexpected and out-of context email.	4.16	0.675	0.817	
Information Security Self-efficacy (ISSe)	ISSe1	I have the skills to protect my business and private data.	3.94	0.683	0.923	0.805
	ISSe2	I have the expertise to protect my business and private data.	4.01	0.542	0.754	
	ISSe3	I think the protection of my data is in my control in terms of information security violations.	4.23	0.742	0.699	
	ISSe4	I have the ability to prevent information security violations.	3.69	0.865	0.783	
Information Security Conscious Care Behaviour (ISCCB)	ISCCB1	I consider security experts recommendations in my information security manner.	3.85	0.915	0.821	0.756
	ISCCB2	Before taking any action that affects information security, I think about its consequences.	3.56	0.972	0.762	
	ISCCB3	I talk with security experts before I do something that relates to information security.	4.11	0.753	0.658	
	ISCCB4	I consider my previous experience in information security to avoid repeating prior mistakes.	3.98	0.832	0.598	
	ISCCB5	I always try to change my habits to security conscious behaviour.	4.07	0.806	0.706	

Factor loading from confirmatory factor analysis.
t-value is significant at $p < 0.05$.

Table 4 – Correlation matrices and discriminant validity.

		Mean	SD	1	2	3	4	5	6	7	8	9
1	ISA	3.95	1.23	0.818								
2	ISOP	4.11	0.87	0.520	0.758							
3	ISEI	4.01	0.95	0.301	0.612	0.769						
4	AT	4.00	1.21	0.509	0.386	0.412	0.739					
5	SN	3.91	1.12	0.289	0.294	0.197	0.365	0.714				
6	PBC	3.97	1.30	0.186	0.265	0.268	0.267	0.208	0.872			
7	TA	3.99	0.98	0.234	0.521	0.442	0.236	0.194	0.369	0.708		
8	SE	3.96	1.23	0.198	0.230	0.196	0.267	0.203	0.295	0.375	0.712	
9	ISCCB	3.91	1.32	0.326	0.316	0.267	0.196	0.197	0.246	0.261	0.203	0.823

Table 5 – Fit indices of the model.

Fit indices	Model value	Acceptable standard
χ^2	1006.89	–
χ^2/Df	1.89	<2
GFI	0.963	>0.9
AGFI	0.936	>0.9
CFI	0.921	>0.9
IFI	0.914	>0.9
NFI	0.938	>0.9
RMSEA	0.072	<0.08

GFI that considers the degrees of freedom. The Comparative Fit Index (CFI) compares the data against the null model. A CFI with a value greater than 0.9 is recommended by researchers (Byrne, 1994; Schumacker and Lomax, 2010). The Incremental Fit Index (IFI) is a useful complement measure that evaluates the model by considering discrepancy and the degrees of freedom. An IFI value close to 1 indicates a very good fit. The Normed Fit Index (NFI) shows minimum discrepancy of the baseline model with the data. In other words, an NFI with a value of 1 shows that the model fits the observed data perfectly. The Root Mean Square Error of Approximation (RMSEA) is another measure that addresses the error approximation and answers the question of "how well does the model fit the population covariance matrix?" An RMSEA with a value less than 0.08 is considered good (Bagozzi and Yi, 2011; Hair et al., 2010). The RMSEA, GFI and AGFI values also show that the hypothesized model provides a good fit with the data. Table 5 shows the model fit indices.

The results of the hypotheses tests are presented in Table 6. The findings show that the path from information security awareness towards attitude ($\beta = 0.641$, $p = 0.012$), from information security organization policies to subjective norms ($\beta = 0.567$,$p = 0.004$), from experience and involvement to perceived behavioural control ($\beta = 0.503$, $p = 0.024$), and information security attitude ($\beta = 0.716$, $p = 0.011$), subjective norms ($\beta = 0.624$, $p = 0.006$), threat appraisal ($\beta = 0.531$, $p = 0.001$), and self-efficacy ($\beta = 0.617$, $p = 0.031$) towards ISCCB were significant. However, the effect of perceived behavioural control on ISCCB was not significant; therefore, hypothesis H6 is rejected.

6. Contribution and implementation

To the best of our knowledge, this is one of the first studies that discusses users' conscious care behaviour formation in the domain of information security as an effective approach to improve information security behaviour in organizations. In a dynamic environment, such as the Internet, with a great potential for security breaches, the prevention of information security incidents seems to be an effective and efficient approach. In this research, we showed how information security conscious care behaviour forms based on information security awareness, organization policies and procedures, and users' experience and involvement. This can guide management and experts to improve information security behaviour in their organizations.

Two advantages exist in this approach: firstly, the Internet is a wide environment in which hackers use different and new methods based on users' mistakes. Proper information security behaviour, or, in other words, information security conscious care behaviour, decreases the employees' behavioural mistakes. Secondly, the technological aspects of information security alone cannot guarantee information security. Considering the technological aspects of information security besides performing information security conscious care behaviour is the most effective approach in this domain. The other significant aspect of this research is derived from the application of two fundamental theories – Theory of Planned Behaviour and Protection Motivation Theory. These theories explain how information security awareness, organization policies and procedures, and users' experiences and involvement affect their information security behaviour.

The results of data analysis showed that information security awareness has a significant effect on attitude towards the formation of information security conscious care behaviour. This finding is in line with the finding in the research of (Haeussinger and Kranz, 2013). Subjective norms in organizations refer to employees' perceptions of what their colleagues think is important to them about a given information security behaviour. The results of statistical analysis revealed that an organization's information security policy has a positive effect on subjective norms towards performing information security conscious care behaviour. A possible reason for this finding can be the effect of information security policies that should be followed by employees in organizations. This can create a mandatory condition for staff to perform in a proper manner to safeguard the information assets. This finding also confirms the results in the research of (Cheng et al., 2013). As confirmed by the results of other research (Tøndel et al., 2014), experience and involvement are shown to have a significant effect on perceived behaviour control. This indicates that experience and involvement affect the perceived ease of performing information security conscious

Table 6 – Results of the hypotheses tests.

Path			Standardized estimate	S.E.	*p*-Value	Results
ISA	→	AT	0.641	0.097	0.012	Support
ISOP	→	SN	0.567	0.121	0.004	Support
ISEI	→	PBC	0.503	0.086	0.024	Support
AT	→	ISCCB	0.716	0.101	0.011	Support
SN	→	ISCCB	0.624	0.082	0.006	Support
PBC	→	ISCCB	0.514	0.189	0.601	Not-Supported
TA	→	ISCCB	0.531	0.221	0.001	Support
SE	→	ISCCB	0.617	0.134	0.031	Support

care by employees in organizations. One plausible explanation for this finding might be that participants have had adequate experience in the domain of information technology and information security. However, the results showed that perceived behavioural control does not have a significant effect on information security conscious care behaviour. One conceivable explanation for this finding might be that the information security domain is a vast and challenging one, thus having perceived ease of performance cannot lead to conscious care behaviour on its own. The relationships between attitude and subjective norms towards ISCCB were found to be positive, which is in line with the results of other research (Cox, 2012; Ifinedo, 2014; Siponen et al., 2014). Information security assessment and self-efficacy are two main factors in PMT; the results of data analysis in this part revealed that threat appraisal and self-efficacy have a significant effect on performing information security conscious care behaviour. These findings confirm the results of other studies (Padayachee, 2012; Vance et al., 2012).

Management should deliver the message that an information security breach is plausible and that such threats can lead to the vulnerability of the organization and the disclosure of private information. Keeping employees updated in terms of information security and increasing their knowledge in this domain have a significant effect on their behaviour. In addition, ensuring the availability of information security policies and procedures is another effective approach to preventing information security breaches. Information security policies and procedures should be clear, concise, and easy to understand for all employees.

7. Conclusion

In this research, we presented a novel model that shows how information security conscious care behaviour forms, based on information security awareness, organizational policies, experience and involvement, attitude, subjective norms, threat appraisal and self-efficacy. Information security conscious care behaviour decreases the risk of information breaches when the area of weakness is human behaviour. The consciousness aspect of users' behaviour plays a vital role, while the reasons for many information security breaches are related to users' ignorance, negligence, lack of awareness, mischievousness, apathy, and resistance. To change information security behaviour, awareness plays an important role. The results of this study show that awareness has a significant effect on users' information security attitude towards conscious care behaviour. Proper information security policies also have an important effect on the formation of subjective norms towards information security behaviour within organizations. The outcomes show that information security experience and involvement affect perceived behavioural control, but that perceived behavioural control does not significantly affect user conscious care behaviour. In addition, information security threat appraisal and self-efficacy can have a significant and direct effect on conscious care behaviour.

There were some limitations to this research. Many of the employees in the organizations were not familiar with some of the concepts used in our research, such as information security behaviour, the tricks that hackers use based on users' mistakes, phishing, information security breaches by social engineering and so on. To produce more reliable results, we asked information security and information technology experts in the organizations to answer our questionnaire due to their greater familiarity with these concepts. This is one of the limitations of our research that was unavoidable. Generalization of the findings can be improved in future research.

In future studies, the proposed conceptual framework can be improved with a greater focus on awareness as a basic element in the prevention of security breaches. The conceptualization of users' experience and observation in this domain has a deep effect on their attitude, and, in the next step, on their behaviour (Konak et al., 2014), which can provide a guide for future studies. Knowledge sharing, intervention (different training methods), and collaboration in the domain of information security are also subjects that can be considered for new research. Information security policies can contain encouragement (reward) or hindrance (penalty) aspects. Individuals have a different personality and attitude. There is limited research in this domain that shows which one of these policies is recommended for different users with different attitudes and personalities. Applying unsuitable policies can reflect unpredictable results that may be hard to compensate. This can also be a relevant cue for future research.

REFERENCES

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

Ajzen Icek. Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behaviour. J Appl Soc Psychol 1991;32:1–20.

Ajzen Icek, Madden Thomas J. Prediction of goal-directed behavior: attitudes, intentions, and perceived behavioral control. J Exp Soc Psychol 1986;22(5):453–74. http://dx.doi.org/10.1016/0022-1031(86. http://dx.doi.org/10.1016/0022-1031(86)90045-4.

Albrechtsen Eirik. 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 Eirik, Hovden Jan. 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.

Allam S, Flowerday SV, Flowerday E. Smartphone information security awareness: a victim of operational pressures. Comput Secur 2014;42:55–65. http://dx.doi.org/10.1016/j.cose.2014.01.005.

Anderson Catherine L, Agarwal Ritu. Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions. MIS Q 2010;34(3):613–43.

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

Bagozzi Richard P, Yi Youjae. Specification, evaluation, and interpretation of structural equation models. Acad Mark Sci 2011;40:8–34. http://dx.doi.org/10.1007/s11747-011-0278-x.

Beas Maria Isabel, Salanova Marisa. Self-efficacy beliefs, computer training and psychological well-being among information and communication technology workers. Comput Hum Behav 2006;22(6):1043–58. http://dx.doi.org/10.1016/j.chb.2004.03.027.

Bryce J, Fraser J. The role of disclosure of personal information in the evaluation of risk and trust in young peoples' online interactions. Comput Hum Behav 2014;30:299–306. http://dx.doi.org/10.1016/j.chb.2013.09.012.

Byrne Barbara M. Structural equation modeling with EQS and EQS-windows: basic concepts, applications, and programming. Thousand Oaks, CA, USA: Sage Publications, Inc; 1994.

Chang Hsin Hsin, Chen Su Wen. The impact of customer interface quality, satisfaction and switching costs on e-loyalty: Internet experience as a moderator. Comput Hum Behav 2008;24(6):2927–44. http://dx.doi.org/10.1016/j.chb.2008.04.014.

Cheng Lijiao, Li Ying, Li Wenli, Holm Eric, Zhai Qingguo. Understanding the violation of IS security policy in organizations: an integrated model based on social control and deterrence theory. Comput Secur 2013;39(Part B(0)):447–59. http://dx.doi.org/10.1016/j.cose.2013.09.009.

Chu Amanda MY, Chau Patrick YK. Development and validation of instruments of information security deviant behavior. Decis Support Syst 2014;66(0):93–101. http://dx.doi.org/10.1016/j.dss.2014.06.008.

Cox James. Information systems user security: a structured model of the knowing–doing gap. Comput Hum Behav 2012;28(5):1849–58. http://dx.doi.org/10.1016/j.chb.2012.05.003.

Da Veiga A, Eloff JHP. A framework and assessment instrument for information security culture. Comput Secur 2010;29(2):196–207. http://dx.doi.org/10.1016/j.cose.2009.09.002.

Dinev Tamara, Hu Qing. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. J Assoc Inf. Syst 2007;8:386–408.

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

Frías Dolores Ma, Rodríguez Miguel A, Castañeda J Alberto. Internet vs. travel agencies on pre-visit destination image formation: an information processing view. Tour Manag 2008;29(1):163–79. http://dx.doi.org/10.1016/j.tourman.2007.02.020.

Furnell Steven, Clarke Nathan. 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.

Furnell Steven, Thomson Kerry-Lynn. From culture to disobedience: recognising the varying user acceptance of IT security. Comput Fraud Secur 2009;2009(2):5–10. http://dx.doi.org/10.1016/S1361-3723(09. http://dx.doi.org/10.1016/S1361-3723(09)70019-3.

Gaur Ajai, Gaur Sanjaya. Statistical methods for practice and research. London: SAGE Publications Inc; 2006.

Haeussinger Felix J, Kranz Johann J. Information security Awareness: Its antecedents and mediating effects on security compliant behavior. In: Paper presented at the International Conference on Information Systems 2013; 2013.

Hair Joseph, Anderson Rolph. Multivariate data analysis. 6th ed. Prentice Hall Higher Education; 2010.

Hair Jr Joseph F, Black William C, Babin Barry J, Anderson Rolph E. Multivariate data analysis. New Jersey: Pearson Prentice Hall; 2010.

Hartono Edward, Holsapple Clyde W, Kim Ki-Yoon, Na Kwan-Sik, Simpson James T. Measuring perceived security in B2C electronic commerce website usage: a respecification and validation. Decis Support Syst 2014;62(0):11–21. http://dx.doi.org/10.1016/j.dss.2014.02.006.

Hasan Bassam. The influence of specific computer experiences on computer self-efficacy beliefs. Comput Hum Behav 2003;19(4):443–50. http://dx.doi.org/10.1016/S0747-5632(02. http://dx.doi.org/10.1016/S0747-5632(02)00079-1.

Herath Tejaswini, 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.

Huang Ching-Yuan, Chou Chia-Jung, Lin Pei-Ching. Involvement theory in constructing bloggers' intention to purchase travel products. Tour Manag 2010;31(4):513–26. http://dx.doi.org/10.1016/j.tourman.2009.06.003.

Ifinedo Princely. 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 Princely. Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. Inf Manag 2014;51(1):69–79. http://dx.doi.org/10.1016/j.im.2013.10.001.

Kim Dae Wook, Yan Peiying, Zhang Junjie. 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.

Konak Abdullah, Clark Tricia K, Nasereddin Mahdi. Using Kolb's experiential learning cycle to improve student learning in virtual computer laboratories. Comput Educ 2014;72(0):11–22. http://dx.doi.org/10.1016/j.compedu.2013.10.013.

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.

Kruger HA, Kearney WD. A prototype for assessing information security awareness. Comput Secur 2006;25(4):289–96. http://dx.doi.org/10.1016/j.cose.2006.02.008.

Lee Younghwa, Larsen Kai R. Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. Eur J Inf Syst 2009;18:177–87. http://dx.doi.org/10.1057/ejis.2009.11.

Leonard Lori NK, Cronan Timothy Paul, Kreie Jennifer. What influences IT ethical behavior intentions—planned behavior, reasoned action, perceived importance, or individual characteristics? Inf Manag 2004;42(1):143–58. http://dx.doi.org/10.1016/j.im.2003.12.008.

Liao Chechen, Liu Chuang-Chun, Chen Kuanchin. Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: an integrated model. Electron Commer Res Appl 2011;10(6):702–15. http://dx.doi.org/10.1016/j.elerap.2011.07.003.

Padayachee Keshnee. Taxonomy of compliant information security behavior. Comput Secur 2012;31(5):673–80. http://dx.doi.org/10.1016/j.cose.2012.04.004.

Park Do-Hyung, Lee Jumin. eWOM overload and its effect on consumer behavioral intention depending on consumer involvement. Electron Commer Res Appl 2008;7(4):386–98. http://dx.doi.org/10.1016/j.elerap.2007.11.004.

Pfleeger Shari Lawrence, Caputo Deanna D. Leveraging behavioral science to mitigate cyber security risk. Comput Secur 2012;31(4):597–611. http://dx.doi.org/10.1016/j.cose.2011.12.010.

Potosky Denise. A field study of computer efficacy beliefs as an outcome of training: the role of computer playfulness, computer knowledge, and performance during training. Comput Hum Behav 2002;18(3):241–55. http://dx.doi.org/10.1016/S0747-5632(01. http://dx.doi.org/10.1016/S0747-5632(01)00050-4.

Rhee Hyeun-Suk, Kim Cheongtag, Ryu Young U. 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.

Rogers RW. Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. New York: Guilford Press; 1983.

Safa Nader Sohrabi, Ismail Maizatul Akmar. 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 Nader Sohrabi, Ghani Norjihan Abdul, Ismail Maizatul Akmar. An artificial neural network classification approach for improving accuracy of customer identification in e-commerce. Malays J Comput Sci 2014;27(3):171–85.

Schumacker Randall E, Lomax Richard G. A Beginner's guide to structural equation modeling. 3rd ed. New York: Taylor & Francis Group; 2010.

Shaw RS, Chen Charlie C, Harris Albert L, Huang Hui-Jou. 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.

Siponen Mikko, Adam Mahmood M, Pahnila Seppo. Employees' adherence to information security policies: an exploratory field study. Inf Manag 2014;51(2):217–24. http://dx.doi.org/10.1016/j.im.2013.08.006.

Son Jai-Yeol. Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. Inf Manag 2011;48(7):296–302. http://dx.doi.org/10.1016/j.im.2011.07.002.

Stanton Jeffrey M, Stam Kathryn R, Mastrangelo Paul, Jolton Jeffrey. 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 Alireza, Bin Baba Mohd Sapiyan, Shuib Nor Liyana Mohd, Rohani Vala Ali. 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.

Tøndel Inger Anne, Line Maria B, Jaatun Martin Gilje. Information security incident management: current practice as reported in the literature. Comput Secur 2014;45(0):42–57. http://dx.doi.org/10.1016/j.cose.2014.05.003.

Vance Anthony, Siponen Mikko, Pahnila Seppo. Motivating is security compliance: Insights from Habit and Protection motivation theory. Inf Manag 2012;49(3–4):190–8. http://dx.doi.org/10.1016/j.im.2012.04.002.

Woon Irene MY, Kankanhalli Atreyi. Investigation of IS professionals' intention to practise secure development of applications. Int J Hum Comp Stud 2007;65(1):29–41. http://dx.doi.org/10.1016/j.ijhcs.2006.08.003.

Zweig David, Webster Jane. Personality as a moderator of monitoring acceptance. Comput Hum Behav 2003;19(4):479–93. http://dx.doi.org/10.1016/S0747-5632(02. http://dx.doi.org/10.1016/S0747-5632(02)00075-4.

Nader Sohrabi Safa received his PhD degree in Information systems in 2014 from 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 has taught different courses in the Labor university in Iran before he started his PhD. He received his bachelor degree in Software Engineering in 1999 and master degree in Industrial Engineering-System Productivity and Management in 2005. He has 15 years of experience in analysing, designing, and programming different systems with C# and SQL server.

Mehdi Sookhak received the B.Sc. degree in Software engineering from Shiraz University, Iran, in 2001 and master of computer science (Information Security) in 2012 from the Universiti Teknologi Malaysia (UTM). He is currently a Ph.D. candidate, research assistant in High Impact Research Project fully funded by Malaysian Ministry of Higher Education. His Ph.D. is sponsored by High Impact Research (HIR), the most prestigious scholarship in Malaysia. He is an active researcher in Center of Mobile Cloud Computing Research (C4MCC) at Faculty of Computer Science and Information Technology, University Malaya, Kuala Lumpur. His areas of interest include Cryptography and Information Security, Mobile Cloud Computing, Computation outsourcing, Access control, Wireless Sensor & Mobile Ad Hoc Network (Architectures, Protocols, Security, and Algorithms), and Distributed Systems

Rossouw von Solms is a Professor and director of Institute for ICT Advancement at Nelson Mandela Metropolitan University (NMMU). He supervises many students in the level of PhD and postdoctoral 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.

Steven Furnell is a Professor of information systems security and leads the Centre for Security, Communications and Network Research at Plymouth University. 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.

Norjihan Abdul Ghani is a Lecturer in the Faculty of Computer Science and Information Technology at department of Information System, university of Malaya. She is expert in database security and privacy, Information system, Electronic Commerce. She supervises several postgraduate students in master and PhD levels. She has many publications in different high quality journals in the domain of Access Control, E-commerce, Security, and Databases.

Tutut Herawan received PhD degree in computer science in 2010 from Universiti Tun Hussein Onn Malaysia. He is currently a senior lecturer at Department of Information System, University of Malaya. His research area includes rough and soft set theory, DMKDD, and decision support in information system. He has published more than 110 articles in various international journals and conference proceedings. He is an editorial board and act as a reviewer for various journals. He has also served as a program committee member and co-organizer for numerous international conferences and workshops.