Understanding human aspects for an effective information security management implementation.

Author(s)
Kör, Burcu; Metin, Bilgin

DOI
10.1504/IJADS.2021.10030447

Publication date
2021

Document Version
Final published version

Published in
International Journal of Applied Decision Sciences

Understanding human aspects for an effective information security management implementation

Article *in* International Journal of Applied Decision Sciences · June 2021

CITATIONS
0

READS
151

2 authors:

Burcu Kör
Amsterdam University of Applied Sciences/Centre for Applied Research on Education
20 PUBLICATIONS **112** CITATIONS
SEE PROFILE

Bilgin Metin
Bogazici University
99 PUBLICATIONS **1,041** CITATIONS
SEE PROFILE

Int. J. Applied Decision Sciences, Vol. 14, No. 2, 2021

Understanding human aspects for an effective information security management implementation

Burcu Kör
Amsterdam School of International Business,
Amsterdam University of Applied Science,
Amsterdam, Netherlands Email:
b.kor@hva.nl

Bilgin Metin*
Management Information Systems Department,
Bogazici University, Turkey
Email:bilgin.metin@boun.edu.tr *Corresponding
author

Abstract: In today's world, information security is a trending as well as a crucial topic for both individuals and organisations. Cyber attacks cause financial loss for businesses with data breaches and production loss. Data breaches can result in loss of reputation, reduced customer loyalty, and fines. Also, due to cyber attacks, business continuity is affected so that organisations cannot provide continuous production. Therefore, organisations should reduce cyber risks by managing their information security. For this purpose, they may use ISO/IEC 27001 information security management standard. ISO/IEC 27001:2013 includes 114 controls that are in both technical and organisational level. However, in the practice of security management, individuals' information security behaviour could be underestimated. Herein, technology alone cannot guarantee the safety of information assets in organisations, thereby a range of human aspects should be taken into consideration. In this study, the importance of security behaviour with respect to ISO/IEC 27001 information security management implementation is presented. The present study extensively analyses the data collected from a survey of 630 people. The results of reliability measures and confirmatory factor analysis support the scale of the study.

Keywords: information security; information security behaviour; information security policy; information security knowledge sharing; self-efficacy; information security training.

Reference to this paper should be made as follows: Kör, B. and Metin, B. (2021) 'Understanding human aspects for an effective information security management implementation', *Int. J. Applied Decision Sciences*, Vol. 14, No. 2, DOI: 10.1504/IJADS.2021.10030447.

Biographical notes: Burcu Kör is an Assistant Professor at Amsterdam School of International Business and researcher at Amsterdam University of Applied Science. She has various research interests, including entrepreneurship, knowledge management, innovation and cybersecurity. She holds a PhD in Management and Organisation from Istanbul University. In the scope of the PhD thesis study, she focused on the individual and contextual factors that affect innovative work behaviour. During the PhD period, she was a visiting

scholar at the University of Texas at Dallas and the Open University of the Netherlands. She is a visiting researcher at the Thapar School of Management in India.

Bilgin Metin is an Associate Professor in the Management Information Systems Department of Bogazici University in Istanbul, Turkey. His research interests include cybersecurity, information security management, IT governance and electronic circuit design for information systems. He has over 40 publications in SCI/SCIE indexed scientific journals and more than 50 papers in the international conference proceedings. He gave lectures at the Budapest University of Technology and Economics in 2014 as a part of Joint International Master in Smart Systems Integration (SSI). He is also currently a Manager of the Bogazici University MIS Cyber Security Center.

This paper is a revised and expanded version of a paper entitled 'Information security behaviour: the influence of organizational and individual factors' presented at 10th INEKA-Innovation, Entrepreneurship and Knowledge Academy Conference, Verona, Italy, 11–13 June 2019.

1 Introduction

In recent years, the rapid growth of the internet has brought lots of innovations, advantages and efficient solutions in all aspects of human life. It has clearly improved the level of productivity of humankind as it addresses all individuals in the world and has become a crucial part of human life that eases all processes (Alam et al., 2014; Bannister and Connolly, 2007). As the internet has become an integral asset in human life, not only organisational but also individual activities widely rely on online technologies. However, the incidence of cyber-attacks and security breaches have made information security a major concern for users, organisations, and nations (Safa and Von Solms, 2016; Albahar, 2017). For enterprises cyber attacks lead to data breaches that cause loss to reputation, reduced customer loyalty. The Ponemon Institute's cost of a data breach study in 2018 indicated that the average cost of a data breach worldwide was $3.86 million, a 6.4% increase over 2017. Even a negligible data breach may lead to a big impact. The report showed that the average cost per compromised record in 2018 was $148. Furthermore, cyber attacks exposed 2.8 billion consumer data records whose cost is more than $654 billion. Also, companies due to cyber attacks lose business continuity and suffer financial losses (Ponemon Institute, 2018). Recently, every information, data center, and even personal computers are somehow connected and reachable through the cyberspace in today's digitalised world. However, apart from the advantages of the internet, new vulnerabilities and security concerns emerged as the borders between countries have lost their significance (Langner, 2011; Dincelli, 2018). Therefore, the topic of information security has existed and became a rising issue for not only the organisational level but also the national level (Dincelli, 2018).

As people started to discover the vulnerabilities of the global network, cyber-crime has become a trending topic in the world. Just because the cost of buying a laptop and setting up internet connection is low and being able to be anonymous on the internet by using some particular tools such as VPN and proxy servers is easy; the number of cyber-attacks has been dramatically increasing. The motivation behind these malicious purposes may be political, gaining an economic advantage or more importantly causing damage to critical infrastructures of a country. Since critical infrastructures are becoming more dependent on information technologies day by day, their vulnerability in the cyberspace is posing a real threat to the communities (Langner, 2011). For instance, in 2012 a new form of virus,

'Stuxnet', has been exposed which was targeting Iranian nuclear facilities to cause significant damage to industrial machinery utilised for uranium enrichment [Lendvay, (2012), p.7]. The detection of the Stuxnet has proved that the viruses or in others say malicious software can cause real-world physical damage. Because of previous cyber incidents, now governments spend billions of dollars on information security. According to Gartner (2015), the world's leading information technology research and advisory company, in 2015, $75.4 billion was spent on information security by companies. However, the technical aspects of information security cannot solely guarantee a secure environment and it is still a controversial issue for users, organisations, and nations by including not only the protection of information resources but also that of other assets, including the person him/herself (Safa et al., 2015). Therefore, there is a requirement for a more holistic information security management approach including technological, organisational, national and social components (Kayworth and Whitten, 2010; Flores et al., 2014).

Experts state that nothing can guarantee any system's security whereas human involvement has to be taken into consideration since in most cases security vulnerability of companies is related to human ignorance and lack of awareness (Furnell and Clarke, 2012; Safa et al., 2015). At this point, individuals' information security behaviours play a significant role in having a secure environment within the cyberspace. Not only individuals but also the organisations can benefit reciprocally by enabling individuals' information security behaviour. However, Safa et al. (2015, p.66) argued that "the importance of human factors in the domain of information security cannot be understated." Herein, it is crucial to find out which individual and/or contextual factors motivate or enable individuals' information security behaviour. However, research on how to motivate appropriate information security behaviour is still at the nascent stage. Therefore, this study investigates a more holistic approach to find out which individual and/or organisational factors guide individuals' information security behaviour.

Additionally, given this call in the previous work, this study aims to contribute to a more holistic information security management approach, including individual and organisational factors. Building upon the substantial works of Safa et al. (2015), the present study aims to empirically examine information security behaviour relationships with individual and organisational factors: information security knowledge share, the intention of attending security training, self-efficacy and organisational information security policy.

As a summary, both technological and organisational control aspects play a critical role in information security, but both of these aspects are closely related to individuals' information security behaviour. For instance, opening an e-mail attachment without checking its source, sharing account information with other people and browsing websites without checking its reliability can be considered as common mistakes in information security behaviour. This study focused on individuals' behaviour dimensions of information security management by scrutinising its relationship with information security knowledge sharing, the information security policy of the organisation, the intention of attending information security training and self-efficacy for better information security management for organisations.

The present study extensively analyses the data collected from a survey of 630 people ranging from students to managers aged between 15 to 79 in order to generalise the Turkish context regarding information security management. The results of reliability measures and confirmatory factor analysis support the scale of the study. This study also shows practically the importance of security behaviour with respect to ISO/IEC 27001 information security management implementation.

The rest of this article is organised as follows. The next section presents a literature review and hypothesis development. Subsequently, the method and results are presented. The last section reveals the discussion and conclusion as well as the limitations and future research suggestions.

2 Theoretical background and hypothesis

2.1 Importance of individuals' security behaviour in information security management systems (ISMSs)

In recent years, information and communication technologies have been more accessible and convenient because of rapid development and lower costs in information and communication technologies. Accordingly, the number of internet users has exploded and corporations rely ever more on technology to run their businesses. As rapid progress in the use of the Internet and technological development have resulted in information security threats, which are becoming a major concern rather than an afterthought (Kruger and Kearney, 2006; Öğütçü et al., 2016). Von Solms and Van Niekerk (2013) defines information security as defending information from unauthorised access, disclosure, use, modification, disruption, inspection, and perusal. Von Solms and Van Niekerk (2013) also emphasise the importance of information confidentiality, integrity, and reliability within information security. Information security is also described as "mechanism by which computer-based equipment, information, and services are protected from illegal and unauthorized access" [Aggarwal et al., (2014), p.1].

In order to cope with the increasing cyber-attacks, an ISMS is required and it depicts an organisation's approach to information security. ISO/IEC 27001:2013 is the globally recognised best practice framework a set of standardised requirements for an ISMS (ISO/IEC 27001:2013, 2013). Implementing ISO/IEC 27001 will demonstrate to the customers, partners, regulatory authorities and other stakeholders that the company seriously deals with information security, identifies and manages the risks. The standard employs a process-based approach for establishing, implementing, operating, monitoring, maintaining, and improving your ISMS. In the ISMS implementations, employee's security behaviour should not be ignored while dealing with different procedures and documentation requirements of an ISMS.

In this study, we try to show information security behaviour related parts in ISO/IEC 27001:2013 standard and we employed related hypotheses to emphasise the importance of security behaviours in the implementation of ISMS.

ISO/IEC IEC 27001 for clause 7.2 basically says that the organisation will ensure that employees are competent on the basis of the relevant education, training or experience. Also, companies should determine the competence of person(s) doing work under its control that affects its information security performance. This clause is related to information security behaviour and self-efficacy, which is tested in Hypothesis 1.

ISO/IEC 27001 clause 7.3 states that employees shall be aware of the information security policy. This clause is related to the information security policy of the organisation and tested in Hypothesis 2.

In clause 7.4 of the main ISO/IEC 27001 requirements to demonstrate 'how' and how effective communication is to actually protect their organisation. It means that dynamic and assured communication for confidence in compliance is required specifically developed in close collaboration with end-users, a major part of the feature set in ISMS. Discuss and collaborate with team members on your policies and progress, and easily evidence it. Sharing and retaining knowledge becomes a breeze. This clause is related to information security knowledge sharing and tested with Hypothesis 3.

Especially ISO/IEC 27001:2013 Annex A 7.2.2 control requires that the employees of the organisation shall receive security awareness training and regularly this should be updated in the organisation. This part has handled the intention of attending the security educational training part of the study in Hypothesis 4.

In this study, we aim to investigate information security behaviour relevant aspects in ISO/IEC 27001:2013 standard and we have emphasised the importance of security behaviours in the implementation of ISMS through aforementioned individual and organisational factors.

2.2 Information security behaviour and self-efficacy

Padayachee (2012, p.673) defined information security behaviour as "a set of core information security activities that have to be adhered to by end-users to maintain

information security as defined by information security policies." Information security behaviour refers to the behaviours of individuals that are associated with protecting information and information systems assets including computer hardware, networking infrastructure, and organisational information (Fagnot, 2007; Stanton et al., 2006; Crossler et al., 2013). There is a growing body of literature where survey-based methodologies are used to measure information security behaviour, as well as there have been plenty of attempts to measure the information security awareness (Parsons et al., 2007). For instance, Mylonas et al. (2013) and Clarke et al. (2016) examined the security awareness of smartphone users, Stanton et al. (2005) examined empirically password-related behaviours, D'Arcy et al. (2009) conducted a survey of e-mail usage, and others have examined security awareness or behaviour on social media (e.g., Acquisti and Gross, 2006; Utz and Krämer, 2009). Galba et al. (2015, p.149) stated that "overall information security [is] significantly affected by an internet user's awareness, knowledge and behavior." In order to examine behaviours of the people regarding information security, Parsons et al. (2017) developed a survey instrument called HAIS-Q assessing different focus areas such as password management, e-mail use, internet use, social media use, mobile devices, information handling, and incident reporting. In line with the aforementioned literature, five focus areas of the items within the HAIS-Q (i.e., password management, e-mail use, internet use, social media use, mobile devices) were selected to measure the behaviour of people.

The term self-efficacy refers to an individual's belief in his/her ability to perform a specific task and it is an important set of determinants of motivation and action towards specific tasks (Bandura, 1977). According to Chai et al. (2006, p.128), "people who have higher levels of self-efficacy toward a specific subject are more like to give greater value to that subject." Previous researches show that students who have a strong cognitive competency toward statistics, they have more value for statistics (Wisenbaker et al., 2000), and children's task-specific beliefs regarding their ability influence how much more they are likely to value the specific task (Wigfield and Eccles, 2000). Derived from the general concept of self-efficacy, self-efficacy in information security is defined as an individual judgment or belief in one's capability to protect information and the systems that use, store, and transmit information, as well as to protect information systems from unauthorised disclosure, modification, loss, destruction, and lack of availability (Rhee et al., 2009). Based on the previous researches, it is assumed that individuals, who have a higher level of self-efficacy in information security, tend to develop a better perception of information security, as well as they have a strong motivation to implement information security behaviour. Self-efficacy in information security is improved by the acquired information regarding information security from training and self-improvement on the cyber security related topics. Previous research demonstrated that there is a relationship between self-efficacy and compliant behaviours of people with security guidelines and policies (Safa et al., 2015; Anwar et al., 2017). Therefore, this study proposes that there is a relationship between self-efficacy and information security behaviour. In light of the above discussion, the following hypothesis is proposed:

H_1 Self-efficacy in information security is positively related to information security behaviour.

2.3 The information security policy of the organisation

Intrinsic and extrinsic motivations affect individuals' behaviour towards compliance with organisational security policies. The role of penalties and pressure exerted by subjective norms and peer behaviour influences individuals' information security behaviour (Herath and Rao, 2009; Safa et al., 2015). Information security policy is defined as "a statement of the roles and responsibilities of the employees to safeguard the information and technology resources of their organizations" [Bulgurcu et al., (2010), pp.526–527]. According to Whitman (2008), information security policy also provides instructions to the individuals as to what they should do when they have specific security issues, as well as interact with the information and technology resources of their organisations. Abraham (2011) stated that understanding the behaviours of users that lead to compliance with security policies is an important feature of building successful security programs within the organisations. However, information security policies and procedures should be clear and understandable

for employees in order to comprise effective security policy within the organisations, thereby the risk of information security breaches in organisations can reduce through enforcement component (Kritzinger and von Solms, 2010; Safa et al., 2015). Employees' behaviour towards compliance with organisation security policies can be affected by intrinsic and extrinsic motivations (Herath and Rao, 2009). In other words, in an organisation, the pressure or the motivation on employees to follow the information security policies that are supported by management, heads of department, and even co-workers, turn to promote individuals' information security behaviour be enhanced (Safa et al., 2015). Parsons et al. (2007, p.41) asserted that "as computer users' level of knowledge of information security policy and procedures rises, their attitude towards information security policy and procedures improves, resulting in improved information security behavior." In light of the above discussion, the following hypothesis is proposed:

H_2 Information security policy of the organisation is positively related to information security behaviour.

2.4 Information security knowledge sharing

Knowledge sharing is considered as an important stage for implementing knowledge management successfully (Lee and Ahn, 2007). Knowledge sharing is defined as "the process by which an individual imparts his or her expertise, insight or understanding to another individual, so, that the recipient may potentially acquire and use the knowledge to perform his or her task(s) in a better way" [Sigala and Chalkiti, (2014), p.801]. As it is also mentioned by Ryu et al. (2003), knowledge is a connecting behaviour in which people try to gain knowledge from others. Knowledge sharing is manifested through both formal (e.g., education and policy communication), and informal (e.g., informal consulting and advisory services) means, and supported by the use of technology (e.g., intranet-based knowledge management systems) (Cummings, 2004; Rhodes et al., 2008; Flores et al., 2014). Accordingly, Wijnhoven (1998) maintained that information media is an important tool for knowledge conveyance in which recipients are able to add new knowledge to their existent knowledge. Interaction and information sharing among users via virtual space or cyberspace have increased incrementally by the impact of the rapid growth of the Internet and the use of information communication technologies (Tamjidyamcholo et al., 2014). Accordingly, home users are becoming more vulnerable to security threats. Herein, effective information security knowledge sharing among home users helps them to protect their privacy (Öğütçü et al., 2016). As effective and robust technological solutions have been developed to mitigate security risks and to protect the information, attackers have been using new and ingenious methods to hack others' computers or systems in line with their benefits (Flores et al., 2014; Safa et al., 2016a). In this dynamic environment, effective information security knowledge sharing among employees increases the level of employees' awareness as an effective approach to reduce the cost of information security in organisations (Öğütçü et al., 2016; Safa et al., 2016b). In addition to home users and employees, information security experts struggle similar problems in the domain of information and/or cyber security. Effective information security knowledge sharing leads to the avoidance of wasting time and extra costs through preventing the development of multiple solutions to similar security problems, thereby helping to save invaluable resources that can be utilised more effectively and constructively (Tamjidyamcholo et al., 2014; Safa et al., 2016b). According to Safa and Von Solms (2016), knowledge sharing plays an important role in the domain of information security, due to its positive effect on employees' information security awareness, which is one of the most important factors that reduce the risk of information security breaches. Moreover, information security knowledge sharing is a valuable resource in information security awareness (Safa et al., 2015; Safa and von Solms, 2016). Therefore, organisations and the individuals should establish appropriate environments for information security knowledge sharing, since knowledge sharing in virtual space mitigates the risk of information security breaches. Accordingly, the following hypothesis is formulated:

H_3 Information security knowledge sharing is positively related to information security behaviour.

2.5 The intention of attending information security educational training

Individuals intentionally or unintentionally are a great potential threat to information assets in the organisations (Safa et al., 2016b). Human error can be one of the most important factors of cyber-incidents. The human impact is also often referred to as the weakest link of information security and most security compromises and exploits are a result of employees' insecure behaviour. Companies lose millions due to staff-related cyber security incidents, so it could be very useful for enterprises to achieve the desired behavioural changes and motivation for the employees. Thus, explaining how to improve users' information security behaviour is an important area (Straub and Welke, 1998; Boss et al., 2009; Jenkins et al., 2012) and organisations should develop more effective information security awareness training programs to increase the overall awareness of information security and to improve compliance-related behaviours (Kayworth and Whitten, 2010). In this regard, information security training or workshops can be used as an effective tool to alleviate information security breaches (Jenkins et al., 2012). According to Zakaria (2006), training programs are a significant mechanism to increase or developed information security knowledge between individuals in an organisation. Information security training also provides general knowledge of information security and impacts the self-efficacy in information security positively. Based on the theory of planned behaviour, interaction with others and sharing knowledge influence individuals' thoughts, feelings, actions and behaviour (Safa and Von Solms, 2016). Therefore, information security training helps employees recognise the threats and vulnerabilities of the information systems in their organisations (Whitman, 2004), accordingly information security training is required to create and improve information security behaviour (Albrechtsen and Hovden, 2010). Intention to attend these kinds of training and their encouragement among people is vital for every organisation, as well as nations. In light of the above discussion, the following hypothesis is proposed:

H_4 Intention of attending information security training or workshops is positively related to information security behaviour.

3 Methodology

3.1 Data collection

The data was collected in Turkey from the beginning of May to the end of June 2017. According to the ICT Development Index (International Telecommunication Union, 2017), published by the United Nations International Telecommunication Union, Turkey ranked 67th among 176 countries in 2017. Additionally, in the 2016 Global Information Technology report (Baller et al., 2016), published by The World Economic Forum, Turkey is ranked 48th out of 139 countries in Networked Readiness Index, an index that measures the capacity of countries to leverage ICT for increased competitiveness and well-being. This report states that digital skills in the population and individual usage are improving because of some of the cheaper mobile and fixed Internet tariffs. However, there is a declining importance of ICTs in the government's vision and promotion. Additionally, Turkey has a Cyber Power Index of 30.4%, ranked 15th among 19 countries (Booz, 2011). According to Karabacak et al. (2016, p.527), "Cyber systems are used significantly in the energy, telecommunications, finance, government services, transportation, and water management sectors in Turkey. In spite of the recent national efforts, critical infrastructures of Turkey still have significant vulnerabilities that make systems prone to cyber threats." Additionally, recently online governmental services have improved and more people are conducting online governmental operations (Öğütçü et al., 2016). Therefore, it is important to increase cyber security maturity and mitigate information security risks in Turkey by investigating individuals' information security behaviour.

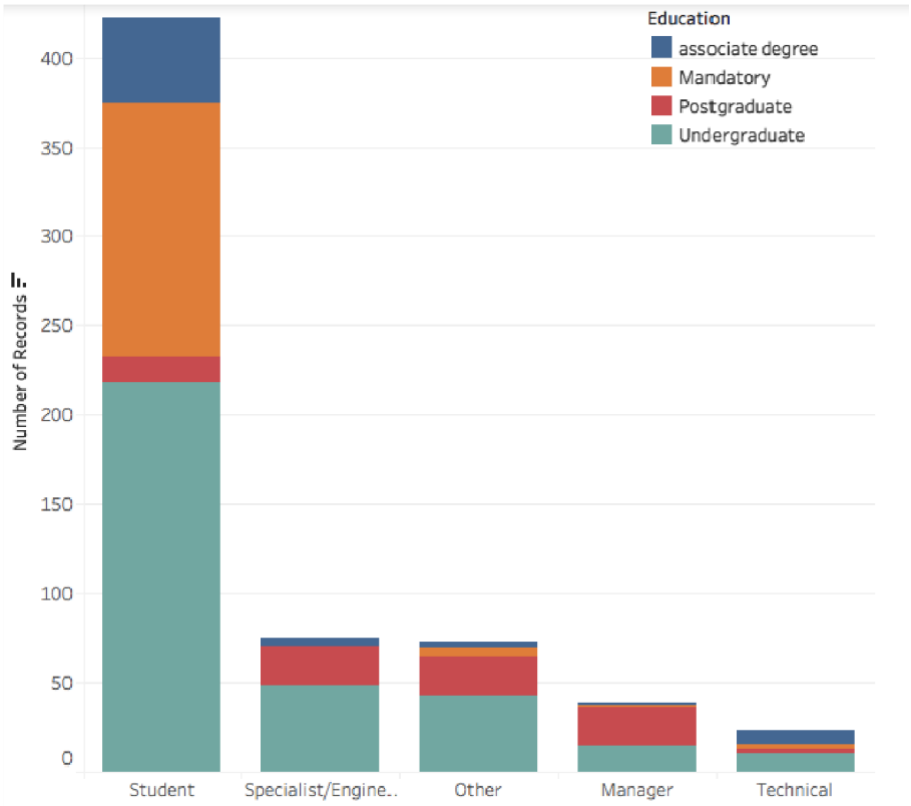
Table 1 Demographic characteristics of the respondents

		No	*Percentage*
Gender	Male	504	80
	Female	126	20
Age	15–19	219	34.8
	20–24	247	39.2
	25–29	96	15.2
	30–34	27	4.3
	35–39	15	2.4
	>40	26	4.1
Education	Mandatory education	152	24.1
	Associate degree	64	10.2
	Undergraduate	331	52.5
	Postgraduate	83	13.2
Position/title	Manager	38	6
	Specialist/engineer	75	11.9
	Technical personnel	23	3.7
	Student	422	67
	Other	72	11.4

The questionnaire consisted of 26 items divided among topics: information security self-efficacy, information security policy of the organisations, information security behaviour, information security knowledge sharing and questions regarding participants' demographic characteristics. Moreover, the data was collected from demographically different age groups and people from a high-school student to a manager in Turkey. The reasons why this sample was selected are "the estimation that in the next 10 years, the most active individuals within the e-government system of Turkey will be 'digital natives' between the ages of 18 and 30" [Öğütçü et al., (2016), p.87] and improving digital skills in a Turkish population (Baller et al., 2016). Participants in this study answered the questionnaire in a voluntary manner and were informed of the aim of the survey. Participants were also assured of the anonymity and the confidentiality of their answers. In the survey, and questions regarding participants' demographic characteristics were optional, thereby there are missing values of participants' demographic characteristics. Reverse code items were used in the questionnaire to reduce the potential effects of the response pattern.

The survey was administered to 1,126 Turkish people and a total of 630 (60% response rate) were usable. The demographic characteristics of the participants, who attended the survey are shown in Table 1. The majority of respondents were male (80%). Most of the respondents had an undergraduate degree (52.2%), followed by mandatory education (24.1%). Figure 1 also summarises the details in Table 1. As can be seen in Figure 1, most of the students have an undergraduate degree and most of the managers have a postgraduate degree.

Figure 1 Education and position of the respondents (see online version for colours)



3.2 Measures

All items in the survey were measured on a five-point Likert scale ranging from 'strongly disagree' to 'strongly agree'. The survey was originally prepared in English and then translated to Turkish. After the translation process was completed, the content validity, clarity, and accuracy of the questionnaires were checked and approved by two faculty members and two postgraduate students. All correlational analyses, tests of reliability, factor analyses and regression analysis were computed by using the software programs SPSS (version 24.0).

In line with the theoretical background mentioned above and the methodology we decided to use during the research, we have prepared a survey consisting of 26 items divided among topics: self-efficacy, information security organisation policy, information security behaviour, information security knowledge sharing, intention to the attendance to relevant educational trainings and questions regarding participants' demographic characteristics.

- *Information security behaviour:* in order to examine behaviours of the people regarding information security, Parsons et al. (2017) developed a survey instrument called HAIS-Q assessing different focus areas such as password management, e-mail use, internet use, social media use, mobile devices, information handling, and incident reporting. Also, Parsons et al. (2017) claimed that the results of the past and present studies provide evidence for the validity and reliability of the HAIS-Q as an instrument to measure information security awareness. Five focus areas of the 13 items within the HAIS-Q (password management, e-mail use, internet use, social media use, mobile devices) were selected to measure information security behaviour. An analysis of reliability on the information security behaviour items resulted in a high corrected item-total correlation of more than 0.3 was found for all the items. These items were excluded from further analysis. The internal reliability of the scale was moderately high (Cronbach's $\alpha = 0.829$).
- *Self-efficacy:* self-efficacy was measured by four items developed by Compeau and Higgins (1995), and based on the study of Chan et al. (2005). Reliability analysis of

the scale yielded a Cronbach's α of 0.919 for the five-items self-efficacy scale, indicating good internal reliability.

- *The information security policy of organisation (ISOP):* ISOP was measured using four items from Safa et al. (2015). ISOP scale had a high internal reliability coefficient for four items (Cronbach's α = 0.851)
- *Information security knowledge sharing:* information security knowledge sharing was measured using three items from the scale of Safa et al. (2015). All items contributed to the internal reliability of the scale and the scale showed good internal consistency with a Cronbach's α reliability of = 0.843.
- *The intention of attending information security educational training*: the intention of attending security educational training was measured by one item. This item was adapted from Han et al. (2017).

4 Analysis and results

Fornell and Larcker (1981) suggested two tests for the assessment of discriminant validity of reflective constructs:

1 The examination of item loadings.

2 The examination of item correlations. Factor analysis was carried out to examine the item loadings (see Table 2).

This was done by conducting principal components of factor analysis with varimax rotation. Factor loadings are above the recommended value of 0.30 (for sample size 350 or greater), and all factor loadings were significant (Hair et al., 2010). The factors extracted corresponded to the model constructs as expected (see Table 2). Table 2 also provides information about Cronbach's . Internal consistency was assessed for each construct using Cronbach's . Cronbach's ranges from 0.829 to 0.919, which indicates that all constructs have acceptable reliability. Additionally, 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 2 Factor loadings, Cronbach's and composite reliability

	Factor loadings	*Cronbach's α*
Information security behaviour	0.482–0.875	0.829
Self-efficacy in information security	0.714–0.946	0.919
ISOP	0.823–0.844	0.851
Information security knowledge sharing	0.848–0.885	0.843

Table 3 Correlations among the variables

	Mean	*1*	*2*	*3*	*4*	*5*
ISOP	3.99	1				
Information security knowledge sharing	3.62	0.518**	1			
Self-efficacy in information security	3.42	0.461**	0.465**	1		
Information security behaviour	3.88	0.340**	0.334**	0.374**	1	
Intention[1]	3.62	0.307**	0.362**	0.302**	0.331**	1

Notes: [1]Intention of attending information security educational training, *p < 0.05, **p < 0.01 and ***p < 0.001.

The main aim of this study was to investigate the relationship between ISOP, information security knowledge sharing, self-efficacy in information security, the intention of attending security educational training and information security behaviour. A correlation matrix (Table 3), including mean, was produced to examine these relationships. Additionally, the discriminant validity of the items was tested by calculating the correlations between all pairs of constructs. As can be seen in Table 3, the correlations between all pairs of constructs were less than 0.9, which shows the discriminant validity of the constructs (Siponen et al., 2014). The results of the correlation analysis indicated that information security behaviour was positively associated with ISOP ($r = 0.340$, $p < 0.001$), information security knowledge sharing ($r = 0.334$, $p < 0.01$), self-efficacy ($r = 0.374$, $p < 0.001$) and intention of attending information security educational training ($r = 0.331$, $p < 0.001$). These results provided initial support for the hypotheses of the study. The highest correlations exist between ISOP and self-efficacy in information security (0.518), which is far less than the problematic level of CMV (e.g., 0.90) (Bagozzi et al., 1991). The remaining correlations among the constructs ranged from 0.302 to 0.465. Thus, the result of the test suggests that CMV is likely not a serious concern in the present study.

Hypotheses predict that all independent variables are positively related to information security behaviour. For testing the hypotheses, regression analysis was performed to investigate the relationship between independent variables (i.e., information security knowledge sharing, the intention of attending information security educational training, ISOP and self-efficacy in information security) and the dependent variable (i.e., information security behaviour). Table 4 shows the findings, which incorporate standardised regression coefficients (β), t-statistics, and adjusted squared multiple correlation coefficient (R^2), significance levels (p) and results of the hypotheses. The outcomes showed that the paths from information security knowledge sharing ($\beta = 0.518$, $p = 0.000$), intention of attending security educational training ($\beta = 0.307$, $p = 0.000$), ISOP ($\beta = 0.340$, $p = 0.000$) and self-efficacy ($\beta = 0.461$, $p = 0.000$) towards information security behaviour were significant. As presented in Table 4, the results of regression analysis supported all hypotheses.

Table 4 The results of the hypotheses testing

Path	β	*t*	*p*	*Adjusted R^2*	*Results*
IS[1] knowledge sharing → IS behaviour	0.518	15.175	0.000***	0.267	Support
Intention[2] → IS behaviour	0.307	8.081	0.000***	0.093	Support
ISOP → IS behaviour	0.340	9.075	0.000***	0.155	Support
Self-efficacy in IS → IS behaviour	0.461	13.005	0.000***	0.211	Support

Notes: [1]Information security, [2]intention of attending information security educational trainings, *p < 0.05, **p < 0.01 and ***p < 0.001.

5 Discussion and conclusions

The growing dependence on the internet and information technologies has created new security concerns. Recently, the issue of information security became vital for both individuals and organisations as every spot in the world became reachable regardless of distance. Furnell and Clarke (2012) indicated that nothing can guarantee any system's security if there is human involvement. Therefore we tried to identify the organisational and individual factors affecting people's information security behaviour. People's behaviour takes a crucial part in information security awareness (Parsons et al., 2017). This is because, hackers, cyber terrorists or government-backed cyber armies might target critical infrastructures with malicious malware to cause physical or economic damage in a country, and countries are now spending billions of dollars each year to improve their security measures in the cyberspace; all those of spending would count as a waste of money and time unless human behaviour in information security is comprehensively developed. Hereby, it is crucial to find out what motivates or enables an individual's

information security behaviour. Therefore, in order to manage cyber risk effectively, ISMS implementation might be necessary and people's security behaviour topics should be carefully taken care of.

ISO/IEC 27001 clause 7.3 is related to employees' information security policy awareness and in the literature several studies indicated the importance of this issue. This study provides evidence that the information security policy of the organisation is positively related to information security behaviour. This finding is in agreement with similar projections made by ISO/IEC 27001 for clause 7.3. In line with the Herath and Rao (2009), the present study supports a positive relationship between organisational information security policy and information security behaviour as well. The study of Herath and Rao (2009) showed that the security norms of organisational policies and their pressure on people influence information security behaviour. The motivation behind this result is that people always tend to ignore the written facts, thereby organisational information security policy might promote individuals' information security behaviour. Because of this relationship, it can be suggested that managers should create a clear and understandable information security policy in order to bring in employees' compliance with information security policy.

ISO/IEC IEC 27001 clause 7.2 requires that the self-efficacy of the employees should be provided with relevant education, training or experience. Also, ISO/IEC 27001:2013 Annex A 7.2.2 requires that the employees of the organisation shall receive security awareness training. The findings of the study indicated that the intention of attending information security training or workshops is positively related to information security behaviour. According to the social cognitive theory, self-efficacy has an important role in behaviour control over potentially threatening events. People with a high level of self-efficacy are more likely focusing their attention on analysing and formulating solutions to problems (Bandura and Jourden, 1991). Therefore, people with a high level of self-efficacy would increase the probability of successful implementation of a task and decrease the probability of causing defects in a system. Additionally, "individuals with stronger conviction on the availability of technology and procedures to control threats to information security, in general, demonstrated firmer belief in their abilities to control threats to information security at the personal level" [Rhee et al., (2009), p.821]. In agreement with the findings of Safa et al. (2015) and Anwar et al. (2017), our findings also indicated that self-efficacy in information security is positively related to information security behaviour. Therefore, from a practical perspective, the findings indicate that individuals' viewpoints on their self-efficacy in information security have an important effect on protecting their information and information systems by using necessary security protection systems and following recommended security conscious behaviour. Additionally, information security training helps employees recognise the threats and vulnerabilities of the information systems in their organisations (Whitman, 2004). Herein, managers need to design or organise information security training, or workshops in the information security domain in order to foster the participants' comprehension of information security risks and information security behaviour. Therefore, the intention to attend these kinds of training and their encouragement among people would be vital for every organisation, as well as nations.

In addition to the facts above, in this study, the importance of employee's behaviours in ISMS emphasised. Especially, Section 7 of ISO/IEC 27001:2013 is found to be related and underlined in this study. Company communication in ISO/IEC 27001:2013 clause 7.4 can also mean knowledge sharing that mitigates the risk of information security breaches. Additionally, Safa and Von Solms (2016) claimed that knowledge sharing in the information security domain leads to a positive effect on employees' information security awareness, thereby reducing the risk of information security breaches. The results of this study provide support for the hypothesis, which is information security knowledge sharing is positively related to information security behaviour. Thus, knowledge sharing in the information security domain would influence individuals' beliefs and attitudes toward information security, in turn, positively affecting information security risk reduction. Organisations should establish appropriate environments for knowledge sharing, which is also supported by the present study. All in all, this study showed that knowledge sharing regarding the topics related to information security, the intention of attending information

security training, the information security policy of an organisation, and self-efficacy in information security have a positive impact on people's information security behaviour.

The results of the study should be considered in light of several limitations. The data were collected from several Turkish organisations and students. This might cause cross-industry variations. Furthermore, generalisations could be made in relation to these variables through different cultures, economies, and sectors, as well as a larger sample size. Additionally, self-reported data from a single source may pose a common method variance. To alleviate this limitation, several procedural and statistical techniques of Podsakoff et al. (2003) were used to minimise potential problems for common method variance: assuring anonymity and confidentiality to all participants and using reverse code items in the questionnaire to reduce the potential effects of response pattern.

References

Abraham, S. (2011) 'Information security behavior: factors and research directions', in *AMCIS*.

Acquisti, A. and Gross, R. (2006) 'Imagined communities: awareness, information sharing, and privacy on the Facebook', in *International Workshop on Privacy Enhancing Technologies*, Springer Berlin Heidelberg, June, pp.36–58.

Aggarwal, P., Arora, P. and Ghai, R. (2014) 'Review on cyber crime and security', *International Journal of Research in Engineering and Applied Sciences*, Vol. 2, No. 1, pp.48–51.

Alam, S.S., Hashim, N.M.H.N., Ahmad, M., Wel, C.A.C., Nor, S.M. and Omar, N.A. (2014) 'Negative and positive impact of internet addiction on young adults: empirical study in Malaysia', *Intangible Capital*, Vol. 10, No. 3, pp.619–638.

Albahar, M. (2017) 'Cyber attacks and terrorism: a twenty-first century conundrum', *Science and Engineering Ethics*, Vol. 25, No. 3, pp.1–14.

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

Anwar, M., He, W., Ash, I., Yuan, X., Li, L. and Xu, L. (2017) 'Gender difference and employees' cybersecurity behaviors', *Computers in Human Behavior*, Vol. 69, pp.437–443.

Bagozzi, R.P., Yi, Y. and Phillips, L.W. (1991) 'Assessing construct validity in organizational research', *Administrative Science Quarterly*, Vol. 36, No. 3, pp.421–458.

Baller, S., Dutta, S. and Lanvin, B. (2016) *The Global Information Technology Report 2016: Innovating in the Digital Economy* [online] http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf (accessed 1 September 2019).

Bandura, A. (1977) 'Self-efficacy: toward a unifying theory of behavioral change', *Psychological Review*, Vol. 84, No. 2, p.191.

Bandura, A. and Jourden, F.J. (1991) 'Self-regulatory mechanisms governing the impact of social comparison on complex decision making', *Journal of Personality and Social Psychology*, Vol. 60, No. 6, p.941.

Bannister, F. and Connolly, R. (2007) 'A risk assessment framework for electronic voting', *International Journal of Technology, Policy and Management*, Vol. 7, No. 2, pp.190–208.

Booz, A.H. (2011) *Cyber Power Index: Findings and Methodology* [online] https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf (accessed 1 September 2019). Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A. and Boss, R.W. (2009) 'If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security', *European Journal of Information Systems*, Vol. 18, No. 2, pp.151–164. Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) 'Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness', *MIS Quarterly*, Vol. 34, No. 3, pp.523–548.

Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H.R. and Upadhyaya, S. (2006) 'Role of perceived importance of information security: an exploratory study of middle school children's information security behavior', *Issues in Informing Science & Information Technology*, Vol. 3, pp.127–135.

Chan, M., Woon, I. and Kankanhalli, A. (2005) 'Perceptions of information security in the workplace: linking information security climate to compliant behavior', *Journal of Information Privacy and Security*, Vol. 1, No. 3, pp.18–41. Clarke, N., Symes, J., Saevanee, H. and Furnell, S. (2016) 'Awareness of mobile device security: a survey of user's attitudes', *International Journal of Mobile Computing and Multimedia Communications (IJMCMC)*, Vol. 7, No. 1, pp.15–31.

Compeau, D.R. and Higgins, C.A. (1995) 'Computer self-efficacy: development of a measure and initial test', *MIS Quarterly*, Vol. 19, No. 2, pp.189–211.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R. (2013) 'Future directions for behavioral information security research', *Computers & Security*, Vol. 32, pp.90–101.

Cummings, J.N. (2004) 'Work groups, structural diversity, and knowledge sharing in a global organization', *Management Science*, Vol. 50, No. 3, pp.352–364.

D'Arcy, J., Hovav, A. and Galletta, D. (2009) 'User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach', *Information Systems Research*, Vol. 20, No. 1, pp.79–98.

Dincelli, E. (2018) 'The role of national culture in shaping information security and privacy behaviors', in Goel, S. (Ed.): *Innovation in Information Security*, Vol. 4, pp.47–68, World Scientific Publishing, Singapore. Fagnot, I.J. (2007) 'Behavioral information security', in Janczewski, L.J. and Colarik, A.M. (Eds.): *Encyclopedia of Cyber Warfare and Cyber Terrorism*, pp.199–205, Information Science Reference, Hershey, PA, USA.

Flores, W.R., Antonsen, E. and Ekstedt, M. (2014) 'Information security knowledge sharing in organizations: investigating the effect of behavioral information security governance and national culture', *Computers & Security*, Vol. 43, pp.90–110.

Fornell, C. and Larcker, D.F. (1981) 'Evaluating structural equation models with unobservable variables and measurement error', *Journal of Marketing Research*, Vol. 18, No. 1, pp.39–50.

Furnell, S. and Clarke, N. (2012) 'Power to the people? The evolving recognition of human aspects of security', *Computers & Security*, Vol. 31, No. 8, pp.983–988.

Galba, T., Solic, K. and Lukic, I. (2015) 'An information security and privacy self-assessment (ISPSA) tool for internet users', *Acta Polytechnica Hungarica*, Vol. 12, No. 7, pp.149–162.

Gartner (2015) *Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach $75.4 Billion in 2015*, 23 September [online] https://www.gartner.com/en/newsroom/pressreleases/2015-09-23-gartner-says-worldwide-informationsecurity-spendingwill-grow-almost-4-percent-to-reach-75- billion-in-2015 (accessed 30 May 2017).

Hair, J.F., Black, W.C., Babin, B.J. and Anderson, R.E. (2010) *Multivariate Data Analysis: International Version*, Pearson, New Jersey.

Han, J., Kim, Y.J. and Kim, H. (2017) 'An integrative model of information security policy compliance with psychological contract: examining a bilateral perspective', *Computers & Security*, Vol. 66, No. 3, 52–65.

Herath, T. and Rao, H.R. (2009) 'Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness', *Decision Support Systems*, Vol. 47, No. 2, pp.154–165.

International Telecommunication Union (2017) *Measuring the Information Society Report* [online] https://www.itu.int/en/ITUD/Statistics/Documents/publications/misr2017/MISR2017_Volume 1.pdf (accessed 10 August 2019).

ISO/IEC 27001:2013 (2013) *Information Technology – Security Techniques – Information Security Management Systems – Requirements* [online] https://www.iso.org/standard/54534.html (accessed 10 August 2019).

Jenkins, J.L., Durcikova, A. and Burns, M.B. (2012) 'Forget the fluff: examining how media richness influences the impact of information security training on secure behavior', in *2012 45th Hawaii International Conference on System Science (HICSS)*, IEEE, January, pp.3288–3296.

Karabacak, B., Yildirim, S.O. and Baykal, N. (2016) 'Regulatory approaches for cyber security of critical infrastructures: the case of Turkey', *Computer Law & Security Review*, Vol. 32, No. 3, pp.526–539.

Kayworth, T. and Whitten, D. (2010) 'Effective information security requires a balance of social and technology factors', *MIS Quarterly Executive*, Vol. 9, No. 3, pp.2012–2052.

Kritzinger, E. and von Solms, S.H. (2010) 'Cyber security for home users: a new way of protection through awareness enforcement', *Computers & Security*, Vol. 29, No. 8, pp.840–847.

Kruger, H.A. and Kearney, W.D. (2006) 'A prototype for assessing information security awareness', *Computers & Security*, Vol. 25, No. 4, pp.289–296.

Langner, R. (2011) 'Stuxnet: dissecting a cyberwarfare weapon', *IEEE Security & Privacy*, Vol. 9, No. 3, pp.49–51.

Lee, D.J. and Ahn, J.H. (2007) 'Reward systems for intra-organizational knowledge sharing', *European Journal of Operational Research*, Vol. 180, No. 2, pp.938–956.

Lendvay, R.L. (2016) *Shadows of Stuxnet: Recommendations for US Policy on Critical Infrastructure Cyber Defense Derived from the Stuxnet Attack*, Naval Postgraduate School Monterey CA, Monterey, USA.

Mylonas, A., Kastania, A. and Gritzalis, D. (2013) 'Delegate the smartphone user? Security awareness in smartphone platforms', *Computers & Security*, May, Vol. 34, pp.47–66.

Öğütçü, G., Testik, Ö.M. and Chouseinoglou, O. (2016) 'Analysis of personal information security behavior and awareness', *Computers & Security*, February, Vol. 56, pp.83–93.

Padayachee, K. (2012) 'Taxonomy of compliant information security behavior', *Computers & Security*, Vol. 31, No. 5, pp.673–680.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. and Zwaans, T. (2017) 'The human aspects of information security questionnaire (HAIS-Q): two further validation studies', *Computers & Security*, May, Vol. 66, pp.40–51.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y. and Podsakoff, N.P. (2003) 'Common method biases in behavioral research: a critical review of the literature and recommended remedies', *Journal of Applied Psychology*, Vol. 88, No. 5, p.879.

Ponemon Institute (2018) *2018 Cost of Data Breach Study: Impact of Business Continuity Management* [online] https://www.ibm.com/downloads/cas/AEJYBPWA (accessed 10 January 2019).

Rhee, H.S., Kim, C. and Ryu, Y.U. (2009) 'Self-efficacy in information security: its influence on end users' information security practice behavior', *Computers & Security*, Vol. 28, No. 8, pp.816–826.

Rhodes, J., Hung, R., Lok, P., Lien, B.Y-H. and Wu, C.M. (2008) 'Factors influencing organizational knowledge transfer: implication for corporate performance', *Journal of Knowledge Management*, Vol. 12, No. 3, pp.84–100.

Ryu, S., Ho, S.H. and Han, I. (2003) 'Knowledge sharing behavior of physicians in hospitals', *Expert Systems with Applications*, Vol. 25, No. 1, pp.113–122.

Safa, N.S. and Von Solms, R. (2016) 'An information security knowledge sharing model in organizations', *Computers in Human Behavior*, April, Vol. 57, pp.442–451.

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A. and Herawan, T. (2015) 'Information security conscious care behaviour formation in organizations', *Computers & Security*, September, Vol. 53, pp.65–78.

Safa, N.S., Von Solms, R. and Furnell, S. (2016a) 'Information security policy compliance model in organizations', *Computers & Security*, February, Vol. 56, pp.70–82.

Safa, N.S., Von Solms, R. and Futcher, L. (2016b) 'Human aspects of information security in organisations', *Computer Fraud & Security*, Vol. 2016, No. 2, pp.15–18.

Sigala, M. and Chalkiti, K. (2014) 'Investigating the exploitation of Web 2.0 for knowledge management in the Greek tourism industry: an utilisation-importance analysis', *Computers in Human Behavior*, Vol. 30, pp.800–812.

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

Stanton, J., Stam, K., Mastrangelo, P. and Jolton, J. (2006) 'Behavioral information security: an overview, results, and research agenda', in Zhang, P. and Galletta, D.F. (Eds.): *Human-computer Interaction and Management Information Systems: Foundations*, pp.262–280, M.E. Sharpe, Armonk, NY, USA.

Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J. (2005) 'Analysis of end user security behaviors', *Computers & Security*, Vol. 24, No. 2, pp.124–133.

Straub, D.W. and Welke, R.J. (1998) 'Coping with systems risk: security planning models for management decision making', *MIS Quarterly*, Vol. 22, No. 4, pp.441–469.

Tamjidyamcholo, A., Baba, M.S.B., Shuib, N.L.M. and Rohani, V.A. (2014) 'Evaluation model for knowledge sharing in information security professional virtual community', *Computers & Security*, June, Vol. 43, pp.19–34.

Utz, S. and Krämer, N.C. (2009) 'The privacy paradox on social network sites revisited: the role of individual characteristics and group norms', *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, Vol. 3, No. 2 [online] https://cyberpsychology.eu/article/view/4223/3265 (accessed 10 May 2018).

Von Solms, R. and Van Niekerk, J. (2013) 'From information security to cyber security', *Computers & Security*, October, Vol. 38, pp.97–102.

Whitman, M.E. (2004) 'In defense of the realm: understanding the threats to information security', *International Journal of Information Management*, Vol. 24, No. 1, pp.43–57.

Whitman, M.E. (2008) 'Security policy: from design to maintenance, in: information security: policy, processes, and practices', *Advances in Management Information Systems*, in Straub, D.W., Goodman, S.E. and Baskerville, R. (Eds.): pp.123–151, M.E. Sharpe, London, England Armonk, New York.

Wigfield, A. and Eccles, J.S. (2000) 'Expectancy-value theory of achievement motivation', *Contemporary Educational Psychology*, Vol. 25, No. 1, pp.68–81.

Wijnhoven, F. (1998) 'Knowledge logistics in business contexts: analyzing and diagnosing knowledge sharing by logistics concepts', *Knowledge and Process Management*, Vol. 5, No. 3, pp.143–157.

Wisenbaker, J.M., Scott, J.S. and Nasser, F. (2000) 'Structural equation models relating attitudes about and achievement in introductory statistics courses: a comparison of results from the US and Israel', in *9th International Congress on Mathematics Education*, Tokyo, Japan, July.

Zakaria, O. (2006) 'Internalisation of information security culture amongst employees through basic security knowledge', in *IFIP International Information Security Conference*, Springer, Boston, MA, May, pp.437–441.

Website

http://www.gartner.com/newsroom/id/3135617/ (accessed 30 May 2017).