Taylor & Francis
Taylor & Francis Group

Journal of Organizational Computing and Electronic Commerce

ISSN: 1091-9392 (Print) 1532-7744 (Online) Journal homepage: https://www.tandfonline.com/loi/hoce20

Violators versus non-violators of information security measures in organizations—A study of distinguishing factors

Habib Ullah Khan & Khalid A. AlShare

To cite this article: Habib Ullah Khan & Khalid A. AlShare (2019) Violators versus non-violators of information security measures in organizations—A study of distinguishing factors, Journal of Organizational Computing and Electronic Commerce, 29:1, 4-23, DOI: 10.1080/10919392.2019.1552743

To link to this article: https://doi.org/10.1080/10919392.2019.1552743

Published online: 17 Feb 2019.

JOURNAL OF ORGANIZATIONAL COMPUTING AND ELECTRONIC COMMERCE
2019, VOL. 29, NO. 1, 4–23
https://doi.org/10.1080/10919392.2019.1552743

Violators versus non-violators of information security measures in organizations—A study of distinguishing factors

Habib Ullah Khan and Khalid A. AlShare

Department of Accounting and Information Systems, College of Business & Economics, Qatar University, Doha, Qatar

ABSTRACT

The present study analyzes the elements that differentiate violators from non-violators of information security measures. Various elements are derived from established theories and models such as general deterrence theory, theory of planned behavior, theory of reasoned action, protection motivation theory, and social cognitive theory. To examine these factors, the data are gathered through an online study conducted in a Midwestern University, USA. The data are collected using questionnaires, and after scrutiny, 195 questionnaires are selected for final analysis. This data are analyzed using second-level statistical techniques, such as chi-square analysis and ANOVA. Results reveal that violators and non-violators of information security measures differ significantly with respect to many factors. These factors include perceived privacy, subjective norms, perceived information security policy (ISP) scope, perceived severity of penalty, perceived celerity of penalty, management support, organizational security culture, and perceived organizational IT capability. The non-significant factors are trust and work load. Implications for practitioners and researchers are provided.

KEYWORDS

Information security (IS); violators; non-violators; information security policy (ISP); organizational IT capability

1. Introduction

Highlighting the serious need for information security programs/policies for the organizations, Knapp and Ferrante (2012) explained the data disaster occurred in Citibank and Sony Company in the year 2011 and its adverse ramifications. Myyry et al. (2009) observed in their work that more than 90% of organizations encounter at least one problem related to data security issues per year and the bulk of them occur due to non-compliance of employees. The information security policies vary as per the nature of organization—health, auditing, software developing, and so forth (Abawajy 2014; Parsons et al. 2014; Awan, Khan, and Zhang 2012; Robinson 2018). It is not just framing the policies of the organization, but it has become imperative to apply these policies to the information security personnel (Aurigemma and Panko 2012; Hu, West, and Smarandescu 2015; Kabanda, Tanner, and Kent 2018). While spell on the employees' side, they believe to be the weakest link in the concatenation of data security and expected non-compliant nature at all tiers (Asai and Hakizabera 2011; Brock and Khan 2017; Warkentin and Wilson 2009).

Ubiquitously, many models and theories are developed to understand the behavior of information technology users and their nature of compliance with the information security measures. Some of them are: Theory of Planned Behavior (TPB), Rational Choice Theory (RCT), Protection Motivation Theory (PMT), General Deterrence Theory (GDT), Social Cognitive Theory (SCT), and Theory of Reasoned Action (TRA) (Aurigemma 2013; Lin 2016; Safa and Von Solms 2016). Mostly, research inferred that perceived benefits and the overall consequences drive the attitudes of violators or non-violators of the

CONTACT Habib Ullah Khan habib.khan@qu.edu.qa Department of Accounting and Information Systems, College of Business & Economics, Qatar University, P.O. Box 2713, Doha, Qatar

Color versions of one or more of the figures in the article can be found online at www.tandfonline.com/hoce.

information security policies (Bulgurcu, Cavusoglu, and Benbasat 2010; Khan, Omonaiye, and Madhavi Lalitha 2017). Hence, there is every need to design stringent regulations with respect to behavior perspective for mitigating the information security policy deviations. The primary aim of this work is to analyze the differences between violators and non-violators, with respect to their perceptions about factors that influence their compliance with information security measures. The study also explores the impact of demographic profile of respondents on their responses. The conceptual framework given in Figure 1 is based on a study conducted by Al-Share and Lane (2008).

There are four main groups of factors that might influence an employee's compliance or not compliance with information security policy, as shown in Figure 1. The first group includes factors related to individual traits, which include perceived privacy, trust, and subjective norms; The information security policy, which includes information security policy scope, the severity of penalty, and celerity of penalty. The work environment aspects, which include management support, organizational security culture, workload, and organization IT capabilities. The demographic factors are based on gender, age, educational level, experience, managerial role, job title, and percentage of computer usage.

With the knowledge attained about the background of information security policy adherence, the following research questions are framed.

Research Questions

RQ1: Is there a significant difference between responses of violators of information security measures and non-violators?

RQ2: Is a violation of information security measures depend on demographic variables such as gender, age, educational level, experience, managerial role, job title (position), and percentage of computer usage?

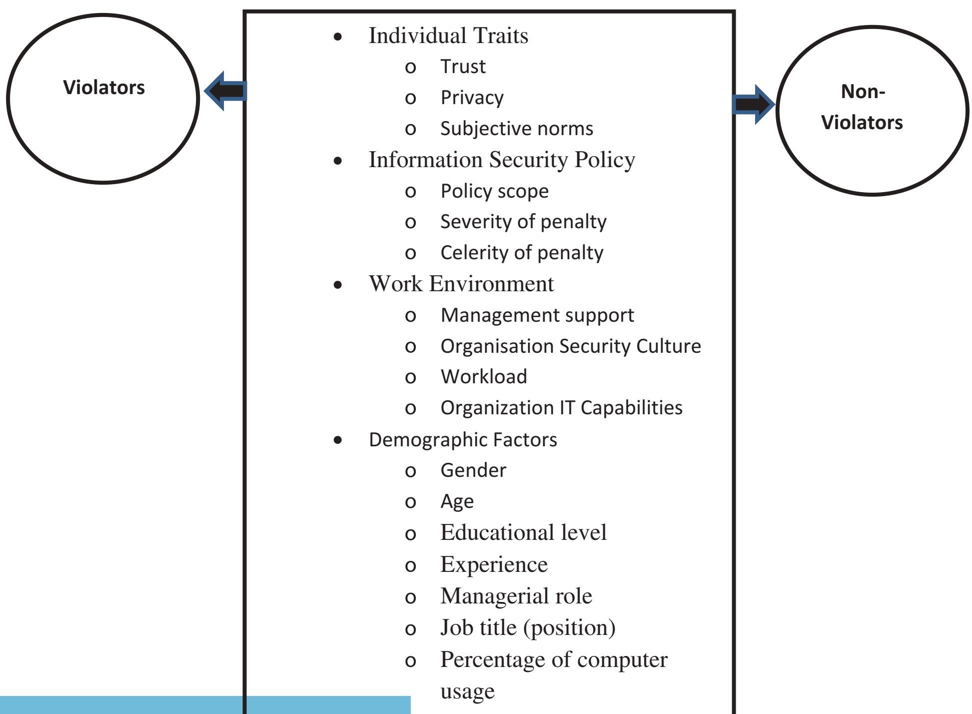

Figure 1. Factors differentiate violators and non-violators of information security measures.

2. Literature review

The literature review covers three main categories, which attribute to the compliance or not compliance with information security policy. The first category is related to the individual traits, which include a perception of trust, a perception of privacy, and subjective norms. The second group of factors is related to information security policy, such as information security policy scope, the severity of the penalty, and celerity of penalty. The third category of factors is related to the work environment such as management support, organizational security culture, workload, and organizational IT capability. The significant differences between violators and non-violators of information security measures would be discussed with respect to each of the above categories. Additionally, the impact of demographic factors such as gender, age, educational level, experience, computer usage, job title (position), and management role on violation of information security measures will also be examined.

2.1. *Individual's traits*

2.1.1. *Trust*

In this study, trust refers to the person's willingness to share work-related information with his/her coworkers. Trust is built over the time in a work environment and it is essential for getting things done; however, trust often prompts risky habits, for example close workers may share their account passwords (Astakhova 2016; Barlow et al. 2013; Rodinson 2018). This practice not only leads to foster violation of security behavior among the individuals but also exposes the company to a myriad serious information security risk. Some of them are data loss, system unavailability and malicious system use (Boehmer et al. 2015; Brock and Khan 2017; Herath and Rao 2009). An information security survey conducted in the US, UK, and Australia for 2500 people from Boulder (2010) found that 40% of users had shared their password with one or more people in the previous 12 months. According to Durgin (2007), many attackers use social engineering, a non-technical attack that takes advantage of the naive and trusting nature of individuals for violation (Kearney and Kruger 2016). It is estimated that on an average, the corporate email user sends 112 emails every day and one out of every seven (approximately) of those messages can be related to gossip (Gilbert and Mitra 2012). Staff engaged in gossip can intentionally or unintentionally disclose sensitive or personal information to colleagues that they trust; an act that not only breaks the information system policy but also the law (Martin, Rice, and Martin 2016; Albrechtsen and Hovden 2009). So, by understanding the role of trust as a differentiating factor between the violators and non-violators of information security measures, the following hypothesis is posited:

H_1: There is a significant difference in the average trust level between violators and non-violators.

2.1.2. *Privacy*

Privacy in this study is defined as the individual's concern about protecting/revealing one's own or other people's personal information. It is mentioned in the prior research that the sparse priority is given to a privacy, in spite of its significance in the perspective of customers and organizations (Khan and Ejike 2017; Mahmoud and Zeki 2016; Mylonas et al. 2013). In addition, security breaches and privacy interruptions, ensure heavy losses to the organizations. The privacy hindrance of the company accrues 1% share loss to the finances every year. (Bashir and Khan 2016; Goel and Shawky 2009). As the technology is developing day by day, to maintain the privacy of the information security measures, along with tight mechanism and software, it is equally important to monitor the violators and non-violators of information security measures (Lin 2016; Son 2011; Zviran 2016). The measures to be taken to encourage non-violators are suggested in the article by Connolly et al. (2014). As per the voice of the members of the organization interviewed in this work, regular awareness of the privacy of data among the personnel can increase the number of non-violators. For instance, the study of Cisco (2013) established that a considerable percentage of smart phone users (40% approx) don't put a password on their cell phones, through which they access vital data. This indicates that their privacy is at stake. Therefore, educating the employees or users, so as to encourage them toward non-violation is the best solution for encountering security threats (Brady 2011; Mahesh and Hooter 2013; Seyal and Turner 2013).

H_2: There is a significant difference in average level of privacy maintained between violators and non-violators.

2.1.3. *Subjective norms*

As per the theory of planned behavior, a subjective norm is one of the attributes in deciding the behavior of individuals (Aizen 1991; Aurigemma 2013; Hassan et al. 2015; Safa and Von Solms 2016). In the context of this research, subjective norm is seen as an individual's perception about certain behavior based on the influence of people like: educators, fellow workers, parents, friends, and media personnel, etc. It also constitutes a basis for the social bonding and so determines the compliance or non-compliance behavior of the individual (Ifinedo 2014). The study of Guo et al. (2011) perceived that through the subjective norms, the non-compliance attitude can be understood well. The same opinion is felt by Li, Zhang, and Sarathy (2010) that, suitable in the circumstances results can be obtained by this construct. Nevertheless, it is significant to hold in mind the opposite viewpoint as well, for example Sommestad et al. (2014) proved that compared to all other attributes, a subjective norm is an inconsistent attribute. Therefore, in that respect there are different views about the credibility of the concept and subjective norm. Nevertheless, the majority of researchers proved that subjective norm has an inverse relationship with the information security non-compliant behavior and hence it grooms the compliance nature (Cheng et al. 2013; Kabanda, Tanner, and Kent 2018; Seyal and Turner 2013).

H_3: There is a significant difference in average level of subjective norms between violators and non-violators.

2.2. *Information security policy*

2.2.1. *Information security policy scope*

Information security policy (ISP) is defined as the "state of roles and responsibilities of employees to safeguard the information and technology resources of their organization" (Bulgurcu, Cavusoglu, and Benbasat 2010). The best way these policies are implemented is to ensure that employees understand these in detail and the management of the organization should always encourage the staff to adhere to the ISP (Al-Share and Lane 2008; Watters and Ziegler 2016). Moreover, there is every need to improve the technical and procedural security measures, which can help to improve information security. As the weakest link and the greatest asset in an organization are the employees, so employees' compliance with information security measures is critical to the success of any information security program (Al-Omari, El-Gayar, and Deokar 2012; Johnston et al. 2016; Khan and Uwemi 2018). It is also found by various studies that the employee's intention to comply with policies is influenced by their attitude, normative beliefs, and self-efficacy (Bulgurcu, Cavusoglu, and Benbasat 2010; Martin, Rice, and Martin 2016).

H_4: There is a significant difference in mean of information security policy scope between violators and non-violators.

2.2.2. *Severity of penalty*

Employee compliance with the information security policies depends on the type of response he gets from his peer group as a result of adherence or non-adherence. That is if the penalty affects the self-respect of the person among his peer group, he may comply with the norms of the organization (Park, Kim, and Park 2017; Siponen, Pahnila, and Vance 2012). In situations where the formal warning/action won't work, enforcement of monetary penalties can increase the number of non-violating staff (D'Arcy, Herath, and Shoss 2014; Knapp and Ferrante 2012). Herath and Rao (2009) consolidated from extolling research that though different organizations use different penalty mechanisms, normal actions did not get due importance. At the same time, the moral commitment of the individual has to be considered before levying penalty (D'Arcy, Hovav, and Galletta 2009; Khan and Uwemi 2018; Tamjidyamcholo et al. 2013). However, the research for understanding the influential factors of information security policy compliance added a piece to the puzzle, the economies of crime literature suggest the trade-off between the severity of the penalty and the attitude to perform crime (Cheng et al. 2013; Humaidi and Balakrishnan 2015).

H_5: There is a significant difference in mean of the severity of penalty between violators and non-violators.

2.2.3. *Celerity of penalty*

Punishment celerity is concerned with the speed with which a punishment is exercised. According to Brink (2011), sanction celerity is defined as the time between the violation act and the sanction of the violation. Schoepfer, Carmichael, and Piquero (2007) concluded from their work that a person would avoid criminal behavior if that behavior provokes swift, severe, and certain punishment. In other words, a punishment delay would diminish the deterrent ability of a sanction. People are less likely to violate a norm, if the perceived consequences of sanction against the violation are greater than the benefits of committing the violation (Dinev et al. 2011; Humaidi and Balakrishnan 2015). Interestingly, most of the research in this area focuses on the certainty and severity of sanctions than the swiftness or celerity of the sanction being enforced (Lowry et al. 2015; Nagin and Pogarsky 2001). According to the Deterrence Theory, there is a positive effect of sanction celerity on deterrence.

H_6: There is a significant difference in the mean of the celerity of penalty between violators and non-violators.

2.3. *Work environment*

2.3.1. *Management support*

In this study, management support is defined as the perception of the employees regarding their managers' support and understanding of importance of the information security. In an organization, if the information security is important, then the management should visibly implement the policy guidelines and enable the employees with adequate training so that management acts as a huge support for their staff (Al Hogail, Mirza, and Bakry 2015; Gadzama et al. 2014; Kabanda, Tanner, and Kent 2018). A well-defined process of secure communication with relevant education, reminders and refresher courses increase employee's feelings of responsibility and ownership in decisions about security and ultimately lead to a more positive attitude about security throughout the whole organization (Greene and D'Arcy 2010; Humaidi and Balakrishnan 2015). Senior management should take initiative with respect to communication, imparting training and playing a pivotal role in implementing the policy and thereby support the staff in such a way that they lean on the management for all the necessities (Kearney and Kruger 2016; Myler and Broadbent 2006). In addition to this commitment from the top management of an organization is also an important factor in grooming the behavior of its employees (Al Hogail 2015;

Herath and Rao 2009). This is motivated by identifying the staff by awarding incentives to those who comply with the organization's security policy. Thus, organizational commitment becomes much more effective behavior, concluding that this influences both the organization and employee's commitment (Hassan and Ismail 2016; Padayachee 2012; Predd et al. 2010). The commitment of the top management toward compliance with security policies leads to a positive attitude, subjective norms and strong perceived behavioral control toward compliance with information security policies (Hu et al. 2012; Khan, Omonaiye, and Madhavi Lalitha 2017).

H_7: There is a significant difference in mean of management support between violators and non-violators.

2.3.2. *Organizational security culture*

Kraemer and Carayon (2007) reported that communication, security culture, policy, and organizational structure are the most frequently cited factors associated with information security. Organizational security culture involves the establishment of policies, standards, training and educational programs. Allen (2006) reveals about security culture that "building an information security culture within an organization starts with making people aware of security issues, providing them with tools to react and encouraging two-way communication among security personnel, managers, and employees (AlHogail 2015; Alhogail and Mirza 2014a; Brock and Khan 2017). The creation of a security culture should be considered as a long-term investment, which requires a constant effort to maintain and grow. Chang and Lin (2007) emphasized that information security is not just a technical issue but a management one as well. Management role becomes very essential in creating a work environment that supports organizational security culture. A company with a strong organizational security culture, appropriate policies, and procedures, including sanctions regarding those policies would sustain well, even in a competitive environment (Culnan and Williams 2009). However, everyone should engage in a secure behavior to create and maintain organizational security culture. As stated by Safa et al. (2015, 68) "Changing the perception or behavior of users towards a positive information security culture is not an easy or straightforward task." With the knowledge about organizational security culture and the role it plays in employees' adherence to the information security policies, the following hypothesis is framed:

H_8: There is a significant difference in mean of perceived organizational security culture between violators and non-violators.

2.3.3. *Workload*

In this study, the workload refers to the employee's perception about the amount of work he/she needs to complete. The previous researches showed that majority of violations of the information security policies are attributed to employees who optimize their behavior by utilization of optimum resources (Arian et al. 2017; Battmann and Klumb 1993). The trade-offs amongst the violation and compliance at an organization level have declined on account of the desire for minimum effort on security compliance (Albrechtsen and Hovden 2009; Rodinson 2018). The outcome of the research of Martin, Rice, and Martin (2016) of 102 IT professional highlighted that the grounds for violation is attributed to the everyday tension and pressure applied to the staff in order to achieve higher financial commitments and goals of the system. On account of this, the gradient shifts slowly in a direction away from the productivity and the tension for increased productivity is feeling a lot more substantial. This also results in security risks as the persistent pressure to perform work often result in employees taking risks to respond to this pressure (Allam, Flowerday, and Flowerday 2014).

H_9: There is a significant difference in mean of perceived workload between violators and non-violators.

2.3.4. *Organization IT capability*

In this study, the organization IT capability refers to the employee's perception regarding the ability of IT in capturing information security violations. Connecting to a complex and risky environment such as the internet is no longer a choice for today's firms and organizations, rather a necessity for surviving in the market (Musa, Khan, and Alshare 2015; Saunders and Brynjolfsson 2016). Alongside, this is the need to give users more privileges to perform their jobs effectively, while keeping in mind the maintenance of adequate levels of access. Maintaining the security of information systems requires spending considerable resources and in spite of that expenditure, incidents related to information breach occur on and off (Al-Omari, El-Gayar, and Deokar 2012; Brock and Khan 2017). In other firms where many systems are used, different access privileges like users and passwords are to be given, the effective administration is necessary (Etezady 2011). This can help to prevent users from installing certain software on their machines or accessing certain websites in insecure locations and can remove undesired and malicious software and keep the virus and internet security software up-to-date on all computers over the network (Connollyl, Lang, and Tygart 2014). Thus, the following hypothesis is proposed to test the difference in mean of perceived organizational IT capability between violators and non-violators:

H_{10}: There is a significant difference in mean of perceived organizational IT capability between violators and non-violators.

3. Demographic factors

In this section, the impact of various demographic factors on the violation or non-violation behavior of the individual is studied. As per prior researches (Barlow et al. 2013; D'Arcy, Hovav, and Galletta 2009; Zhang, Reithel, and Li 2009), the factors like gender, age, educational level, experience, computer usage, job title (position), and managerial role are identified as some of the important factors to understand such behavior. Zhang, Reithel, and Li (2009) used gender, age, education, and experience (years employed) as control variables in predicting intention to comply with information security policy. There are different views produced by the existing research on the impact of the demographic profile of individuals. Gender and age have been used in information systems research related to an individual's information security behavioral intention. Putri and Hovav (2014) proved from the analysis that while age has a strong impact on the intentions of the person to comply with the security policy, gender is found to have a weak impact. D'Arcy, Hovav, and Galletta (2009) found that gender and age are not significant in predicting the intention of information security misuse at work. However, Herath and Rao (2009) mentioned that females have higher intentions for compliance with security policy. On the other hand, Barlow et al. (2013) found that gender, age, work experience, and level of education did not have much effect on violation of information security policies. Results of prior research revealed a strong relationship between the level of education and awareness of information security policy (Bulgurcu, Cavusoglu, and Benbasat 2010; Parsons et al. 2014). In addition to the knowledge, employee's "prior experience" or years employed is a preceding factor for Protection Motivation Theory and the research strongly affirms that habit is a parameter that has a strong compliance with information security policies (Siponen and Vance 2010). It is also added by Takemura (2012) that permanent employees exhibit a tendency to violate the rules and it is a challenge to control psychological factors such as the individual's attitude toward this risk.

Overall, one can say that misuse of computers and access to malicious software leads to perceived susceptibility of perceived severity. During this state of mind, people are to be motivated to avoid the threat if they realize that safeguarding measure is not effective (Al-Omari et al. 2013; Watters and Ziegler 2016). Managers play a pivotal role in guiding, supporting and not the least in motivating the staff for abiding by the organization's information security policies and procedure protocol. The onus is on the managers to communicate about the policies and guidelines in a much clear, concise, and easy way so that the staff is able to comprehend them correctly (Boss et al. 2009; Herath and Rao 2009). According to Gist (1987), the implications of the self-efficacy of top management on training and organizational development are numerous. Thus, one can expect that managers are less prone to violate IS measures. It is also added that sometimes, the employee's designation may lead to the violation information security measure, especially if such measures are not clearly stated. So, as there are different views about the relationship between the demographic profile of the employee and the practices of violation/non-violation of information security measures, the study intends to test them using the collected data. Thus, the following hypotheses are framed in connection to the different variables discussed above:

H_a: Violation of information security measures is not independent of gender.

H_b: Violation of information security measures is not independent of age.

H_c: Violation of information security measures is not independent of educational level.

H_d: Violation of information security measures is not independent of experience.

H_e: Violation of information security measures is not independent of computer usage.

H_f: Violation of information security measures is not independent of job title (position).

H_g: Violation of information security measures is not independent of the managerial role.

4. Methodology

4.1. *Survey development*

An online survey link is sent to the employees of the Midwestern University of USA for data collection. Employees are asked to participate if they meet the following two requirements: 1) they are currently employed either as a full-time employee, part-time employee, temporary worker, or as a consultant; and 2) they use the organization's computer system in completing their job tasks. The questionnaire had three sections. The first section contained a few demographic questions that included gender, age, educational level, experience, job title (position), managerial role, and the percentage of computer usage at work. The second section addressed the primary constructs of the study.

4.2. *Survey statements*

Each construct included three statements whose answers ranged from strongly disagree (1) to strongly agree (7). For example, the following statement was used to measure trust factor "I am not worried about revealing information related to my job to my co-workers." On the other hand, this statement "I consider information privacy as one of my major concerns" was used to measure the privacy factor. The items for the constructs are mainly adopted from prior studies to fit the current study context, such as Siponen and Vance (2010), D'Arcy, Hovav, and Galletta (2009), and Asai and Hakizabera (2011). The list items are reported in Appendix A.

4.3. *Data collection*

The survey is tested by asking a few participants to provide their feedback on the questionnaire. Established on the received feedback, the survey instrument is modified; for example, many factors are measured by three items. A total of 208 responses are received. However, five respondents indicated that they did not wish to participate, three did not meet the participation criteria, and five responses are incomplete. Therefore, 195 completed responses are used in the analysis among which 84 indicated that they have violated information security measures and 111 respondents did not.

4.4. *Statistical analysis*

The statistical analysis is carried out by using the Statistical Package for the Social Sciences (SPSS 22). Descriptive data analysis techniques such as frequencies, means, and standard deviations are calculated from the data. The reliability and validity of the constructs are evaluated using Cronbach's Alpha and Principal Component Factor Analysis. ANOVA and Chi-square are used to test the proposed hypotheses.

4.5. *Samples profile*

Fifty percent of the violators' sample compared to 60 percent of the non-violators sample are females as shown in Table 1. Approximately, 55 percent of violators sample, compared to 45 percent of the non-violators sample are above 50 years old. It can likewise be noted that the bulk of both the samples hold graduate degrees. Moreover, for both the samples, the number one job title (position) is "faculty" followed by "director". Forty percent of the violators' sample, compared to 28 percent of the non-violators sample, has more than 15 years of experience. With respect to the percentage of computer usage at work, 38 percent of violators and 42 percent of non-violators use the computer for more than 84 percent of the time. Based on the above data, one can describe the violators as being older, with a high level of education and experience and have high usage of the computer at work.

Table 1. A summary of key demographic variables.

	Violators N = 84		Non-Violator N = 111	
Variable	No. of Responses	%	No. of Responses	%
Gender:				
Male	42	50.0	45	40.54
Female	42	50.0	66	59.46
Age:				
Less than or 50 years	38	45.2	60	54.1
Greater than 50	46	54.8	51	45.9
Educational Level:				
Undergraduate	32	38.1	40	36.0
Graduate	52	61.9	71	64.0
Managerial Role:				
Yes	35	41.7	43	38.7
No	49	58.3	68	61.3
Job title (position):				
Administrative assistant	14	16.7	27	24.3
Director	25	29.8	27	24.3
Faculty	29	34.5	31	28.0
Other	16	19.0	26	23.4
Percentage of computer usage:				
Less 65%	26	31.0	32	28.8
Between 65–84%	26	31.0	33	29.7
More than 84	32	38.0	46	41.5
Experience:				
1–6 years	24	28.6	39	35.2
Between 7 and 15	26	31.0	41	36.9
More than 15	34	40.4	31	27.9

5. Data analysis

5.1. *Reliability and validity of constructs*

As mentioned earlier, Cronbach's Alpha is used to determine the reliability of the model constructs. The values for Cronbach's Alpha are above 0.80 except for two constructs; privacy is 0.66 and trust is 0.79 as shown in Table 2. Although the common acceptable lower value for Cronbach's Alpha is 0.7, according to Hair et al. (2006, 137), Cronbach's Alpha of 0.60 is considered as acceptable for exploratory studies. Additionally, the convergent and the discriminant validity of the constructs are assessed by performing a Principal Component Factor Analysis with varimax and the correlation matrix. Only items with loadings of at least 0.50 are retained (Hair et al. 2006). All items had a load of more than 0.65 as shown in Table 2. In order to obtain discriminant validity, no item should have a loading higher on another construct than the one it intends to measure. As shown in Table 2, all items loaded on their intended constructs. Moreover, there is no item with a loading greater than 0.35 on two or more constructs. As shown in Table 3, items related to a particular construct had stronger correlation values, compared to the correlation values with other items of the other constructs. This is an indication of a convergent as well as discriminant validity. Based on the above results, the reliability and validity of the instrument are satisfactory. The list of items and their descriptive statistics are reported in Appendix A.

6. Results

This section includes two parts; the first part reports the results for the hypotheses H1–H10. The second part discusses the results of the effect of demographic factors (hypotheses H_a–H_g).

6.1. *Testing hypotheses*

ANOVA procedure is used to test if there are significant differences in means of the identified factors in the study between violators and non-violators. The significant factors are shown in Figure 2 and the ANOVA results are reported in Table 4.

Compared to violators, the non-violator respondents are more concerned about privacy and they are more positively affected by subjective norms as shown in Table 4. Additionally, compared to their counterparts, non-violators had a stronger belief toward the organizational IT capability, management support for information security measures and the organizational security culture. Moreover, the non-violators had a stronger agreement with the statements related to severity and celerity of penalty, policy scope. Table 5 provides a summary of the hypothesis testing results.

6.2. *Effects of demographic variables*

As shown in Table 6, none of the demographic factors are significant. Based on the results of Chi-square test, violations of the security measures are independent of gender, age, educational level, experience, job title (position), managerial role, and percentage of computer usage at work. As it is cited in the literature review section, mixed results are reported regarding the effect of demographic factors.

7. Discussion

While discussing the implications of the results of any study, the researcher should consider not only the statistical significance but also the practical significance. In this study, the "effect size" measure is employed to evaluate the practical significance. As reported in Table 4, the values of the estimated effect size have ranged from 0.28 to 1.2. According to Cohen's classifications (1977), [0.2 is a small

Table 2. Reliability and validity assessment.

Items	Trust	Privacy	Subjective Norm	IT Resource	Manag. Support	Policy scope	Org. Sec. Culture	Work Load	Severity of Penalty	Celerity of Punsh.
TRS1	**.859**	−.060	−.003	.011	.014	.002	.048	.003	.088	−.153
TRS2	**.827**	−.041	.145	.121	.091	−.051	−.061	−.035	.017	−.057
TRS3	**.817**	.145	−.009	−.063	−.027	.145	.051	−.104	−.044	.140
PRV1	.112	**.664**	−.123	.130	−.186	.222	−.011	−.094	−.086	.277
PRV2	−.018	**.742**	−.056	−.008	.171	.012	.083	.053	.079	−.067
PRV3	.226	**.816**	.157	−.106	.070	.077	−.081	−.251	.117	−.170
SN1	.179	.117	**.779**	.301	.170	−.015	−.007	.093	.143	.018
SN2	.310	.102	**.716**	.017	.170	.297	.124	.077	−.009	−.131
SN3	.317	.137	**.761**	.128	.244	.149	.029	.125	.132	−.071
ITR1	.274	.241	−.023	**.818**	.151	.235	.026	−.006	.010	−.059
ITR2	.295	.278	−.032	**.806**	.146	.199	.047	.045	−.019	−.090
ITR3	.267	.334	−.073	**.778**	.173	.230	.041	−.022	.006	−.069
EE1	.228	−.067	.137	−.006	.181	.074	.109	.001	.063	.100
EE2	.301	−.002	.141	−.053	.236	.090	.021	.070	.050	.003
EE3	.312	.047	.085	−.084	.203	.053	−.004	.076	.040	.089
PE1	.143	.079	.091	−.152	.153	.159	.022	.093	.014	.109
PE2	.270	.012	.076	−.063	.261	.073	−.037	.099	.020	.125
PE3	.212	.203	.236	−.114	−.034	.067	.044	.043	.263	−.175
MAG1	.193	−.012	.045	.053	**.838**	.208	.065	.062	.035	−.039
MAG2	.064	.014	−.046	.063	**.782**	−.014	.040	.009	.066	.317
MAG3	−.018	.080	−.167	.156	**.787**	−.133	−.080	−.096	−.017	.287
SCP1	.072	.158	.043	.183	.055	**.751**	.049	.116	.044	−.009
SCP2	.155	.186	−.026	.090	.163	**.821**	.008	.047	.058	−.038
SCP3	.170	.179	−.002	.127	.173	**.835**	−.033	.063	.061	.022
OSC1	.160	.178	−.026	.161	.196	−.007	**.766**	.041	.187	−.010
OSC2	.246	.171	−.039	.159	.202	.020	**.803**	.037	.083	.022
WL1	−.020	.052	−.073	−.045	−.075	−.021	−.020	**.925**	.080	.035
WL2	.039	−.112	.068	−.109	.084	.002	.001	**.884**	−.060	.077
WL3	−.056	−.014	−.077	−.079	−.060	−.057	.028	**.943**	.085	.018
SP1	.124	.265	−.032	.030	.284	.066	−.055	−.014	**.750**	.161
SP2	.214	.165	−.043	.091	.223	.051	.010	.024	**.889**	−.026
SP3	.206	.223	−.008	.106	.201	.048	−.026	−.003	**.883**	−.026
CEL1	.278	.224	.295	−.032	.087	.060	.034	.055	−.065	**.807**
CEL2	.208	.228	.234	−.044	.161	.042	−.017	.052	−.030	**.792**
CEL3	.212	.209	.196	−.009	.144	−.044	.037	.065	−.014	**.807**
Cronbach's Alpha	0.79	0.66	0.86	0.96	0.90	0.92	0.89	0.92	0.93	0.93

Table 3. Correlation matrix for items.

	TRS1	TRS2	TRS3	PRV1	PRV2	PRV3	SN1	SN2	SN3	ITR1	ITR2	ITR3	M AG1	M AG2	M AG3	SCP1	SCP2	SCP3	OSC1	OSC2	WL1	WL2	WL3	SP1	SP2	SP3	CEL1	CEL2	CEL3
TRS1	1																												
TRS2	0.62	1																											
TRS3	0.56	0.51	1																										
PRV1	−.121	−.129	−.105	1																									
PRV2	.036	−.009	−.053	0.397	1																								
PRV3	−0.08	−0.08	−0.12	0.467	0.402	1																							
SN1	.020	.063	.051	0.112	.117	0.111	1																						
SN2	.109	.107	0.1	0.115	.135	0.129	0.58	1																					
SN3	.043	.058	.108	0.125	0.111	0.183	0.72	0.77	1																				
ITR1	.046	0.11	.019	.097	.008	.088	0.14	0.19	0.25	1																			
ITR2	.061	0.11	.046	.116	.039	.131	0.13	0.18	0.25	0.91	1																		
ITR3	.049	0.11	.079	.044	−.002	.099	0.17	0.2	0.11	0.89	0.89	1																	
M AG1	−.063	−.062	.137	0.209	0.142	0.183	0.14	0.2	0.18	0.18	0.16	0.18	1																
M AG2	.003	.124	.122	.119	.092	0.189	0.18	0.23	0.19	0.13	0.16	0.16	0.706	1															
M AG3	.022	.133	0.11	.118	.091	0.118	0.13	0.24	0.19	0.19	0.11	0.2	0.716	0.839	1														
SCP1	.000	.083	.110	0.143	.137	0.215	0.18	0.26	0.16	0.25	0.27	2443	0.322	0.278	0.256	1													
SCP2	.002	.060	.071	.120	.085	0.153	0.16	0.2	0.13	0.23	0.22	0.3	0.332	0.337	0.384	0.74	1												
SCP3	−.081	.033	.067	0.115	.078	0.175	0.19	0.22	0.12	0.23	0.22	0.21	0.362	0.398	0.335	0.83	0.84	1											
OSC1	.010	.002	.079	.139	.118	0.137	0.16	0.21	0.2	0.21	0.24	0.22	0.208	0.319	0.326	0.32	0.37	0.39	1										
OSC2	.020	.041	.103	.097	.084	0.176	0.13	0.23	0.22	0.23	0.22	0.26	0.281	0.391	0.304	0.33	0.33	0.33	0.801	1									
WL1	−.066	−.030	−.012	−.039	.017	−.039	−.020	−.040	−.050	−.090	−.123	−.125	−.016	−.003	−.007	−.013	−.046	−.038	−.051	−.051	1								
WL2	−.063	−.060	.024	.020	.033	−.099	−.045	.012	−.056	−.014	−.007	−.051	.020	−.030	.054	.031	−.040	−.009	−.023	−.012	0.71	1							
WL3	−.106	−.073	−.041	−.013	.054	−.024	−.075	−.063	−.075	−.132	−.138	−0.19	−.065	−.097	−.062	−.044	−.090	−.073	−.094	−0.14	0.87	0.77	1						
SP1	.040	.100	.139	−.002	−.030	−.020	0.19	0.28	0.3	0.21	0.21	0.26	0.238	0.152	0.144	0.27	0.33	0.35	0.39	0.313	−.049	−.022	−.100	1					
SP2	.061	0.1	.059	.010	−.053	0.159	0.15	0.29	0.23	0.29	0.22	0.25	0.202	0.19	0.154	0.27	0.21	0.2	0.316	0.36	−.045	−.096	−.095	0.77	1				
SP3	.039	0.11	.056	−.018	−.084	.131	0.13	0.28	0.29	0.22	0.26	0.28	0.213	0.175	0.22	0.27	0.39	0.31	0.391	0.354	−.015	−.057	−.084	0.76	0.95	1			
CEL1	.084	.129	.079	.103	−.009	0.147	0.21	0.23	0.19	0.29	0.2	0.22	0.336	0.252	0.261	0.38	0.38	0.31	0.396	0.307	−.078	−.013	−.139	0.33	0.31	0.39	1		
CEL2	.083	.087	.092	.021	−.002	.101	0.12	0.26	0.12	0.29	0.25	0.21	0.336	0.214	2462	0.34	0.38	0.36	0.374	0.391	−.091	−.041	−.115	0.32	0.35	0.33	0.82	1	
CEL3	−.021	.029	.025	.050	.101	.129	0.14	0.26	0.16	0.25	0.24	0.26	0.327	0.29	0.216	0.32	0.35	0.35	0.369	0.364	−.062	−.004	−.093	0.37	0.35	0.35	0.81	0.8	1

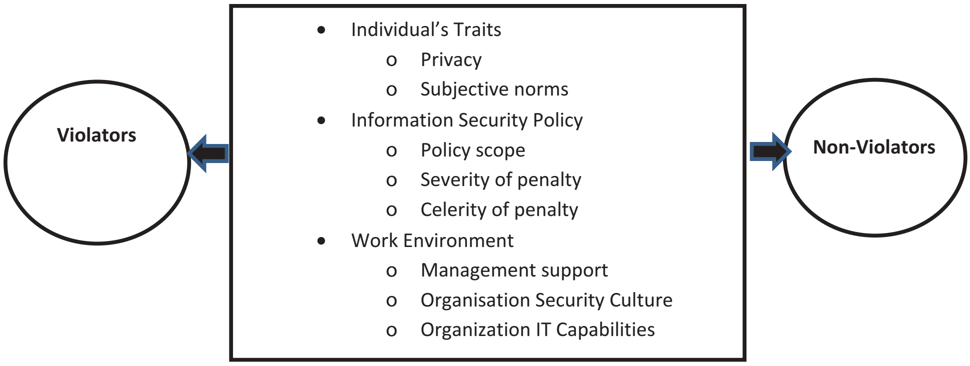

Figure 2. Significant factors.

Table 4. ANOVA results.

	Factors	Non-Violators $N = 111$ Mean	Non-Violators $N = 111$ Standard Deviation	Violators $N = 84$ Mean	Violators $N = 84$ Standard Deviation	F	Sig.	Effect Size*
H1	Trust	4.06	1.65	4.21	1.44	0.486	0.487	
H2	Privacy	6.25	0.68	5.92	0.865	9.05	0.003	0.42
H3	Subjective Norm	5.76	1.10	5.39	1.11	5.388	0.021	0.33
H4	Policy Scope	4.91	1.45	4.51	1.20	4.202	0.042	0.30
H5	Severity of penalty	4.80	1.41	4.12	1.22	12.296	0.001	0.50
H6	Celerity of Penalty	4.52	1.44	3.86	1.11	12.327	0.001	0.49
H7	Management Support	5.42	1.23	5.06	1.34	4.024	0.048	0.28
H8	Organizational Security Culture	4.98	1.30	4.52	1.25	6.084	0.015	0.35
H9	Workload	4.34	1.48	4.64	1.46	1.859	0.174	
H10	Organization IT Capability	6.07	1.34	4.50	1.23	9.246	0.003	1.20

*. A measure of practical significance; it is calculated as follows: the effect size (d) = Difference in means for the two groups divided by the pooled standard deviation (Stevens 1996).

Table 5. A summary of hypotheses testing results.

Hypothesis	Result	Remarks
H1	Not Supported	The trust has no effect on both groups (violators and non-violators)
H2	Supported	Privacy could differentiate between the two groups in the sense that non-violators were more concern about protecting their own personal information as well as other people information.
H3	Supported	Subjective norm could differentiate the two groups in the sense that non-violators, compared to violators, were more impacted by their influential circles of people around them.
H4	Supported	Policy scope could differentiate the two groups in the sense that non-violators agreed that the information security policy is clear and well communicated.
H5	Supported	The severity of penalty for violation of information security policy could distinguish the two groups in the sense that non-violators strongly believed in the severity of the penalty.
H6	Supported	Celerity of the penalty could make a distinction between the two groups in the sense that non-violators believe the enforcement of the penalty will be fast and in a timely manner.
H7	Supported	Management support for implementing information security policy could differentiate the two groups in the sense that non-violators felt that their management provide the necessary support for implementing information security policy.
H8	Supported	Organizational security culture could separate the two groups in the sense that non-violators believe that their organization promotes information security culture.
H9	Not supported	The workload could not be used as a distinguisher between the two groups.
H10	Supported	Organization IT capability could differentiate the two groups in the sense that non-violators, compared to violators, had more confidence in their organization IT capability in securing their systems.

Table 6. Chi-Square results for demographic effects.

Variable	Chi-Square	Significance level	Conclusion
Gender	1.732	0.188	Violation of information security measure does not depend on gender.
Age	1.487	0.223	Violation of information security measure does not depend on age .
Educational level	0.087	0.768	Violation of information security measure does not depend on educational level.
Experience	3.395	0.183	Violation of information security measure does not depend on employee's experience.
Managerial role	0.171	0.679	Violation of information security measure does not depend on whether the employee has a managerial role or not.
Job title (position)	2.965	0.397	Violation of information security measure does not depend on the employee's job title (e.g., administrator or director).
Percentage of computer usage	0.230	0.891	Violation of information security measure does not depend on the percentage of computer usage at work.

effect, 0.5 Medium, 0.8 large, and 1.3 very large effect]. Based on the magnitude of the effective size, one can conclude that among all factors in the three categories, perception about organization IT capability (effective size = 1.2) was the most distinguishing factor between the two groups, followed by severity of penalty (0.5), and celerity of the penalty (0.49). On the other hand, the least important factor in separating the two groups was management support (0.28), followed by policy scope (0.30).

8. Managerial implications

The results indicate that violators and non-violators of information security measures differ significantly with respect to three main categories of factors that influence personnel to violate information security measures. For example, regarding the privacy issue which affects the behavior of the people with respect to violating information security measures, violators are less sensitive to privacy issue compared to non-violators. Likewise, they are less affected by the severity and celerity of the penalty of violation of information security measures. Therefore, management should make it clear to its employees that there is no tolerance in applying a severe penalty once the violations have occurred. There are a number of previous researches including: Robinson (2018); Khan, Omonaiye, and Madhavi Lalitha (2017); Brink (2011); and Lowry et al. (2015) found their outcomes in the line of this study in terms of management role and the penalty of violation of information measure. Moreover, management needs to communicate and educate its employees regarding its IT capability in dealing with any information security violations because non-violators had the impression that their company does have IT capability to capture violations of information security measures. Similar to this outcome the researches of Kabanda, Tanner, and Kent (2018) and Brock and Khan (2017) advocates the same pattern. Additionally, organizations should promote an information security culture, which emphasizes knowledge sharing and provides a clear information security policy scope. Table 7 provides management with a taxonomy of significant factors that differentiate the violators from the non-violators. This taxonomy provides a distinct line that could distinguish the character of the violators from their counterparts, the non-violators. For example, management needs As the two groups differ on the privacy issues, management needs to educate their employees regarding privacy issues such as respecting others privacy and protecting one's personal information. Moreover, management may rely on the non-violators and close people of the violators who may influence their perceptions regarding the privacy as well as other issues related to violation of information security measures.

Individual end-users need to adapt the non-violators' behavior, follow and respect the information security rules by being more sensitive to privacy issues, and listening to advice related to security violation issues by their close relatives and friends. Moreover, the end-users should have a clear understanding of the security policy of their company and have a strong confidence in the capability of their management in capturing security violations and enforcing the severe penalty on the information security violators.

Table 7. Violators versus non-violators profiles.

Factor	Violators	Non-Violators	Recommended Actions for Management
Organizational IT Capability	Perceived as it is less capable	Perceived as it is capable	Ensure the readiness of IT infrastructure in protecting its IT resources and preventing any violations of information security measures.
Severity of penalty	Perceived as less severe	Perceived as more severe	Revisit its corrective actions by increasing the penalty.
Celerity of penalty	Perceived as being not fast	Perceived as being relatively fast	Management needs to enforce the penalty
Privacy issue	Less sensitive	More sensitive	Educating employees about the importance of privacy policy. This could be accomplished by offering training sessions and workshops provided by the experts in this field
Organizational security culture	Perceived as it is less evident	Perceived as it is evident	Support the IT staff in promoting and creating information security culture among the employees by providing necessary resources and fostering information security orientation.
IS policy scope	Perceived as less clear	Perceived as relatively clear	Make information security rules and measures very clear and simple so that they can be easily followed and implemented.

9. Limitations and future research

As with any other exploratory study, this study also has limitations, such as relatively small sample size and confined to one institution. This may limit the generalizability of the results and self-reported information, which raises the possibility of common method variance concern. To test that, Harman's single factor test is employed and it is found that only 33% of the variance is accounted for one factor (less than the threshold value of 50%) (Podsakoff et al. 2003). This result suggests that a common method variance is unlikely to confound the interpretation of the results of this study. Therefore, researchers are encouraged to consider testing the same factors in different organizations. A plausible future research project could include more factors that might influence employees' behavior such as personal innovativeness and awareness of security measures. It would be interesting to examine if the interaction effect between demographic variables and violations of information security policy exist. For example, does gender behave differently under different organizational culture or under different levels of severity/celerity of penalty? Another potential future research endeavor could be replicating the study across different cultures and countries.

10. Conclusion

The primary objectives of this study are: 1) to investigate the differences between violators and non-violators of information security measures on a number of related factors; and 2) to examine the impact of demographic factors on the participant's responses. The results indicated that there are significant differences in means of privacy, subjective norms, perceived information security policy scope, perceived severity of the penalty, perceived celerity of penalty, management support, organizational security culture, and perceived organizational IT capability between violators and non-violators. The empirical research findings suggest that violation of information security measures is independent of gender, age, educational level, experience, job title (position), managerial role, and percentage of computer usage at work.

Toward these ends, the study achieved its objectives. Additionally, the present study offers a basis for conducting comparative research across different countries. The authors hope that the findings will stimulate further research in this area.

ORCID

Habib Ullah Khan http://orcid.org/0000-0001-8373-2781

References

Abawajy, J. 2014. User preference of cyber security awareness delivery methods. *Behavior and Information Technology* 33 (3):236–47. doi:10.1080/0144929X.2012.708787.

Ajzen, I. 1991. The theory of planned behavior. *Organizational Behavior and Human Decision Processes* 50 (2):179–211. doi:10.1016/0749-5978(91)90020-T.

Al Hogail, A. 2015. Design and validation of information security culture framework. *Computers in Human Behavior* 49:567–75. doi:10.1016/j.chb.2015.03.054.

Al Hogail, A., A. Mirza, and S. H. Bakry. 2015. A comprehensive human factor framework for information security in organizations. *Journal of Theoretical and Applied Information Technology* 78 (2):201–11.

Albrechtsen, E., and J. Hovden. 2009. The information security digital divide between information security managers and users. *Computers & Security* 28:476–90. doi:10.1016/j.cose.2009.01.003.

Alhogail, A., and A. Mirza. 2014a. A framework of information security culture change. *Journal of Theoretical and Applied Information Technology* 64 (2):540–49.

Allam, S., S. V. Flowerday, and E. Flowerday. 2014. Smartphone information security awareness: A victim of operational pressures. *Computers & Security* 42:56–65. doi:10.1016/j.cose.2014.01.005.

Allen, M. 2006. Social engineering: A means to violate a computer system, he SANS Institute. www.sans.org.

Al-Omari, A., A. Deokar, O. El-Gayar, J. Walters, and H. Aleassa 2013. Information security policy compliance: An empirical study of ethical ideology, 46th Hawaii International Conference on System Sciences, IEEE, Grand Wailea, Maui, Hawaii.

Al-Omari, A., O. El-Gayar, and A. Deokar 2012. Security policy compliance user acceptance perspective. Proceedings of the 45th Annual Hawaii International Conference on System Sciences (HICSS-45 '12), HI, Wailea, Maui, Hawaii.

Al-Share, K., and P. Lane 2008. A conceptual model for explaining violations of the information security policy (ISP): A Cross cultural perspective. Proceedings of AMCIS 2008, Toronto, Ontario, Canada.

Arian, T., A. Kusedghi, B. Raahemi, and A. Akbari. 2017. A collaborative load balancer for network intrusion detection in cloud environments. *Journal of Computers* 12 (1):28–47. doi:10.17706/jcp.12.1.28-47.

Asai, T., and A. U. Hakizabera. 2011. Human-Related problems in information security in Thai Cross-Cultural Environments. *Contemporary Management Research* 7 (2):117–42. doi:10.7903/cmr.6191.

Astakhova, L. V. 2016. The ontological status of trust in information security. *Scientific and Technical Information Processing* 43 (1):58–65. doi:10.3103/S0147688216010123.

Aurigemma, S. 2013. A composite framework for behavioral compliance with information security policies. *Journal of Organizational and End User Computing* 25 (3):67–82. doi:10.4018/joeuc.2013070103.

Aurigemma, S., and R. Panko 2012. A composite framework for behavioral compliance with information security policies. Proceedings of 45th Hawaii International Conference on System Sciences, Maui, Hawaii USA, pp: 3248–57.

Awan, M. A., H. U. Khan, and W. Zhang. 2012. . A comparative study on online service quality perception of two major regional economies. *International Journal of e-Education, e-Business, e-Management and e-Learning (IJEEEE)* 2 (6):529–51.

Barlow, J. B., M. Warkentin, D. Ormond, and A. R. Dennis. 2013. Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security* 39:145–59. doi:10.1016/j.cose.2013.05.006.

Bashir, G. M., and H. U. Khan 2016. Factors affecting learning capacity of information technology concepts. A Classroom Environment Of Adult Learner, 15th International Conference on Information Technology Based Higher Education and Training (IEEE Conference), Istanbul, Turkey, September 8th – September 10, 2016. (Conference Proceeding).

Battmann, W., and P. Klumb. 1993. Behavioural economic and compliance with safety regulations. *Safety Science* 16 (1):35–46. doi:10.1016/0925-7535(93)90005-X.

Boehmer, J., R. LaRose, N. Rifon, S. Alhabash, and S. Cotten. 2015. Determinants of online safety behavior: Towards an intervention strategy for college students. *Behavior & Information Technology* 34 (10):1022–35. doi:10.1080/0144929X.2015.1028448.

Boss, S. R., L. J. Kirsch, I. Angermeier, R. A. Shingler, and R. W. Boss. 2009. If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems* 18 (2):151–64. doi:10.1057/ejis.2009.8.

Boulder, C. O. 2010. New web root survey reveals poor password practices that may put consumers' identities at risk. Accessed October 2, 2018. www.webroot.com

Brady, J. W. 2011. Securing health care: Assessing factors that affect HIPAA security compliance in academic medical centers. Proceedings of the 44th Hawaii International Conference on System Sciences, IEEE, Koloa, Kauai, Hawaii.

Brink, A. 2011. *Corporate governance and ethics: An introduction*. Dordrecht Heidelberg London New York: Springer.

Brock, V. F., and H. U. Khan. 2017. Big data analytics: Does organizational factor matters impact technology acceptance? *Journal of Big Data* 4 (1):28. doi:10.1186/s40537-017-0081-8.

Bulgurcu, B., H. Cavusoglu, and I. Benbasat. 2010. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly* 34 (3):523–48. doi:10.2307/25750690.

Chang, S. E., and C. S. Lin. 2007. Exploring organizational culture for information security management. *Industrial Management & Data Systems* 107 (3):438–58. doi:10.1108/02635570710734316.
Cheng, L., Y. Li, W. Li, E. Hol, and A. Zhaic. 2013. Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security* 39:447–59. doi:10.1016/j.cose.2013.09.009.
Cisco. 2013. BYOD insights 2013. Accessed October 2, 2018. http://www.ciscomcon.com/sw/swchannel/registration/internet/registration.cfm?SWAPPID=91&RegPageID=350200& SWTHEMEID=12949
Cohen, J. 1977. *Statistics power analysis for the behavioral sciences*. New York: Academic Press.
Connollyl, L., M. Lang, and D. Tygart. 2014. Managing employee security behaviour in organizations: The role of cultural factors and individual values. *International Federation for Information Processing* 428:417–30.
Culnan, M. J., and C. C. Williams. 2009. How ethics can enhance organizational privacy: Lessons *from* the choice point and TJX data breaches. *MIS Quarterly* 33 (4):673–87. doi:10.2307/20650322.
D'Arcy, J., T. Herath, and M. K. Shoss. 2014. Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems* 31 (2):285–318. doi:10.2753/MIS0742-1222310210.
D'Arcy, J., A. Hovav, and D. F. Galletta. 2009. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research* 20 (1):79–98. doi:10.1287/isre.1070.0160.
Dinev, T., Q. Hu, Z. Xu, and H. Ling. 2011. Does deterrence work in reducing information security policy abuse by employees. *Association for Computer Machinery (ACM)* 54 (6):54–60.
Durgin, M. 2007 Understanding the Importance of and Implementing Internal Security Measures", SANS Institute, InfoSec Reading Room, Available at: www.sans.org (Accessed October 2, 2018).
Etezady, N. 2011. The impact of ERP investments on organizational performance. *International Journal of the Academic Business World* 5 (2):27–33.
Gadzama, W. A., J. I. Katuka, Y. Gambo, A. M. Abali, and M. J. Usman. 2014. Evaluation *of* employees awareness and usage of information security policy in organizations of developing countrties: A study of federal inland revenue service, Nigeria. *Journal of Theoretical and Applied Information Technology* 67 (2):443–60.
Gilbert, E., and T. Mitra 2012. Have you heard? How gossip flows through workplace email. Proceedings of the Sixth International Conference on Weblogs and Social Media", Dublin, Ireland, Accessed June 4–7, 2012.
Gist, M. 1987. Self-efficacy: Implications for organizational behavior and human resource management. *Academy of Management Review* 12 (3):472–85. doi:10.5465/amr.1987.4306562.
Goel, S., and H. A. Shawky. 2009. Estimating the market security breach announcements on firm values. *Information & Management* 46 (7):404–10. doi:10.1016/j.im.2009.06.005.
Greene, G., and J. D'Arcy 2010. Assessing the impact of security culture and the employee-organization relationship on IS security compliance. Fifth Annual Symposium on Information Assurance, NY.
Guo, K. H., Y. Yuan, N. P. Archer, and C. E. Connelly. 2011. Understanding non- malicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems* 28 (2):203–36. doi:10.2753/MIS0742-1222280208.
Hair, J., B. Black, B. Babin, R. Anderson, and R. Tatham. 2006. *Multivariate data analysis*. Upper Saddle River, NJ: Pearson Prentice Hall.
Hassan, I. M., H. U. Khan, R. Zaitun, and G. Mardini 2015. Pedagogical potentials of IEEE 802.11 WLAN to higher educational institutions: A case study of Nigerian based University. IEEE 9th International Conference on Semantic Computing (IEEE ICSC 2015), Anhaim, CA, USA, Accessed February 7-9, 2015. (Conference Proceeding).
Hassan, N. H., and Z. Ismail. 2016. Information security culture in healthcare informatics: A preliminary investigation. *Journal of Theoretical and Applied Information Technology* 88 (2):202–09.
Herath, T., and H. R. Rao. 2009. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems* 47 (2):154–65. doi:10.1016/j.dss.2009.02.005.
Hu, Q., T. Dinev, P. Hart, and D. Cooke. 2012. Managing employee compliance with information security policies: The critical role of top management organizational culture. *Decision Sciences* 43 (4):615–59. doi:10.1111/j.1540-5915.2012.00361.x.
Hu, Q., R. West, and L. Smarandescu. 2015. The role of self-control in information security violations: Insights from a cognitive neuroscience perspective. *Journal of Management Information Systems* 31 (4):6–48. doi:10.1080/07421222.2014.1001255.
Humaidi, N., and V. Balakrishnan. 2015. The moderating effect of working experience on health information system security policies compliance behavior. *Malaysian Journal of Computer Science* 28 (2):70–92.
Ifinedo, P. 2014. Information security policy compliance: An empirical study of the effects of socialization, influence, and cognition. *Information & Management* 51 (1):69–79. doi:10.1016/j.im.2013.10.001.
Johnston, A. C., M. Warkentin, M. McBride, and L. Carter. 2016. Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems* 25 (3):231–51. doi:10.1057/ejis.2015.15.

Kabanda, S., M. Tanner, and C. Kent. 2018. Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce* 28 (3):269–82. doi:10.1080/10919392.2018.1484598.

Kearney, W. D., and H. A. Kruger. 2016. Can perceptual differences account for enigmatic information security behavior in an organization? *Computers and Security* 61:46–58. doi:10.1016/j.cose.2016.05.006.

Khan, H. U., and A. C. Ejike. 2017. An assessment of the impact of mobile banking on traditional banking in Nigeria. *International Journal of Business Excellence* 11 (4):446–63. doi:10.1504/IJBEX.2017.082573.

Khan, H. U., J. F. Omonaiye, and V. V. Madhavi Lalitha. 2017. Employees' perception as internal customers about online services: A case study of banking sector in Nigeria. *International Journal of Business Innovation and Research* 13 (2):181–202. doi:10.1504/IJBIR.2017.083540.

Khan, H. U., and S. Uwemi. 2018. Possible impact of E-commerce strategies on the utilization of E-commerce in Nigeria'. *International Journal of Business Innovation and Research* 15 (2):231–46. doi:10.1504/IJBIR.2018.089145.

Knapp, K. J., and C. J. Ferrante. 2012. Policy awareness, enforcement and maintenance: Critical to information security effectiveness in organizations. *Journal of Management Policy and Practice* 13 (5):66–80.

Kraemer, S., and P. Carayon. 2007. Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics* 38 (2):143–54. doi:10.1016/j.apergo.2006.10.007.

Li, H., J. Zhang, and R. Sarathy. 2010. Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems* 48 (4):635–45. doi:10.1016/j.dss.2009.12.005.

Lin, K. M. 2016. Understanding undergraduates' problems from determinants of Facebook continuance intention. *Behavior and Information Technology* 35 (9):693–705. doi:10.1080/0144929X.2016.1177114.

Lowry, P. B., C. Posey, R. Bennett, and T. L. Roberts. 2015. Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organizational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal* 25 (3):193–273. doi:10.1111/isj.12063.

Mahesh, S., and A. Hooter 2013. Managing and securing business networks in the smartphone era. Proceedings of *Annual General Business Conference*, Sam Houston State University, Houston, Texas, USA, 1–17.

Mahmoud, F. Z. M., and A. M. Zeki. 2016. Edward Snowden disclosures turn the fears of surveillance into reality: The impact and transformation in information security. *Journal of Theoretical and Applied Information Technology* 83 (2):173–79.

Martin, N., J. Rice, and R. Martin. 2016. Expectations of privacy and trust: Examining the views of IT professionals. *Behavior & Information Technology* 35 (6):500–10. doi:10.1080/0144929X.2015.1066444.

Musa, A., H. U. Khan, and K. Alshare. 2015. Factors influence consumers' adoption of mobile payment devices in Qatar. *International Journal of Mobile Communications* 13 (6):670–89. doi:10.1504/IJMC.2015.072100.

Myler, E., and G. Broadbent. 2006. ISO 17799: Standard for security. *Information Management Journal* 40 (6):43–52.

Mylonas, A., D. Gritzalis, B. Tsoumas, and T. A. Apostolopoulos 2013. A qualitative metrics vector for the awareness of smartphone security users. Proceedings of the 10th international conference on trust, privacy, and security in digital business, Springer, Prague, Czech Republic, 173–84 (LNCS-8058).

Myyry, L., M. Siponen, S. Pahnila, and A. Vance. 2009. What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems* 18 (2):126–39. doi:10.1057/ejis.2009.10.

Nagin, D., and G. Pogarsky. 2001. Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: Theory and evidence. *Criminology; an Interdisciplinary Journal* 39 (4):865–92. doi:10.1111/crim.2001.39.issue-4.

Padayachee, K. 2012. Taxonomy of complaint information security behavior. *Computers & Security* 31 (5):673–80. doi:10.1016/j.cose.2012.04.004.

Park, E. H., J. Kim, and Y. S. Park. 2017. The role of information security learning and individual factors in disclosing patients' health information. *Computers and Security* 65:64–76. doi:10.1016/j.cose.2016.10.011.

Parsons, K., A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram. 2014. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security* 42:165–76. doi:10.1016/j.cose.2013.12.003.

Podsakoff, P. M., S. B. MacKenzie, J.-Y. Lee, and N. P. Podsakoff. 2003. Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology* 88 (5):879–903. doi:10.1037/0021-9010.88.5.879.

Predd, J., S. L. Pfleeger, J. Hunker, and C. Bulford. 2010. Insiders behaving badly. *Security & Privacy, IEEE* 6 (4):66–70. doi:10.1109/MSP.2008.87.

Putri, F., and A. Hovav 2014. Employees' compliance with BYOD security policy: Insights from reactance, organizational justice, and protection motivation theory. Twenty Second European Conference on Information Systems, Tel Aviv 2014, Tel Aviv, Israel, 1–17.

Rodinson, S. C. 2018. Factors predicting attitude toward disclosing personal data online. *Journal of Organizational Computing and Electronic Commerce* 28 (3):214–33. doi:10.1080/10919392.2018.1482601.

Safa, N., M. Sookhak, R. Solms, S. Furnell, N. Abdul Ghani, and T. Herawan. 2015. Information security conscious care behaviour formation in organizations. *Computer and Security* 53:65–78. doi:10.1016/j.cose.2015.05.012.

Safa, N. S., and R. Von Solms. 2016. An information security knowledge sharing model in organizations. *Computers in Human Behavior* 57:442–51. doi:10.1016/j.chb.2015.12.037.

Saunders, A., and E. Brynjolfsson. 2016. Valuing information technology related intangible assets. *MIS Quarterly* 40 (1):83–110. doi:10.25300/MISQ.

Schoepfer, A., S. Carmichael, and N. L. Piquero. 2007. Do perceptions of punishment vary between white-collar and street crimes? *Journal of Criminal Justice* 35:151–63. doi:10.1016/j.jcrimjus.2007.01.003.

Seyal, A. H., and R. Turner. 2013. A study of executives' use of biometrics: An application of theory of planned behavior. *Behavior & Information Technology* 32 (12):1242–56. doi:10.1080/0144929x.2012.659217.

Siponen, M., S. Pahnila, and A. Vance. 2012. Motivating IS Security policy compliance: Insights from habits and protection motivation theory. *Information and Management* 49:190–98. doi:10.1016/j.im.2012.04.002.

Siponen, M., and A. Vance. 2010. Neutralization: New insight into the problem of employee IS security policy violations. *MIS Quarterly* 34 (3):487–502. doi:10.2307/25750688.

Sommestad, T., J. Hallberg, L. K. Lundholm, and J. Bengtsson. 2014. Variables influencing information security policy compliance – A systematic review of quantitative studies. *Information Management & Computer Security* 22 (1):42–75. doi:10.1108/IMCS-08-2012-0045.

Son, J.-Y. 2011. Out of fear or desire? Towards a better understanding of employees' motivation to follow IS security policies. *Information & Management* 48:296–302. doi:10.1016/j.im.2011.07.002.

Stevens, J. 1996. *Applied multivariate statistics for the social sciences*. Mahwah. New Jersey: Lawrence Erlbaum.

Takemura, T. 2012. Who sometimes violates the rule of the organizations? Empirical Study on Information Security Behaviors and Awareness. Accessed May 3, 2018. http://weis2012.econinfosec.org/papers/Takemura_WEIS2012.pdf

Tamjidyamcholo, A., M. S. Bin Baba, H. Tamjid, and R. Gholipour. 2013. Information security - Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language. *Computers and Education* 68:223–32. doi:10.1016/j.compedu.2013.05.010.

Warkentin, M., and R. Wilson. 2009. Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems* 8 (4):101–05. doi:10.1057/ejis.2009.12.

Watters, P. A., and J. Ziegler. 2016. Controlling information behaviour: The case for access control. *Behavior and Information Technology* 35 (4):268–76. doi:10.1080/0144929X.2015.1128976.

Zhang, J., B. J. Reithel, and H. Li. 2009. Impact of perceived technical protection on security behaviors. *Information Management & Computer Security* 17 (4):330–40. doi:10.1108/09685220910993980.

Zviran, M. 2008. User's perspectives on privacy in web-based applications. *Journal of Computer Information Systems* 48 (4): 97–105.

Notes on contributors

Habib Ullah Khan is an Associate Professor of MIS in the Department of Accounting & Information Systems, College of Business and Economics, Qatar University, Qatar. He completed his Ph.D. degree in Management Information Systems from Leeds Metropolitan University, UK. He has more than 18 years of industry, teaching and research experience. He is an active researcher and his research work published in leading journals of the MIS field. His research interests are in the area of IT Security, Online Behaviour, IT Adoption in Supply Chain Management, Internet Addiction, Mobile Commerce, Computer Mediated Communication, IT Outsourcing, Big data, cloud computing, and E-learning. He is member of such leading professional organizations as IEEE, DSI, SWDSI, ABIS, FBD, and EFMD. He is a reviewer of leading journals of his field and also working as an editor for some journals.

Khalid A. AlShare is a Professor of Information Systems at Qatar University. He received his Ph.D. from the University of Texas at Arlington. His teaching interests include database systems, systems analysis and design, strategic MIS, and project management. His research interests include technology acceptance models, behavioral information security, cross-cultural studies in MIS, distance education, and data envelopment analysis. His work has appeared in various academic journals. He has served numerous professional organizations such as the DSI (session chair, reviewer), SWDSI (Council member, track chair, session chair, discussant, and reviewer), AMCIS (mini-track chair, session chair, and reviewer), and The Consortium for Computing Sciences in Colleges (board member, papers chair, and treasurer).

Appendix A

List of Scale Items

Construct	Item	Description	Mean	Std.
Trust	TRS1	I am not worried about revealing information related to my job to my co-workers	4.28	1.89
α = 0.79	TRS2	I am willing to provide my co-workers with access to my computer system at work	3.19	2.00
	TRS3	I have trust in my co-workers in sharing information related to my job	4.92	1.68
Privacy	PRV1	I am concerned about protecting the information privacy of others	6.40	.776
α = 0.66	PRV2	I am cautious about revealing my own personal information	6.35	.893
	PRV3	I consider information privacy as one of my major concerns	5.58	1.307
Subjective Norms α = 0.86	SN1	People who are important to me think that I should respect the information security measures set forth by my organization.	5.93	1.08
	SN2	My co-workers encourage me to apply my organization's measures (standards) for information security	5.25	1.43
	SN3	People who influence my behavior think I should understand and value my organization's policies regarding information security	5.64	1.25
Organizational IT capability	ITR1	If I committed an information security violation on the computer system, my organization would catch me	4.84	1.39
α = 0.96	ITR2	If I committed an information security violation on the computer system, the probability that my organization would catch me is high	4.88	1.41
	ITR3	Employees committing an information security violation on the computer system will be caught by my organization	4.76	1.32
Management Support	MAG1	Management understands the importance of information security within my organization	5.68	1.29
α = 0.9	MAG2	Management provides necessary help and resources to implement information security efforts	5.01	1.46
	MAG3	Management gives strong and consistent support to information security efforts	5.11	1.47
ISP SCOPE	SCP1	Our information security rules are clear and understandable.	5.02	1.43
α = 0.92	SCP2	The scope of our information security rules is well communicated to everyone in the organization.	5.54	1.54
	SCP3	The scope of our information security rules provide clear direction for employees for what is permitted and forbidden	4.67	1.41
Organizational	OSC1	The overall organization environment fosters information security minded thinking.	4.82	1.361
security culture α = 0.89	OSC2	Information security is a key norm shared by the members in our organization	4.75	1.381
Work load	WL1	The amount of work I am expected to do is too great.	4.24	1.58
α = 0.92	WL2	I never seem to have enough time to get everything done at work	4.71	1.60
	WL3	It often seems like I have too much work for one person to do.	4.48	1.61
Severity of penalty α = 0.93	SP1	Employees caught committing an information security violation on the computer system will be punished by my organization.	4.77	1.447
	SP2	It is likely that the punishment given by my organization to employees who commit information security violations on the computer system would be severe	4.34	1.489
	SP3	Organizational sanctions for employee violations of information security on the computer system would be severe.	4.41	1.459
Celerity of sanction α = 0.93	CEL1	My organization's response to information security violations on the computer system by employees would be instantaneous	4.16	1.434
	CEL2	Very little time would elapse between detection of information security violations on the computer system by employees and my organization's disciplinary response to them.	4.21	1.489
	CEL3	My organization's response process to employee violations of information security on the computer system would be very timely	4.35	1.422