Information security policy compliance: a higher education case study

Khaled A. Alshare
Department of Accounting and Information Systems, Qatar University, Doha, Qatar

Peggy L. Lane
School of Accounting, Financial and Information Services, University of Louisiana at Monroe, Monroe, Louisiana, USA, and

Michael R. Lane
Stephen L. Craig School of Business, Missouri Western State University, Saint Joseph, Missouri, USA

Received 3 August 2015
Revised 9 September 2016
15 March 2017
29 June 2017
Accepted 4 October 2017

Abstract

Purpose – The purpose of this case study is to examine the factors that impact higher education employees' violations of information security policy by developing a research model based on grounded theories such as deterrence theory, neutralization theory and justice theory.

Design/methodology/approach – The research model was tested using 195 usable responses. After conducting model validation, the hypotheses were tested using multiple linear regression.

Findings – The results of the study revealed that procedural justice, distributive justice, severity and celerity of sanction, privacy, responsibility and organizational security culture were significant predictors of violations of information security measures. Only interactional justice was not significant.

Research limitations/implications – As with any exploratory case study, this research has limitations such as the self-reported information and the method of measuring the violation of information security measures. The method of measuring information security violations has been a challenge for researchers. Of course, the best method is to capture the actual behavior. Another limitation to this case study which might have affected the results is the significant number of faculty members in the respondent pool. The shared governance culture of faculty members on a US university campus might bias the results more than in a company environment. Caution should be applied when generalizing the results of this case study.

Practical implications – The findings validate past research and should encourage managers to ensure employees are involved with developing and implementing information security measures. Additionally, the information security measures should be applied consistently and in a timely manner. Past research has focused more on the certainty and severity of sanctions and not as much on the celerity or swiftness of applying sanctions. The results of this research indicate there is a need to be timely (swift) in applying sanctions. The importance of information security should be grounded in company culture. Employees should have a strong sense of treating company data as they would want their own data to be treated.

Social implications – Engaging employees in developing and implementing information security measures will reduce employees' violations. Additionally, giving employees the assurance that all are given the same treatment when it comes to applying sanctions will reduce the violations.

Originality/value – Setting and enforcing in a timely manner a solid sanction system will help in preventing information security violations. Moreover, creating a culture that fosters information security will help in positively affecting the employees' perceptions toward privacy and responsibility, which in turn, impacts information security violations. This case study applies some existing theories in the context of the US higher education environment. The results of this case study contributed to the

Information and Computer Security
Vol. 26 No. 1, 2018
pp. 91-108
© Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-09-2016-0073

extension of existing theories by including new factors, on one hand, and confirming previous findings, on the other hand.

Keywords Information security, Computer security, Information security policy, Information security policy compliance, Organizational justice theory, Violations of information security

Paper type Research paper

Introduction

The 24/7 nature of the internet has provided not only many opportunities but also many challenges including information security risks (Soomro *et al.*, 2016). Information security threats from insiders continue to be one of the greatest concerns to information systems security managers (Willison and Warkentin, 2013). Examples of cyber security incidents caused by employees can readily by found, and many of these breaches are accidental. For example, a staffer accidentally sent confidential information to a broker, including Social Security numbers of 2,400 insurance agents (Crosby, 2013). In another report, it was reported that "about 58 per cent of cyber security incidents in the public sector were caused by employees," according to the annual Verizon Data Breach Investigations Report (Government Security News, 2014). The breakdown of the 58 per cent is "about 34 per cent of cyber security incidents in the public sector were caused by employee accidents in handling data and about 24 per cent by unapproved or malicious data use" (Government Security News, 2014). External examples include:

> In the manufacturing and mining industries, cyber espionage, the largest data breach source, accounted for 30 per cent and 40 per cent of incidents, respectively. For utilities, 38 per cent of data breaches were caused by Web application attacks and 31 per cent by crimeware. (Government Security News, 2014).

Civilized societies have created laws to mitigate behaviors deemed to be unacceptable to their society. Research into the effectiveness of these laws has focused on several areas. In particular, Schoepfer *et al.* (2007) focused their research on the impact of the perception of the severity of sanctions' potential on criminal activities. Likewise, organizations create policies to mitigate behaviors which are unacceptable to the organization. One of those critical areas where such policies exist is information systems security. Organizations create information security policies (ISP) for a variety of reasons, ranging from data security, proprietary access to information or prevention from external penetration of the system to managing productivity of workers or employee use policies and restricting access to external sources. Numerous studies (Bulgurcu *et al.*, 2010; Ifinedo, 2016; Yazdanmehr and Wang, 2016) have studied the severity of sanctions in addition to other factors on information systems policy (ISP) compliance. The concept is that the greater the perception of severity of sanction, the less likely the individual will violate the ISP. Although penalties will not prevent accidental disclosures, any penalties imposed because of accidents may reduce future errors, as employees may be more careful to avoid such errors. In addition to studying the impact of sanctions and organizational security culture, other studies [Willison and Warkentin (2013) and Li *et al.* (2014)] suggest the use of or examine the impact of organizational justice theory on ISP compliance. The authors have examined the severity of sanctions context as one of the measures in this case study, as it relates to information security policy and violations of such policy by employees. Other factors included in this case study are celerity of sanction, organizational security culture, privacy, responsibility and organizational justice theory.

The paper is organized as follows: the following section provides a related literature review and the hypotheses. In the third section, a description of the survey development, data collection and statistical analysis are discussed. In the fourth section, data analysis is reported, which includes the sample profile and data reliability. Results and discussion are reported in the fifth section along with limitations and future directions for additional research. The findings are summarized in the conclusion section.

Literature review

In this case study, university employees were informed in the survey that information security measures could include information security policy, procedures and rules. We use the term "information security measures" to include any type of information security policy. In this section, factors that affect violations of information security measures are discussed and hypotheses are formulated. The factors include celerity of sanction, severity of penalty, organizational security culture, privacy, responsibility and three classifications from justice theory – procedural justice, interactional justice and distributive justice.

Celerity of sanction

Celerity of sanction is concerned with the swiftness with which a sanction is carried out. Bentham (1843) hypothesized that people will avoid criminal behavior if that behavior elicits swift, severe and certain punishment. Schoepfer *et al.* (2007, page 151) included a modern version of this hypothesis in their discussion on deterrence theory when they state, "The perceived threat of swift, certain, and severe sanctions will inhibit criminal activity." According to deterrence theory, people are in general rational in their actions, and they are less likely to commit criminal acts if the perceived certainty, severity, and celerity of sanction against the acts are greater than the benefits of committing the crime (Dinev *et al.*, 2011). Safa *et al.* (2016, p. 73) suggested that "relevance, timeliness, and consistency are the important characteristics of security awareness programmes." Interestingly, most of the research in the area of information security policy focuses on the certainty and severity of sanctions more than the swiftness or celerity of the sanction being enforced. For example, Friesen (2012) found that severity of punishment is a more effective deterrent than the probability of punishment. We hypothesize the more swift the sanctions are carried out, the more employees will avoid violating the information security measures:

H1. Celerity of sanction is negatively correlated with violations of information security measures.

Severity of penalty

In addition to clearly defining the scope, rules and regulations, information security policies may also explicitly state the consequences for non-compliant behavior that vary in severity based on the nature of the information security violation. A simple violation should trigger a mild corrective measure, while major violations would trigger punishments as severe as terminating the employment of the violator and, when appropriate, filing criminal or civil charges against the violators. According to deterrence theory, an employee would avoid a certain course of action that is considered a violation if they are aware that it would trigger a punishment which they consider severe. Ifinedo (2016) found that sanctions can discourage noncompliance with information security policy as long as the employee's concerns and the organization's concerns and liabilities are understood. Dinev *et al.* (2011) found that deterrence really works in reducing employee abuse of information systems. Interestingly, they found that if the perceived benefits from the abuse outweigh the risks, then employees will abuse the system. Hu *et al.* (2011, page 58) further found that:

> The individual's intrinsic satisfactions that would be gained from the misconduct, such as thrill and happiness, are even more influential than the extrinsic material gains, such as the possession of money and goods, on the behavioral choice of the individual.

Therefore, the penalties should be severe enough to effectively deter employees from violating the policy. Potential abusers would be deterred if they realize that they will be severely punished if caught. It also raises the cost of breaching the policy in relation to the perceived benefits, and therefore, according to the rational choice theory (Vance and Siponen, 2012), the employee would not be willing to violate the policy. The same argument is true for perceived severity and response with respect to rewards (protection motivation theory – Siponen, Pahnila, and Vance, 2012). If the severity of the response significantly exceeds the rewards, employees will be discouraged from violating the policy. To this end, D'Arcy *et al.* (2009) discuss increasing the perceived severity of penalty for information systems misuse. Based on the above discussion we posit the following hypothesis:

H2. Perception of severity of penalty is negatively correlated with violations of information security measures.

Organizational security culture

When a company has a culture of organizational security, employees are aware of the policies through educational efforts, as well as clear statements for penalties of violations (Straub, 1990), and information security is a "natural aspect of the daily activities of all members of an organization" (Chang and Lin 2007, p. 452). They (Chang and Lin, 2007) further remind us that information security is not just a technical problem but a management problem as well and requires the involvement of top management in establishing procedures, policies and organizational structures to improve information security. In a company with a strong organizational security culture, appropriate policies and procedures including sanctions and education programs regarding those policies will exist (Culnan and Williams, 2009). Bulgurcu *et al.* (2010) concluded the role of information security awareness positively affects attitude and outcome beliefs which impact an employee's intention to comply with the information security policy. Establishing an organizational security culture is important to the acceptance of and adherence to the information security measures. We therefore posit the following hypothesis:

H3. Strong organizational security culture is negatively correlated with *violations of information security measures.*

Privacy

With the many technological advances including mobile devices available to employees, data privacy can be problematic in any company. Newspapers and TV broadcasts include information about privacy violations more often than we would like. Culnan and Williams (2009) define privacy as the problems resulting from the storage, analysis, use or sharing of personal information generated by consumer transactions. Posey *et al.* (2011) found that when employees experience computer monitoring, there is an increase in internal computer abuse. When employees have a strong sense of respect for the privacy of their own data, they will be more likely to adhere to the information security measure and less likely to violate it. We posit that:

H4. Strong respect for privacy is negatively correlated with *violations of information security measures.*

Responsibility

Responsibility is another factor that could influence employee behavior. It refers to the employees' feeling of personal responsibility for protecting company assets. Even if companies invested in educating and training employees about the importance of information security policy, and its role and alignment with their daily activities, irresponsible employees could still violate the policy for reasons that would vary from personal gain, to contempt for the job or the manager to a lack of understanding that the behavior is placing the security of data at risk. According to Cisco System, Inc. (2008) study, 39 per cent of those surveyed answered that they would violate the information security policy because security was not a personal priority for them. Further, 38 per cent of those surveyed indicated that they would violate the policy because they simply did not care; 25 per cent said they often violated the policy because they were in a hurry. The answers above clearly demonstrate a serious lack of responsibility. Yazdanmehr and Wang (2016) suggest employees with a high ascription of responsibility toward an information security policy are less likely to deny their responsibility toward the policy. Culnan and Williams (2009) encourage companies to avoid decoupling the idea of customers' data and employees' data; they encourage their managers to ask when confronted with a privacy issue, "How would I feel if *my* information was handled in this way? (p. 685)" While there is a need to develop mechanisms to address such behaviors (which could be through deterrence), it might still be impossible to prevent a further major problem, because not all violations of information security measures are detectable. Adherence should come from the employee themselves. From the above we posit that:

H5. Responsibility is negatively correlated with *violations of information security measures.*

Organizational justice theory

Procedural, interactional and distributive are the three common classifications of justice (Eigen and Litwin, 2014). Procedural justice is concerned with the fairness of processes in the way decisions are made (Thibaut and Walker 1975; Lind *et al.*, 1988; Harcourt *et al.*, 2013). Interactional justice is concerned with the perceived fairness of interpersonal treatment (Bies and Moag, 1986). Distributive justice is concerned with the fairness or equity of outcomes or rewards (Folger, 1977). Before computers were ubiquitous in industry, Leventhal *et al.* (1980) discussed the idea that perceived fairness of policies and procedures significantly affected employee attitudes and behavior at work. Willison and Warkentin (2013) suggest using organizational justice to address the issue of employee disgruntlement. Li *et al.* (2014) examined organizational justice and ethics and concluded that organizations need to implement their use policies consistently across all employees. These three classifications of organizational justice theory are explained further in the literature review in the next sections.

Procedural justice

People want to have a say in decisions about the process and they want to know the process is fair. Knowing the process is free from personal biases and motivations and instead relies on objective data is important (Workman *et al.*, 2009). Having a way to appeal decisions that are felt to be made in error is also important (Baldwin *et al.*, 2008). When examining internet use policy compliance, Li *et al.* (2014) found that procedural justice directly influenced internet use policy compliance. We hypothesize that the more employees perceive procedural justice exists, the less likely they are to violate the information security measures. We therefore posit:

H6. Procedural justice is negatively correlated with *violations of information security measures.*

Interactional justice

Eigen and Litwin (2014) summarized findings in the literature by saying, interactional justice:

> Measures the extent to which employees believe their needs are taken into account in making decisions and the extent to which employees are provided with adequate explanations when decisions are finalized (p. 175).

The manner in which an aggrieved employee is treated with regard to interpersonal treatment and how the penalty is enacted heavily influence the employee's perceptions of the fairness of the procedures (Tyler and Blader, 2000). Factors influencing the perception of fairness include honesty, courtesy, respectfulness and appropriate professional decorum (Sheppard *et al.*, 1992). We posit the stronger the perception of interactional justice, the less likely employees are to violate the information security measures. The hypothesis is stated below:

H7. Interactional justice is negatively correlated with *violations of information security measures.*

Distributive justice

Willison and Warkentin (2013) explained the work by Adams (1965) who laid the groundwork for distributive justice. At the core of the idea is that individuals compare the ratio of their own output (rewards) and input (contributions) with a colleague's ratio. In the comparison process, the employee uses "normative expectations" learned through prior socialization and upbringing. When the comparison of the ratios is not as expected, the employee has feelings of inequity. Theories of distributive justice have been classified as reactive when the focus is on the reaction after the decision has been made or as proactive when the focus is on using appropriate decision-making rules to make sure the decisions are just when made (Greenberg, 1987). Harcourt *et al.* (2013, p. 311) suggested the outcomes include the allocation of both rewards and punishments and that the "importance of fairness increases as a decision's potential impact on an employee increases." In a related study, Li *et al.* (2014) found that distributive justice directly influenced internet use policy compliance. Based on the discussion above, we posit:

H8. Distributive justice is negatively correlated with *violations of information security measures.*

Based on the literature review and suggested hypotheses, the research model was proposed as depicted in Figure 1.

Methodology

Survey development

The questionnaire had three sections. The first section contained a few demographic questions that included gender, age, educational level, job type and experience. The second

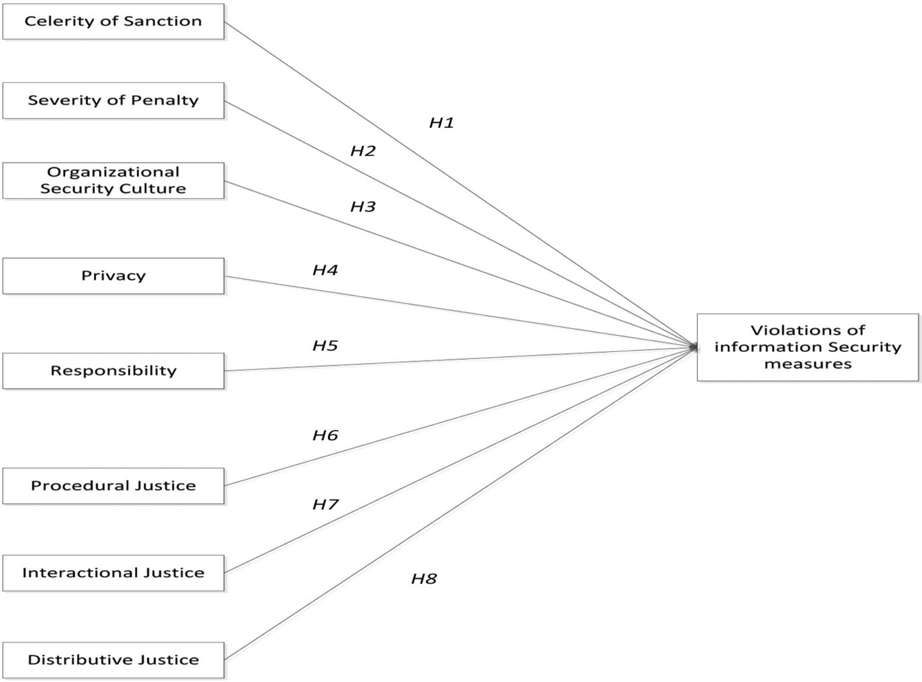


Figure 1. The proposed research model

section addressed the primary factors of the case study. Each construct included three statements which ranged from strongly disagree (1) to strongly agree (7), with the exception of one construct (organizational security culture) which was measured by two items. It is not unusual to use two items per construct as reported by Raubenheimer (2004) "Scales with more than one factor may be identified with as little as two items per factor." However, this should be the exception, especially if there is a need to improve the reliability of the scale. In our case, the reliability for the organizational security culture factor was 0.89.

The last section of the survey recorded the responses regarding violations of information security measures, which ranged from never (1) to very frequently (7), by asking the respondents eight statements such as "The following items refer to violations of information security measures (e.g. policies, procedures and/or rules):" an example of these statements is "One or more of my co-workers have deliberately bent or broken an information security measure."

The three items related to the severity of the penalty were adapted from Siponen and Vance (2010) and D'Arcy *et al.* (2009). Items related to responsibility were adapted from Asai and Hakizabera (2010). Items related to organizational justice dimensions (procedural, interactional and distributive) were adapted from Colquitt (2001), Asai and Hakizabera (2011), Dols and Silvius (2010), and Yalya (2011). Items for *violations of information security measures* and all other remaining items were developed by the authors. The list of items is reported in the Appendix.

Data collection

The data were collected using an online survey which was sent to all employees in a Midwestern university. Employees were asked to participate if they met the following two requirements:

(1) they are currently employed by the organization 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.

Before the survey was distributed openly to participants, it was pilot-tested. Many participants reported that the survey was too long, and therefore, the number of questions for each factor was reduced to 3. After addressing all of the comments from the pilot test, the survey was ready to be distributed to the intended audience. A total of 208 responses were collected. Five respondents indicated that they did not wish to participate, three did not meet the participation criteria and five responses were incomplete. Thus, 195 completed responses were used in the analysis.

Statistical analysis

The statistical analysis was carried out by using Statistical Package for the Social Sciences (SPSS 22). Descriptive data analyses, such as frequencies, means and standard deviations were calculated. The reliability of the constructs was evaluated using Cronbach's alpha. The validity of the constructs was assessed by performing factor analysis on all items that measure the model constructs. Principal component analysis with varimax was used. After assessing the reliability and the validity of the constructs, multiple linear regression was used to test the proposed hypotheses.

Data analysis

Sample profile

In total, 55 per cent of the participants were females. The average age of the participants was 50 years. About 63 per cent of the respondents hold graduate degrees. With respect to the participants' job title, the highest number (31 per cent) were faculty, the next category was director with 27 per cent. The level of experience in their current organization was approximately equally distributed among the three groups – 1-6 years (32.3 per cent), between 7 and 15 years (34.4 per cent) and more than 15 years (33.3 per cent) (Table I).

Reliability and validity of constructs

As mentioned earlier, Cronbach's alpha was used to determine the reliability of the model constructs. It is reported by Eisinga *et al.* (2013, p. 637) that the most frequently reported reliability measure for item scales is Cronbach's coefficient alpha. Cronbach's alpha is the most widely used measure of internal consistency ("reliability"). It is appropriate to use Cronbach's alpha to determine if the scale is reliable when you have multiple items in the scale (e.g. Likert questions in a survey/questionnaire) [Hair *et al.* (2006), Goo *et al.* (2014), Statistics.laerd.com (2017)]. This applies to our case study.

The values for Cronbach's alpha were 0.80 or above except for one construct (privacy) which was 0.66 as shown in Table II. Although the common acceptable lower value for Cronbach's alpha is 0.7, according to Hair *et al.* (2006, p. 137), Cronbach's alpha of 0.60 is considered as acceptable for exploratory studies. One item (PJS3) was dropped to improve the reliability for procedural justice. The validity of the constructs was assessed by performing factor analysis on all items that measure the model constructs. Principal component analysis with varimax was used. Only items with loadings of at least 0.50 were retained (Hair, *et al.*, 2006). All items had a loading of more than 0.74 except for one item (PRV1) which was 0.664. Moreover, there was no cross-loading issue [all cross-loadings were less than 0.40 which is less than 0.5; the minimum difference between the cross loadings

Factor	No. of responses	(%)
Gender		
Male	87	44.6
Female	108	55.4
Age		
Less than or 40 years	38	19.5
Between 41 and 50	60	30.8
Greater than 50	97	49.7
Educational level		
High school	20	10.2
Undergraduate degree	52	26.7
Master degree	48	24.6
Doctorate degree	75	38.5
Job Type		
Administrative assistant	41	21.0
Director	52	26.7
Faculty	60	30.8
Other	42	21.5
Percentage of computer usage		
Less than 65%	58	29.7
Between 65-84%	59	30.3
More than 84	78	40.0
Experience		
1-6 years	63	32.3
Between 7 and 15	67	34.4
More than 15	65	33.3

Table I. Frequency distributions of key variables

item (PRV1) was larger than 0.2 (0.664-0.347) as shown in Table II]. The list of items and their descriptive statistics are reported in the appendix.

Results and discussion

Before testing the hypotheses, the assumptions of the multiple regression model were examined. For example, multicollinearity was not a problem, as the variance inflation factor (VIF) was low (< 2.31). Autocorrelation was also not an issue since the Durbin–Watson (DW) value was 2.07. Finally, the plotted histograms of the data depicted a normal distribution. The regression model was significant ($p = 0.000$) with $R^2 = 0.24$ as reported in Figure 2.

To test each hypothesis, we compared the significance (p value) of the t-values obtained from the regression analysis for each variable with the significance level ($\alpha = 0.05$) identified by the researchers. If the p value is less than or equal to the significance level, then we concluded that the variable is significant in predicting the dependent variable (Evans, 2016). According to the results of the regression model as shown in Table III, all hypotheses were significant at 0.05 or less with the exception of *H7* (the path between interactional justice and violations of information security measures).

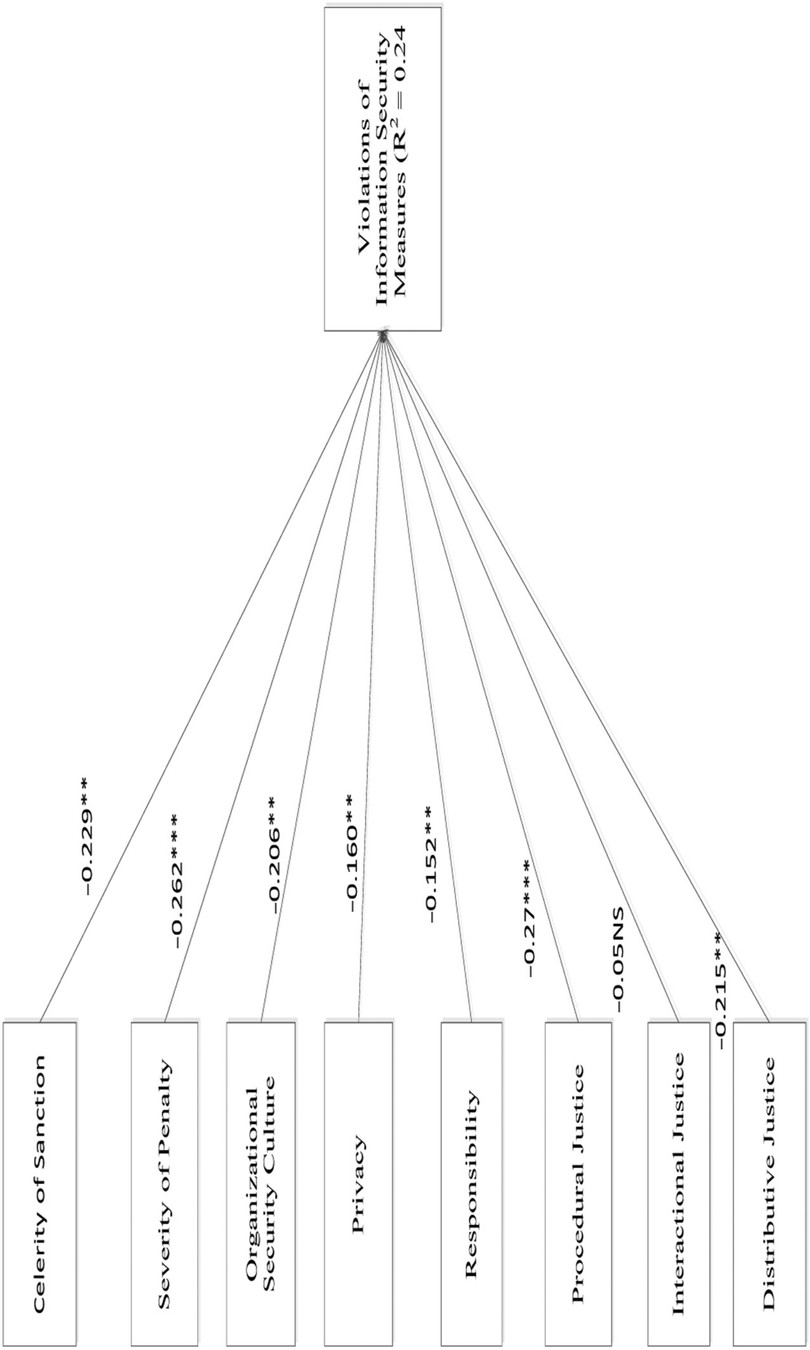
It should be noted that among the significant factors, procedural justice had the most significant impact on ISP violations with a standardized coefficient equal to -0.270, followed by severity of penalty and celerity of sanction with standardized coefficients

Table II.
Reliability and validity assessment

Item	Interactional justice	Severity	Responsibility	Distributive justice	Celerity	Privacy	Procedural justice	Org. security culture
IJS2	0.955	0.000	0.130	0.179	0.073	0.057	0.091	0.072
IJS3	0.948	0.022	0.156	0.175	0.075	0.038	0.088	0.082
IJS1	0.921	−0.036	0.211	0.186	0.054	0.059	0.091	0.036
SEV3	−0.026	0.895	−0.015	0.142	0.281	0.014	−0.056	0.162
SEV2	0.005	0.889	0.023	0.159	0.289	0.040	−0.078	0.162
SEV1	−0.011	0.742	0.110	0.215	0.353	−0.098	−0.120	0.082
RES3	0.183	0.054	0.911	0.037	0.031	0.097	0.060	0.054
RES2	0.199	0.013	0.798	0.058	0.107	0.176	−0.008	0.203
RES1	0.097	0.025	0.793	0.078	0.090	0.209	0.092	0.150
DJS2	0.179	0.197	0.055	0.850	0.181	0.021	0.140	0.102
DJS3	0.180	0.218	0.066	0.839	0.112	0.021	0.134	0.155
DJS1	0.240	0.080	0.072	0.804	0.226	0.122	0.164	0.100
CEL3	0.084	0.276	0.113	0.259	0.807	0.042	0.097	0.242
CEL1	0.091	0.366	0.076	0.164	0.807	0.050	0.038	0.161
CEL2	0.081	0.327	0.079	0.163	0.792	−0.008	0.030	0.138
PRV3	0.047	0.172	0.116	−0.014	−0.073	0.816	0.104	0.239
PRV2	0.050	−0.238	0.144	0.117	0.136	0.742	−0.109	0.017
PRV1	0.065	0.044	0.347	0.046	−0.005	0.664	0.031	−0.181
PJS2	0.091	−0.068	0.072	0.164	0.014	−0.004	0.912	0.038
PJS1	0.136	−0.112	0.056	0.175	0.087	0.016	0.875	0.130
OSC2	0.052	0.262	0.227	0.205	0.264	0.075	0.094	0.803
OSC1	0.178	0.203	0.237	0.199	0.286	0.073	0.148	0.766
Cronbach's Alpha	0.98	0.93	0.86	0.90	0.93	0.66	0.85	0.89

of −0.262 and −0.229, respectively. Distributive justice had a standardized coefficient of −0.215. Organizational security culture had a standardized coefficient of −0.206. Thus, managers in this environment, need to make sure that their employees not only have been able to express their views and feeling about the security measures, but also they were involved in their development and implementation. Additionally, these security measures should have been applied consistently through the organization without any bias. Moreover, managers need to emphasize the severity and celerity of penalty for any violation of information security measures by establishing restrictive rules and exercising the disciplinary actions in a timely manner. There are employees who will respect the rules and follow them when those rules are followed and applied by managers first. This would be consistent with a supportive organizational security culture. Additionally, a clear sanction scheme will make the employees aware of the consequences of their actions which could influence their behavior. Our results indicate that it is also very important for management to make it clear to all employees that the sanctions for violations of information security measures will be applied equitably and with justice regardless of the status of the violator. This will make employees expect the same treatment and will strengthen their confidence in the system. These suggested steps will have a stronger effect on employees' behavior if they are supported by or nurtured with a company culture that fosters information security minded thinking and considers information security to be a key norm.

The other two significant factors were employees' perception of privacy and responsibility with standardized coefficients of −0.160 and −0.152, respectively. These two factors are intrinsic ones and therefore, managers have limited influence on them. However, through education and training programs, managers could influence employees' perceptions regarding privacy and responsibility issues. Additionally, creating a culture that helps build a sense of community will help in creating a positive atmosphere regarding sharing responsibility in protecting a company's assets. Protiviti (2012) a risk and business



Notes: $^{**}p < 0.05$, $^{***}p < 0.01$; NS: not significant

Figure 2.
Model results
(standardized
regression
coefficients)

consulting firm, reported that according to senior information security and risk professionals, 71 per cent of the sample believed that employees are not aware of their important role in reducing security risks.

Limitations

As with any exploratory case study, this research has limitations such as the self-reported information and the method of measuring the violation of information security measures. With respect to the first limitation, which raises the possibility of common method variance concern, the Harman's single-factor test was used to investigate if the common method variance is of concern for this research. It was determined that only 29.05 per cent of variance was accounted for by one factor, which is less than the threshold value of 50 per cent (Chandra *et al.*, 2011). This result suggests that common method variance is not of great concern and thus, is unlikely to confound the interpretation of the results for this research. With respect to the method of measuring information security violations, it has been a challenge for researchers. Of course, the best method is to capture the actual behavior. Another limitation to our case study which might have affected the results is the significant number of faculty members in the respondent pool. The shared governance culture among faculty on a US university campus might bias the results more than in a company environment. In US higher education shared governance environments, faculty members are usually involved with the development of policies which directly impact them and their working conditions. Certainly policies on data security do impact faculty directly so they would expect to have involvement in the development of such policies. This participation in policy development might not be true in corporate environments or in higher education environments outside the USA. Therefore, caution should be applied when generalizing the results. Interestingly, a similar limitation was listed in a study in which fear appeals were used to determine compliance of ISP by government officials in Finland (Johnston *et al.*, 2015).

Future directions

This case study has selected certain variables that influence violation of information security measures. This effort is not by any means exhaustive. Consideration for future research is to include other factors that might influence employees' behavior such as violation types, job responsibility, employees' affective commitment, rewards, fear, organization types, culture, job types and work environment. Adding to the literature regarding the factor of top management involvement in the ISP is another possible direction for future research. Another study could consider another way of measuring violations of information security measures, as direct

Table III.
Regression results

Variable	Standardized coefficient (beta)	*T* value	Significance (*p*-value)	Hypothesis result
Celerity of Sanction	−0.229	−2.357	0.019	*H1* is supported
Severity of Penalty	−0.262	−3.649	0.000	*H2* is supported
Organizational security culture	−0.206	−2.312	0.022	*H3* is supported
Privacy	−0.160	−2.216	0.028	*H4* is supported
Responsibility	−0.152	−2.134	0.034	*H5* is supported
Procedural justice	−0.270	−3.698	0.000	*H6* is supported
Interactional justice	−0.05	−0.066	0.947	*H7* is not supported
Distributive justice	−0.215	−2.421	0.016	*H8* is supported

questions might have made the respondents reluctant to complete the survey; for example, using actual human actions or scenarios. Future research may examine the moderating role of justice theory dimensions on hypothesized relationships. Another plausible study could be to replicate the study across universities from different countries to test if the results of this case study hold across different universities outside the USA.

Conclusion

This case study examined factors that impact violations of information security measures by utilizing deterrence theory and organizational justice theory in US higher education. The results indicated that procedural justice, distributive justice, severity and celerity of sanction, organizational security culture, privacy and responsibility toward information security were significant factors in predicting the violations of information security measures in US higher education. Only interactional justice was not significant.

Security breaches that are both accidental and deliberate continue to occur in industry. These findings validate past research, at least as they relate to US higher education, and should encourage managers to ensure employees are involved with developing and implementing information security measures if it fits within the organizational culture. Additionally, the information security measures should be applied consistently and in a timely manner. Past research has focused more on the certainty and severity of sanctions and not as much on the celerity or swiftness of applying sanctions. The results of this research indicate that there is a need to be timely (swift) in applying sanctions especially in the US higher education environment. The importance of information security should be grounded in organization culture. Employees should have a strong sense of treating company data as they would want their own data to be treated.

Even though this research is built on well-grounded theories, there will be a need for investigating and conceptualizing salient factors that might add to our understanding of the issues at hand. In this regard, and as cited by Venkatesh *et al.* (2012), Johns (2006) and Alvesson and Karreman (2007) contend that there will be many valuable contributions from using existing theories in different contexts such as enhancing the understanding of studied phenomenon which could lead to extension of the original theories, through lack of supporting the original hypotheses or creating new relationships in the proposed models. This case study applies some of those theories in the context of the US higher education environment. The results of this case study also contributed to the extension of existing theories by including new factors, on one hand, and confirming previous findings, on the other hand.

References

Adams, J. (1965), "Inequity in social exchange," *Advances in Experimental Social Psychology*, Berkowitz, L. (Ed.), Academic Press, New York, NY, Vol. 2, pp. 267-299.

Alvesson, M. and Karreman, D. (2007), "Constructing mystery: empirical matters in theory development", *Academy of Management Review*, Vol. 32 No. 4, pp. 1265-1281.

Asai, T. and Hakizabera, A.U. (2010), "Empirical analysis of human-related problems of information security in cross-cultural environments (East African community)", *Information Management & Computer Security*, Vol. 18 No. 5.

Asai, T. and Hakizabera, A.U. (2011), "Human-related problems in information security in Thai cross-BIU cultural environments", *Contemporary Management Research*, Vol. 7 No. 2, pp. 117-142.

Baldwin, T., Bommer, W.H. and Rubin, R. (2008), *Developing Management Skills: What Great Managers Know and Do*, McGraw-Hill/Irwin, Boston, MA.

Bentham, J. (1843), "Principles of Penal Law", in Browning, J. (Ed.), *The Works of Jeremy Bentham*, London, 1838-1843; Reprinted New York, 1962.

Bies, R.J. and Moag, J.F. (1986), "Interactional justice: communication criteria of fairness", in Lewicki, R.J., Sheppard, B.H. and Bazerman, M.H. (Eds), *Research on Negotiations in Organizations*, JAI Press, Greenwich, CT, Vol. 1, pp. 43-55.

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.

Chandra, S., Theng, Y., O'Lwin, M. and Foo, S. (2011), "Examining trust for organizational collaborations via the virtual world", *Journal of Computer Mediated Communication*, pp. 1-20.

Chang, S.E. and Lin, C.S. (2007), "Exploring organizational culture for information security management", *Industrial Management & Data Systems*, Vol. 107 No. 3, pp. 438-458.

Cisco System, Inc (2008), *Data Leakage Worldwide: The Effectiveness of Security Policies*, Cisco Public Information, available at: www.cisco.com (accessed 2 October 2013).

Colquitt, J.A. (2001), "On the dimensionality of organizational justice: a construct validation of a measure", *Journal of Applied Psychology*, Vol. 86 No. 3, pp. 386-400.

Crosby, J. (2013) "Errant e-mail creates security breach at MNsure", available at: www.startribune.com/business/223564521.html?page=all&prepage=1&c=y#continue (accessed 9 March 2015).

Culnan, M.J. and Williams, C.C. (2009), "How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches", *MIS Quarterly*, Vol. 33 No. 4, pp. 673-687.

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.

Dinev, T., Hu, Q., Xu, Z. and Ling, H. (2011), "Does deterrence work in reducing information security policy abuse by employees", *Association for Computer Machinery (ACM)*, Vol. 54 No. 6.

Dols, T. and Silvius, G. (2010), "Exploring the influence of national cultures on non-compliance behavior", *Communications of the IIMA (CIIMA)*, Vol. 10 No. 3, pp. 11-32.

Eigen, Z.J. and Litwin, A.S. (2014), "Justice or just between us?", *Industrial and Labor Relations Review*, Vol. 67 No. 1, pp. 171-201.

Eisinga, R., Grotenhuis, M. and Pelzer, B. (2013), "The reliability of a two-item scale: Pearson, Cronbach or spearman-brown?", *International Journal of Public Health*, Vol. 58 No. 4, pp. 637-642.

Evans, J. (2016), *Business Analytics: Methods, Models, Decisions*, 2nd ed., Pearson International.

Folger, R. (1977), "Distributive and procedural justice: combined impact of "voice" and improvement on experienced inequity", *Journal of Personality and Social Psychology*, Vol. 35 No. 2, pp. 108-119.

Friesen, L. (2012), "Certainty of punishment versus severity of punishment: an experimental investigation", *Southern Economic Journal*, Vol. 79 No. 2, pp. 399-421.

Goo, J., Yim, M. and Kim, D. (2014), "A path to successful management of employee security compliance: an empirical study of information security climate", *IEEE Transactions on Professional Communication*, Vol. 57 No. 4, pp. 286-308.

Government Security News (2014), "Most government data breaches caused by employees, says Verizon study", available at: www.gsnmagazine.com/article/41007/most_government_data_breaches_caused_employees_say (accessed 9 March 2015).

Greenberg, J. (1987), "A taxonomy of organizational justice theories", *The Academy of Management Review*, Vol. 12 No. 1, pp. 9-22.

Hair, J., Black, B., Babin, B., Anderson, R. and Tatham, R. (2006), *Multivariate Data Analysis*, Prentice Hall, Upper Saddle River, NJ.

Harcourt, M., Hannay, M. and Lam, H. (2013), "Distributive justice, employment-at-will and just-cause dismissal", *Journal of Business Ethics*, Vol. 115 No. 2, pp. 311-325.

Hu, Q., Xu, Z., Dinev, T. and Ling, H. (2011), "Does deterrence work in reducing information security policy abuse by employees?", *Communications of the ACM*, Vol. 54 No. 6, pp. 54-60.

Ifinedo, P. (2016), "Critical times for organizations: what should be done to curb workers' noncompliance with IS security policy guidelines?", *Information Systems Management*, Vol. 33 No. 1, pp. 30-41.

Johns, G. (2006), "The essential impact of context on organizational behavior", *Academy of Management Review*, Vol. 31 No. 2, pp. 386-408.

Johnston, A., Warkentin, M. and Siponen, M. (2015), "An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric", *MIS Quarterly*, Vol. 39 No. 1, pp. 113-134.

Leventhal, G., Karuza, J. and Fry, W. (1980), Beyond fairness: a theory of allocation preferences, in Mikula, G., (Ed.), *Justice and Social Interaction*, Springer-Verlag, New York, NY, pp. 167-218.

Li, H., Sarathy, R., Zhang, J. and Luo, X. (2014), "Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance", *Information Systems Journal*, Vol. 24 No. 6, pp. 479-502.

Lind, E., Allan, E. and Tyler, T. (1988), *The Social Psychology of Procedural Justice*, Plenum, New York, NY.

Posey, C., Bennett, R., Roberts, T. and Lowry, P. (2011), "When computer monitoring backfires: invasion of privacy and organizational injustice as precursors to computer abuse", *Journal of Information System Security*, Vol. 7 No. 1, pp. 24-47.

Protiviti (2012), "Warning over ineffectiveness of information security awareness training within UK business", available at: www.protiviti.com (accessed 2 October 2013).

Raubenheimer, J. (2004), "An item selection procedure to maximize scale reliability and validity", *Journal of Industrial Psychology*, Vol. 30 No. 4, pp. 59-64.

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

Schoepfer, A., Carmichael, S. and Piquero, N.L. (2007), "Do perceptions of punishment vary between white-collar and street crimes?", *Journal of Criminal Justice*, Vol. 35 No. 2, pp. 151-163.

Sheppard, B.H., Lewicki, R.J. and Minton, J.W. (1992), *Organizational Justice*, Lexington Books, New York, NY.

Siponen, M. and Vance, A. (2010), "Neutralization: new insight into the problem of employee IS security policy violations", *MIS Quarterly*, Vol. 34 No. 3, pp. 487-502.

Siponen, M., Pahnila, S. and Vance, A. (2012), "Motivating IS security policy compliance: insights from habits and protection motivation theory", *Journal of Information and Management*, Vol. 49 Nos 3/4, pp. 190-198.

Soomro, Z., Shah, M. and Ahmed, J. (2016), "Information security management needs more holistic approach: a literature review", *International Journal of Information Management*, Vol. 36 No. 2, pp. 215-225.

Statistics.laerd.com (2017) Cronbach's Alpha (α) using SPSS Statistics, available at: https://statistics.laerd.com/spss-tutorials/cronbachs-alpha-using-spss-statistics.php (accessed 15 February 2017).

Straub, D.W. (1990), "Effective IS security: an empirical study", *Information Systems Research*, Vol. 1 No. 3, pp. 255-276.

Thibaut, J.L. and Walker, L. (1975), *Procedural Justice: A Psychological Analysis*, Lawrence Erlbaum Associates, Hillsdale, NJ.

Tyler, T.R. and Blader, S.L. (2000), *Cooperation in Groups: Procedural Justice, Social Identity, and Behavioral Engagement*, Psychology Press, Philadelphia, PA.

Vance, A. and Siponen, M. (2012), “IS security policy violations: a rational choice perspective”, *Journal of Organizational and End User Computing*, Vol. 24 No. 1, pp. 21-41.

Venkatesh, V., Thong, J. and Xu, X. (2012), “Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology”, *MIS Quarterly*, Vol. 36 No. 1, pp. 157-178.

Willison, R. and Warkentin, M. (2013), “Beyond deterrence: an expanded view of employee computer abuse”, *MIS Quarterly*, Vol. 37 No. 1, pp. 1-20.

Workman, M., Bommer, W.H. and Straub, D. (2009), “The amplification effects of procedural justice on a threat control model of information systems security behaviours”, *Behaviour & IT*, Vol. 28 No. 6, pp. 563-575.

Yalya, A. (2011), “Enforcing information security policies through cultural boundaries: a multinational company approach” AIS electronic library”, *ECIS Conference Proceedings*, Vol. 2011, pp. 23-24.

Yazdanmehr, A. and Wang, J. (2016), “Employees’ information security policy compliance: a norm activation perspective”, *Decision Support Systems*, Vol. 92, pp. 36-46.

Further reading

Sykes, G. and Matza, D. (1957), “Techniques of neutralization: a theory of delinquency”, *American Sociological Review*, Vol. 22 No. 6, pp. 664-670.

Appendix

Construct	Item	Description	Mean	SD
Celerity of sanction $\alpha = 0.93$	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
Severity of penalty $\alpha = 0.93$	SEV1	Employees caught committing an information security violation on the computer system will be punished by my organization	4.77	1.447
	SEV2	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
	SEV3	Organizational sanctions for employee violations of information security on the computer system would be severe	4.41	1.459
Organizational security culture $\alpha = 0.89$	OSC1	The overall organization environment fosters information security minded thinking	4.82	1.361
	OSC2	Information security is a key norm shared by the members in our organization	4.75	1.381
Privacy $\alpha = 0.66$	PRV1	I am concerned about protecting the information privacy of others	6.40	0.776
	PRV2	I am cautious about revealing my own personal information	6.35	0.893
	PRV3	I consider information privacy as one of my major concerns	5.58	1.307
Responsibility $\alpha = 0.86$	RES1	I believe I share responsibility for preventing violations of information security within my organization	6.26	0.810
	RES2	I believe that I should respect the rules set forth by my organization regarding information security	6.45	0.697
	RES3	I believe that preventing violations of information security within my organization is a shared responsibility	6.49	0.629
Procedural justice $\alpha = 0.85$	PJS1	Have you been able to express your views and feelings about those security measures?	3.60	1.795
	PJS2	Have you had influence over the development or implementation of those security measures?	2.77	1.796
	PJS3*	Have those security measures been applied consistently throughout your organization?	4.71	1.471
Interactional justice $\alpha = 0.93$	IJS1	Has (he/she) treated you in a polite manner?	5.71	1.331
	IJS2	Has (he/she) treated you with dignity?	5.72	1.334
	IJS3	Has (he/she) treated you with respect?	5.71	1.355
Distributive justice $\alpha = 0.90$	DJS1	Is your organization fair in how it disciplines those who violate the computer system security policies?	4.97	1.276

(*continued*)

Table A1. List of items and reliability test results

Construct	Item	Description	Mean	SD
	DJS2	Would the discipline applied to employees found misusing the computer system be equal?	4.71	1.415
	DJS3	Can your co-workers expect to receive the same punishment that you would receive for inappropriate behavior while using the computer system?	4.94	1.370
Violations of information security measure $\alpha = 0.93$	VIO1	One or more of my co-workers have deliberately bent or broken an information security measure	2.08	1.245
	VIO2	One or more of my co-workers have intentionally violated an information security measure	1.99	1.264
	VIO3	One or more of my co-workers have inadvertently bent or broken an information security measure	2.35	1.252
	VIO4	One or more of my co-workers have inadvertently violated an information security measure	2.30	1.295
	VIO5	I have deliberately bent or broken an information security measure	1.51	0.887
	VIO6	I have intentionally violated an information security measure	1.39	0.782
	VIO7	I have inadvertently bent or broken an information security measure	1.67	0.883
	VIO8	I have inadvertently violated an information security measure	1.70	0.986

Table A1.

Note: *Item was deleted to improve reliability value

Corresponding author
Peggy L. Lane can be contacted at: plane@ulm.edu