Journal of Applied Structural Equation Modeling

eISSN: 2590-4221 *Journal of Applied Structural Equation Modeling: 2(1),13-28, January 2018*

SECURITY POLICY COMPLIANCE IN PUBLIC INSTITUTIONS: AN INTEGRATIVE APPROACH

Daniel Koloseni[a*], Chong Yee Lee[b] and Gan Ming Lee[c]

[a,b]Faculty of Business and Finance, Universiti Tunku Abdul Rahman, Malaysia
[c]Faculty of Information and Communication Technology, Universiti Tunku Abdul Rahman, Malaysia

**koloseni@utar.edu.my*

ABSTRACT

The success of organizational information security policies depends on employee's continuous compliance from the time when it was first introduced into the organization. Hence, the purpose of this study is to investigate continuous compliance with information security policy among public organizations. Data were collected from 265 employees working in Tanzania public organizations. Data analysis employed a Structural Equation Modelling (SEM) approach. The study found that the effects of organizational commitment, perceived susceptibility and perceived severity have a positive influence on employee's continuance intention to comply with security policies, while perceived barriers have a negative influence. Moreover, the effects of perceived benefits, self-efficacy, cues and information security awareness have no significant influence. Based on these findings, recommendations were given. There is a paucity of empirical research which investigates key issues that may influence information security policy continuous compliance in organizations. This study addresses this research gap, by integrating the Health Belief Model (HBM) with employee's organizational commitment and information security awareness constructs to investigate information security policy continuance compliance in organizations.

Keywords: *Security policy, continuance intention, compliance, commitment, security awareness*

INTRODUCTION

There is a general consensus among organizations that information is crucial for its operations and therefore it should be protected (Hardy & Williams, 2010; Hong, Yen-Ping, Chao, & Tang, 2003; Posey, Roberts, Lowry, & Bennett, 2013). Protection of information requires investment in both technical and non-technical issues (Hentea, Dhillon, & Dhillon, 2006). However, non-technical issues have yet to receive a deserved attention. Recent trends in information security budgets indicate much of the funds are located on technical aspects of information security (Dignan, 2016). While the focus of many organizations is on technical aspects of information security, a large portion of security incidents is of non-technical nature (Lewis, 2003; PWC, 2015; Wood & Banks, 1993). Moreover, previous researchers indicate that majority of security incidents are caused by the intentional or unintentional negligence of employees (Herath & Rao, 2009a). To control employee's negligence and reduce security incidents, security controls are widely adopted. A good example of security control is information security policy. Unfortunately, the adoption of security policies have yet to provide a shield against security incidents. In fact, Dhillon and Moores (2001) argue that violation of security controls such security policies contributes immensely to security incidents happening in organizations. Further, often users of information systems violate security policies (Herath & Rao, 2009b).

To address violation of information security policies, the extant literature in information security favours the use of sanctions and rewards with assumption that users of information system intentionally chose to violate the policies (Bulgurcu, Cavusoglu, & Benbasat, 2010; D'Arcy, Hovav, & Galletta, 2009; Pahnila, Siponen, & Mahmood, 2007) and ignored the role played by other factors such as employee's organization commitment. Paine (1994) argue that over-emphasis on sanctions may be superfluous and counterproductive; causing employees to rebel against the control measures.

Organization commitment ties an employee with organization goals and therefore cultivates employee's sense of responsibility (Eisenberger, Huntington, Hutchison, & Sowa, 1986). Employee's increased sense of responsibility, in turn, increases employee's devotion towards compliance with organization policies (Hu, Dinev, Hart, & Cooke, 2012). Further, information security awareness is equally important. Adoption of security policies and continuity of its use depends widely on security awareness of users. If the users are not aware of the policies it will be difficult to adhere to them, thus information security plays a key role to motivate users to comply with security policies (Bulgurcu et al., 2010). Thus, this study integrates the HBM with employee's organizational commitment and information security awareness constructs to investigate security policy continuance compliance among the employees.

Past studies focused on acceptance or intention to comply or compliance with security policies in organizations (Bulgurcu, Cavusoglu, & Benbasat, 2010; D'Arcy, Hovav, & Galletta, 2009; Hu et al., 2012; Ifinedo, 2012, 2014; Pahnila, Siponen, & Mahmood, 2007). However, initial intention or acceptance of information systems does not necessarily imply that users will continue to use the information system (Bhattacherjee, 2001; Zhao, Stylianou, & Zheng, 2013), the same applies to security policy. Users of information systems may stop to comply with security policies after initial acceptance when any of these circumstances occur, 1) diminished signs of security threats, lack of susceptibility and severity to security threats (Warkentin, Johnston, Shropshire, & Barnett, 2016) and lack of belief on efficacy of the security control measures and cues such as persuasive messages (Siponen, Mahmood, & Pahnila, 2009). Thus, it is imperative to understand information security policies continued usage phenomenal for its successful usage and information security management in the organizations.

This study contributes to the literature on information security compliance in the following ways. First, a meta-analysis of literature in information security policy compliance indicates that that only Warkentin, Johnston, Shropshire, & Barnett (2016) have investigated post-compliance to information security policies in organizations. Thus, this study further enriches our understanding of continuance behaviour in the context of information security policy compliance in organizations. Second, this study extends the HBM by including the constructs of employee's organizational commitment and security awareness to measure its influence on information security policy continued compliance. To the best knowledge of the researchers, no study has extended the HBM this way.

Theoretical Background and Hypotheses Development

Organization commitment is defined as employee's total assurance and determination with regard to matters related to the organization (Herath & Rao, 2009a; Mowday, 1999). Organization commitment has a strong influence on employee's behaviours in various ways. For example, organization commitment has been found to influence innovative behaviour (Jafri, 2010), leadership behaviour (Çokluk & Yılmaz, 2010) and loyalty behaviour (Amine, 1998). In fact, previous studies (Herath & Rao, 2009a) confirm that organizational commitment is related to employee's intention comply to practice various information security behaviours. The higher level of employee's commitment to organization provides a guarantee for the higher level of employee work performance (Herath & Rao, 2009a) including employee continued participation in information security-related activities or behaviours. Therefore, it is reasonable to hypothesize that,

H1: Employee's organizational commitment is positively related to continuance intention of employees to comply with information security policies.

HBM was originally developed in 1950's as in an attempt to understand why US citizens were not interested to participate in free Tuberculosis (TB) screening (Hochbaum, 1958). The model consists of six constructs: perceived severity, perceived susceptibility, perceived barriers, perceived benefits, cues to action and self-efficacy which play a key role to motivate an individual to participate into a particular behaviour (Ng, Kankanhalli, & Xu, 2009; Rosenstock, 1974). Several empirical studies have confirmed the relationship between the above constructs and intention to engage in life-changing behaviours both in information system research and health-related behaviours context. The next paragraphs use previous studies findings to establish the hypotheses related to HBM constructs.

IS researchers argue that the users' tendency to practice information security behaviour will increase if they feel that their actions would enhance their work productivity (Bowen, Chew, & Hash, 2007; Li, Zhang, & Sarathy, 2010; Rahman & Donahue, 2010). Additionally, healthcare researchers also suggest that an individual will engage in health behaviour if the derived benefits are positively perceived (Lee, 2013; Reiser, 2007). This suggests that an employee is likely to comply with organization information security policies if the benefits of doing so exist. Thus, despite the presence of barriers an employee can still continue to comply with ICT security policies if the benefits outweigh the barriers. Information systems (IS) studies indicate that perceived barrier can affect user's intention to practice information security behaviours (Claar, 2011; Claar & Johnson, 2012; Ng et al., 2009). Barriers such as additional or unnecessary security controls in computer systems and time constraints may impede user's intention to practice security behaviour (Claar, 2011). In such circumstances, users are likely to continue to violate security policies as long as such barriers continue to exist. The further relationship between perceived benefits, perceived barriers on continuance intention is seen in the work of McKnight, Lankton and Tripp (2011). Hence, it is reasonable to postulate that:

H2: Perceived benefit is positively related to continuance intention of employees to comply with information security policies.

H3: High perceived barriers would reduce employees' continuance intention of employees to comply with information security policies.

HM suggest that an individual's perception of security threats is shaped by levels of perceived susceptibility and perceived severity (Rosenstock, 1974). Perceived susceptibility refers to individual's perceived probability of falling victim of information security attack, while perceived severity constitutes of the consequences an individual may get if she or he did not engage into a recommended security behaviour (Liang & Xue, 2010). IS literature argues that individuals with high levels of susceptibility are more likely to engage in the practice of safe computing or behave more vigilantly while online (Ng et al., 2009; Siponen, Mahmood, & Pahnila, 2014). On the other hand, that if individual's perceived severity levels of a security incident are high, she or he would be more likely to engage in practising safe computing behaviour (Lee & Larsen, 2009; Ng et al., 2009; Woon et al., 2005). For an individual to continue to adhere to organization ICT security policies, the levels of perceived susceptibility and severity should continue to be high as well (Warkentin et al., 2016). Thus, this study anticipates that,

H4: Continued increase in perceived severity has a positive influence on employee's continuance intention to comply with information security policies.

H5: Continued increase in perceived susceptibility has a positive influence on employee's continuance intention to comply with information security policies.

Cue to action is an important tool that could stimulates an individual's readiness to engage in appropriate health behaviour (Janz & Becker, 1984; Strecher & Rosenstock, 1997). In information security context, cues to action refer to information security tips, advice, reminders, word of mouth that remind or motivate an individual to practice information security behaviours (Claar, 2011). Great cues to action may motivate an individual to engage in protective information security behaviour (Ng et al., 2009). Cues such as reminder message improve individual's adherence to life-changing behaviours (Vervloet et al., 2012). It therefore reasonable to postulate that, as long as cues with regard to the importance of complying with information security policies are provided, there is potential for users to continue to observe the policies after its initial adoption or acceptance. Hence, this study predicts that,

H6: Cues to action has a positive influence on employee's continuance intention to comply with information security policies.

Confidence in ability and determination to perform a particular behaviour (termed as self-efficacy) provides a motivation to execute that behaviour (Bandura, 1977). For example, an individual would perform certain health behaviour if that person has the skills and confidence to perform that behaviour (Armitage & Conner, 2001; Floyd, Milne et al., 2000; Peyman et al., 2009). Equally, users who have confidence in the ability to perform security behaviours, are more likely to practice the information security behaviour (Claar & Johnson, 2012; Ng et al., 2009; Workman, Bommer, & Straub, 2008). As the confidence in the capability to comply with information security policies increases, the likelihood of an individual to continue to comply also increases (Warkentin et al., 2016). The relationship between self-efficacy and behavioural continuance intention is also documented in (Yaojun & Yongliang, 2015). Based on the above findings, the study, hypothesize that:

H7: Self–efficacy has a positive influence on employee's continuance intention to comply with information security policies.

Awareness of information security and overall importance of information security in the organization are the key factors to motivate employees to continue to comply with organization's information security policies. For example (Stanton, Stam, Mastrangelo, & Jolton, 2005) found that high levels of awareness are related to the continued practice of information security related behaviours. Further, awareness is the driver of user's motivation to comply with security policies (Whitman, Townsend, & Aalberts, 2001) and can be promoted through security awareness programs (Dhillon, 1999). Awareness to information security is therefore expected to reduce non-compliance with security policies (Lee & Lee, 2002) because the secure-aware user knows the consequences of non-compliance with security policies, therefore he/she likely to continue to comply with security policies. Thus the hypothesis;

H8: Awareness of ICT policies is positively related to intention to continue to comply with information security policies.

The hypothetical relationships between the constructs of the study are indicated in figure 1.

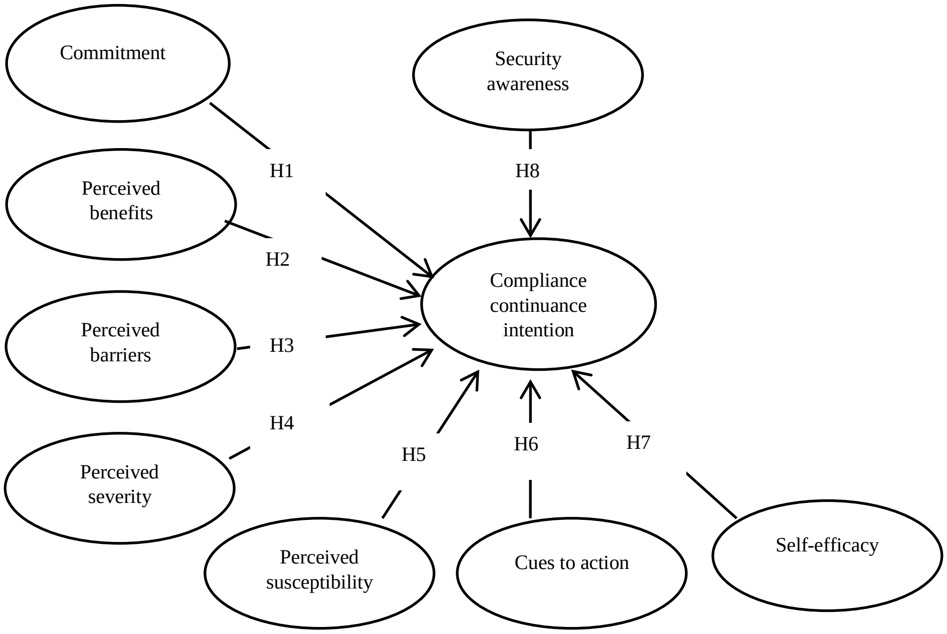


Figure 1: Research model

METHODS

Data Collection Instruments

Items used to measure the constructs of the study were adopted from previous studies. The adopted items were modified to suit the context of this study. Specifically, items for measuring organization commitment were adapted from Mowday (1999), perceived benefits, perceived barriers, and cues to action from Claar and Johnson (2011) and Ng et al.(2009), perceived susceptibility, perceived severity and self-efficacy from Claar and Johnson (2011), Herath and Rao (2009) and Ng et al.(2009), items for security awareness were borrowed from Mahabi (2010), while items for compliance continuance intentions were borrowed from Warkentin et al. (2016). Measurement items are reported in table 1.

Table 1: Measurement Items

Construct	Code	Measurement items
Commitment	CMT1:	I am willing to put in a great deal of effort beyond that normally expected in order to help this organization be successful.
	CMT2:	I really care about the fate of this organization.
	CMT3:	For me, this is the best of all possible organizations for which to work.
	CMT4:	I am proud to tell others that I am part of this organization.
Perceived Benefits	BEN1:	Information security policy is effective in protecting malicious software from infecting my computer.
	BEN2:	Information security policy is effective in minimizing the risk of data leak or loss from my computer.
	BEN3:	Information security policy controls misuse of organization's internet resources hence could increase my work productivity.
Perceived Barriers	BAR1:	Complying with information security policy would change the way I use my computer.
	BAR2:	Complying with information security policy effectively is time-consuming.
	BAR3:	Complying with information security policy it would require a considerable investment of effort other than time.

Perceived Severity	SEV1:	Losing data as a result of non- compliance with security policy would be a serious problem for me.
	SEV2:	My personal and organization's information could be collected by malicious software as result of non-compliance with information security policy.
	SEV3:	If my computer were infected by malicious software as result of non-compliance with information security policy, it would be significant.
	SEV4:	Malicious software could steal my personal and organization's information without my knowledge as result of non-compliance with information security policy.
	SEV5:	Malicious software could crash my computer from time to time as result of non-compliance with information security policy.
Perceived Susceptibility	SUS1:	My computer is at risk of becoming infected with malicious software if I fail to comply with information security policy.
	SUS2:	It is likely that my computer will become infected with malicious software if I fail to comply with information security policy.
	SUS3:	It is possible that my computer will become infected with malicious software if I fail to comply with information security policy.
	SUS4:	Data in my computer are likely to be damaged by malicious software if I fail to comply with information security policy.
	SUS5:	There is a chance that organization information will be disclosed by malicious software if I fail to comply with information security policy.
	SUS6:	It is possible that hackers could steal the organization data that is stored on my computer if I fail to comply with information security policy.
Cues to action	CUE1:	If a friend were to tell me about a recent experience with a computer virus, I would be more conscious of my computer's chance of being attacked.
	CUE2:	If I saw a news report, or read a newspaper or magazine about a new computer vulnerability, I would be more concerned about my computer's chances of being attacked.
	CUE3:	My organization constantly reminds me to practice computer security.
	CUE4:	My organization's IT helpdesk sends out alert messages/emails concerning security.
Self-efficacy	SE1:	My interaction with organization's information security policy was clear and understandable.
	SE2:	I found organization's information security policy easy to comply.
	SE3:	I can correctly comply with organization's information security policy.
	SE4:	I can find the information I need if I have problems to comply with organization's information security policy.
Awareness	SAW1:	I am aware of information security incidents and try to take action to prevent them.
	SAW2:	My department educates employees on their computer security responsibilities.
	SAW3:	I am aware of malicious software (such as computer virus, spyware).
	SAW4:	I am aware of social engineering practices (such as phishing).
Continuance Intention	IC1:	I plan to continue to comply with organization's information security policy in the future.
	IC2:	I plan to continue to comply with organization's information security policy to protect organization's information.

The five-point Likert scale was used to measure the items, whereby, 1 represented strongly disagree while 5 represented strongly agree. To ensure measurement items are free from ambiguity, the question was sent to an IS expert for content validation.

Sample and Data Collection Procedures

The number of organizations with active information security policies in place is not known, therefore it was difficult to establish a sampling frame. To establish a sampling frame, a list of organizations with information security policy was first developed. To achieve that, the researchers inquired information on the existence of information security policies from the ICT departments or sections in 61 public organizations. Out of 61 public organizations visited, only 46 had active information security policy in place. Only employees who use computers in their daily undertakings from organizations with information security policies and were selected to participate in the study. A sample size of 389 respondents was used. The sample size was estimated using Cochran formula (Cochran, 1977). The formula is applied to estimate the appropriate sample size in a situation where the size of the population of the study is unknown. Similarly, in this study the number of employees who use computers for their daily activities from the sampled public organizations which have information security policies is unknown, thus Cochran formula is appropriate in estimating the sample size of the study.

To ensure that each respondent has an equal chance of being selected respondents were selected using simple random sampling technique from the list of potential respondents sourced from public organizations with active information security policies (Kothari, 2011). Questionnaires were administered using face to face approach to participants from the 46 public organizations. After two months (2), we collected back 265 complete responses which were used for data analysis. Profile of respondents is reported in table 2.

Table 2: Profile of respondents

Variables	Frequency	Percentage (%) (Approx.)
Gender		
Female	107	40.37
Male	158	59.63
Education Level		
O'level	4	0.02
A'level	7	0.03
Diploma or Equivalent	115	0.43
Bachelor Degree or Equivalent	97	0.37
Master's Degree	41	0.15
PhD	1	0.004
Computer usage Frequency		
Less than 3 hours	53	0.20
3 to 5 hours	119	0.45
More than 5 hours	93	0.35
Working Experience		
Less than 1 Year	1	0.004
1-5 Years	156	0.59
More than 5 Years	108	0.41

Common Method variance

Since data were collected using a self-reported instrument, it is likely that data used in this study suffers from the common method (CMV). To minimize the chance of the occurrence of CMV, we reminded respondents that that confidentiality of data and anonymity of respondents will be observed. Further, we randomized measurement items to reduce the chance of guessing the relationships between the items. Next, we tested the existence of CMV using Harman's single factor method (Chang, Van Witteloostuijn, & Eden, 2010). Using this method, CMV exists only if the resulting model does not fit with research data (i.e. does not generate recommended model fit indices) (Podsakoff, Mackenzie, Lee, & Podsakoff, 2003).We found that the resulting model produced the following model fit indices: x2/df = 6.299, RMSEA = 0.139, CFI = 0.489 and IFI = 0.492, meaning that the resulting model did not fit the research data. Generally, this finding suggests that data used in this study is free from CMV.

Data Normality Assessment

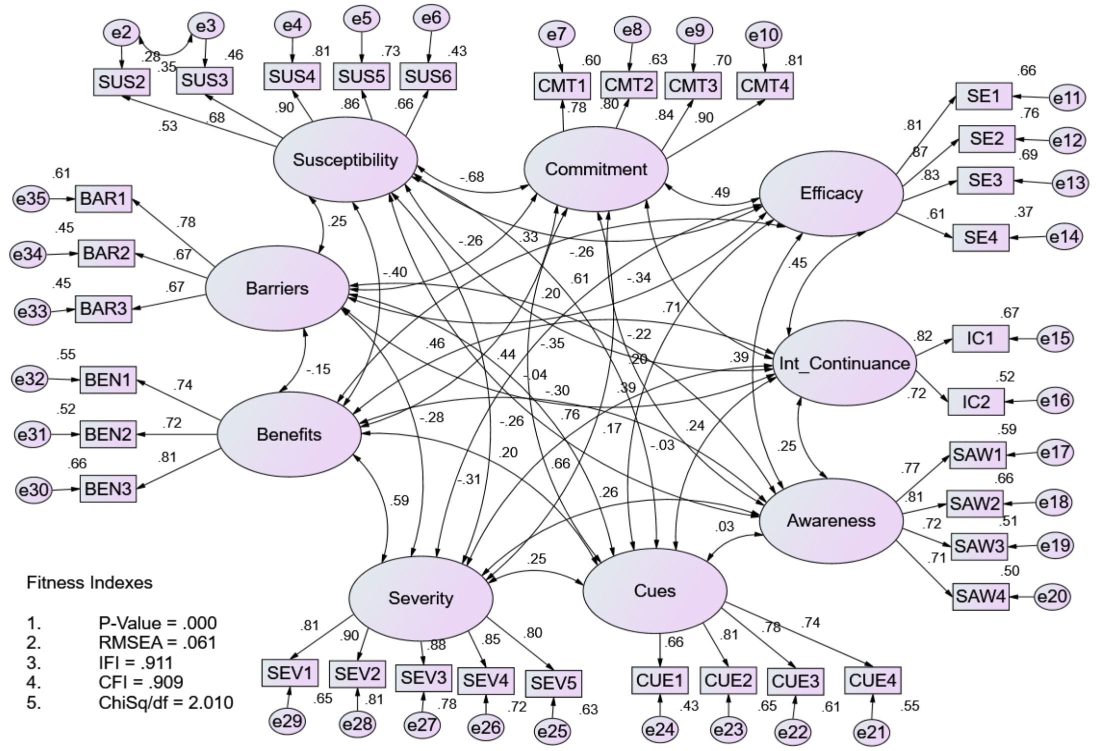
Multivariate normality assessment is a pre-requisite for studies which employ covariance – based (CB) SEM since CB- SEM assumes that data follow a multivariate normal distribution, such that the means and the covariance contain all the information (Hox & Bechger, 1998). Therefore, it is important to assess multivariate normality. To achieve that, Mahalanobis distance was computed to detect multivariate outliers. Mahalanobis distance shows the distance of each case from the centroid of all cases in the data set (Tabachnick & Fidell, 2007). A case is considered as an outlier if its distance from the centroid is too far as compared to the majority of cases. The p-value less than 0.001 is recommended by Kline (2015) and Hox and Bechger (1998) as a baseline for statistical significance of multivariate outliers. The study found that six (6) multivariate outliers (responses with p < 0.001) which is equivalent to 0.023 % (6/265), suggesting that a few multivariate outliers were present in the dataset. The presence of multivariate outliers could have a significant effect on the final results if the sample size is less than 50 (Hair, Black, Babin, Anderson, & Tatham, 2006). Therefore this study did not perform any data transformation or removed the multivariate outliers because a sample size used in this study (N = 265) is large enough to suppress the effect of multivariate outliers in the data set.

Structural Equation Modelling

Analysis of the data was conducted using structural equation modelling techniques (SEM) in which AMOS 21 was used as a data analysis tool. In order produce honest and reliable results, the measurement model should produce acceptable model indices and constructs of the study should be reliable and valid (Awang, 2015). Employing a two-stage SEM analysis approach suggested by (Anderson & Gerbing, 1988); we first assessed the quality of the measurement model to ensure reliability and factorial validity of the measurement model. Second, a structural model was assessed to test the underlying hypotheses of the study.

Quality of the Measurement Model

To assess model fit, this study employed Chi-square (x^2) and its associated degree of freedom (*df*), relative Chi-square (x^2/df), Root Mean Square Error of Approximation (RMSEA), Comparative Fit Index (CFI) and Incremental Fit Index (IFI) to represent each category of model fit indices as advocated by Hair, Black, Babin and Anderson (2010). The measurement model is deemed fit if x2/df < 3, RMSEA< 0.08, CFI and IFI > 0.9 (Hu & Bentler, 1999;Hair Jr et al., 2010). We conducted confirmatory factor analysis (CFA) to estimate model fit. Estimation of model fit is an iterative process in which items with low factor loading (i.e. less than 0.5) should be removed (Awang, 2015; Schwab, 1980). Following the above recommendation, item SUS 1 produced factor loading value below 0.5, therefore, was dropped. Further, measurement items SUS2 and SUS3 were constrained to improve model fit (Awang, 2015). The final adjusted model met the recommended model fit indices as follows: x^2/df = 2.010, RMSEA = 0.061, CFI = 0.909 and IFI = 0.911. With respect to chi-square results, the model produced statistically significant chi-square (x^2 = 984.7694, *df* = 490, *p* = 0.000), suggesting that the model has not achieved a good fit. Chi-square statistic is likely to increase with an increase in sample size and number of observed variables (Hair et al., 2010). Therefore it is expected that in a study with a large sample size and many observed variables, similar to this study to illustrate significant chi-square (Hair et al., 2010; Ho, 2006). Due to its sensitivity to sample size and number of observed variables it should be used cautiously as a measure of model fit (Kline, 2015). Hence, in a situation where a large sample size has been used, it assumed that the model has achieved good fit irrespective of chi-square results given that the recommended threshold levels for other indices have been achieved (Fry, Drennan, Previte, White, & Tjondronegoro, 2014; Kline, 2015). Generally, the assessment of the measurement model indicates that the measurements used in this study are of acceptable quality. Figure 2 shows the final adjusted measurement model used in subsequent analysis.



Fitness Indexes

1. P-Value = .000
2. RMSEA = .061
3. IFI = .911
4. CFI = .909
5. ChiSq/df = 2.010

Figure 2: The Final Measurement Model

Next, construct reliability was assessed. Construct reliability is defined as the extent to which measurement items consistently measure the construct (Perry, 1996). It is usually measured using Cronbach alpha or composite reliability. In this study, we used composite reliability(CR) as the measure of reliability due to its superiority in generating reliable measures as compared to Cronbach alpha in structural equation modelling (Bacon, Sauer, & Young, 1995). The study found that CR values were above 0.6 indicating the acceptable reliability of all measurement items of the constructs (Fornell & Larcker, 1981; Hair et al., 2010). Construct validity was assessed by analysing discriminant validity, defined as the degree to which the measurement items used to measure construct are different from each other (Bagozzi, Yi, & Phillips, 1991; Henseler, Ringle, & Sarstedt, 2015) and convergent validity, refers to as how well the measurement items measures the construct it was supposed to measure (Bagozzi et al., 1991). Discriminant validity was assessed by checking that the square root of AVE for each construct if is great than the correlation values in its row and column (Fornell & Larcker, 1981). Based on Fornell- Larcker criterion for assessing discriminant validity, all constructs demonstrated acceptable discriminant validity (see table 3). With regard to convergent validity, (Fornell & Larcker, 1981; Hair, Ringle, & Sarstedt, 2015) suggest that convergent validity is deemed achieved if the AVE values are above 0.5. In this study, the AVE values were in the range of 0.504 to 0.720 indicating that constructs have achieved convergent validity.

Table 3: Correlation matrix, Average Variance Extracted and Reliability Statistics of the Constructs

	CR	AVE	SE	SUS	BAR	BEN	CMT	SEV	SAW	IC	CUE
SE	0.865	0.619	**0.787**								
SUS	0.859	0.554	-0.266	**0.744**							
BAR	0.752	0.504	-0.336	0.268	**0.710**						
BEN	0.803	0.577	0.334	-0.407	-0.153	**0.760**					
CMT	0.898	0.687	0.488	-0.709	-0.256	0.441	**0.829**				
SEV	0.928	0.720	0.606	-0.323	-0.275	0.585	0.660	**0.848**			
SAW	0.840	0.568	0.394	-0.265	-0.217	0.169	0.389	0.259	**0.753**		

IC	0.745	0.595	0.450	-0.366	-0.296	0.462	0.710	0.759	0.252	**0.771**	
CUE	0.836	0.562	0.205	-0.041	-0.043	0.200	0.197	0.253	0.030	0.243	**0.749**

CR: Composite Reliability, AVE: Average Value Extracted, SE: Self-Efficacy, BAR: Barriers, BEN: Benefits, SUS: Susceptibility, CMT: Commitment, SEV: Severity, IC: Intention Continuance, CUE: Cues to action

Structural Model Analysis

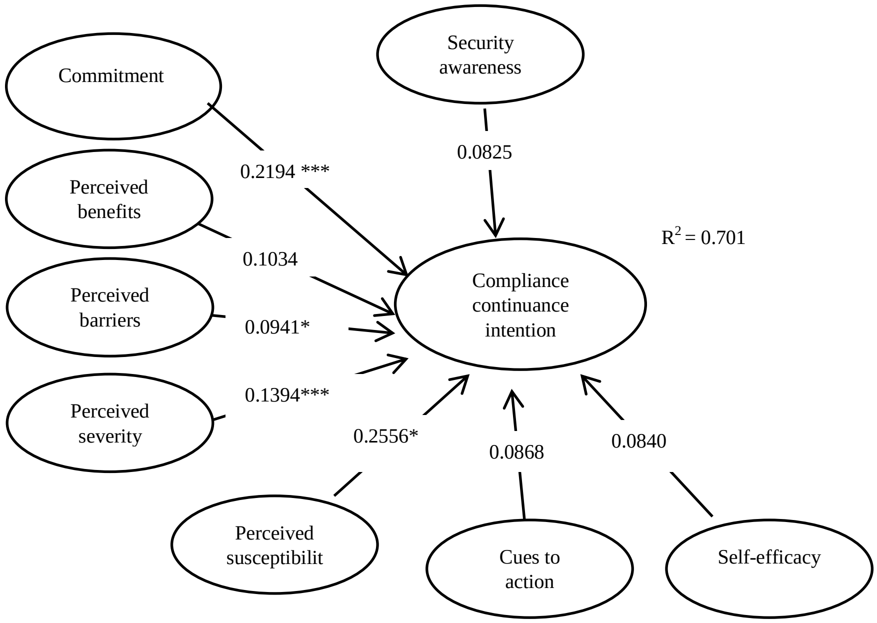
The results of the structural model analysis are indicated in table 4 and figure 3. Based on recommended model fit indices suggested by Hu and Bentler (1999) and Hair et al. (2010), the structural model achieved the acceptable threshold values as follows: x^2/df = 1.868, RMSEA = 0.056, CFI = 0.922 and IFI = 0.923. Further, analysis of paths analysis between the constructs indicated that four (4) hypotheses out of eight (8) were supported. The paths between employee's organizational commitment and continuance to comply with security policies H1 (β = 0.2194, p = 0.001), the paths between employee's perceived barriers and continuance to comply with security policies H3 (β = 0.0941, p = 0.05), employee's perceived severity and continuance to comply with security policies H4 (β = 0.1394, p = 0.05) and employee's perceived susceptibility towards continuance to comply with security policies H5 (β = 0.2556, p = 0.05) were supported. On the other hand, the paths between employee's perceived benefits and continuance to comply with security policies H2 (β = 0.1038, p = 0.466), cues to action and continuance to comply with security policies H6 (β = 0.0868, p = 0.757), self-efficacy and continuance to comply with security policies H7 (β = 0.0840, p = 0.222) and employee's information security awareness towards continuance to comply with security policies H8 (β = 0.0825, p = 0.68) were not supported. The final structural model shown in figure 3 indicates that the dependent variable (compliance continuance intention) had explained 70% of the total variance (R^2).

Table 4: Results of Hypotheses Testing

Hypotheses and Paths			Estimate	S.E.	P- Value	Remarks
H1	Commitment	Continuance Intention	0.769	0.219	0.000**	Supported
H2	Benefits	Continuance Intention	0.075	0.103	0.466	Not Supported
H3	Barriers	Continuance Intention	-0.184	0.094	0.050*	Supported
H4	Severity	Continuance Intention	0.466	0.139	0.000**	Supported
H5	Susceptibility	Continuance Intention	0.523	0.255	0.040*	Supported
H6	Cues	Continuance Intention	0.026	0.086	0.758	Not Supported
H7	Self- Efficacy	Continuance Intention	0-.102	0.084	0.222	Not Supported
H8	Awareness	Continuance Intention	-0.034	0.082	0.680	Not Supported

Note : * $p < 0.05$, *** $p < 0.001$

As indicated in table 4 and figure 3, employee's continued intention to comply with security policies depends on levels of perceived susceptibility and severity of security attacks on organization information resources. In other words, employees will continue to adhere to security policies as long as the organizational information systems are at risk of being attacked and if the attacks would be severe. This finding is consistent with (Warkentin et al., 2016). Furthermore, as expected, when the commitment of an employee towards organization activities is high, the likelihood to continue to follow organization security policies also increases. On the other hand, the presence of barriers such as lack of time, difficultness of security controls etc., may discourage users of organization information systems to continue to following security policies. The presence of barriers has been documented in the literature such that have a negative effect on the execution of information security behaviours (Claar & Johnson, 2012; Davinson & Sillence, 2010; Johnson, 2015).



*Note: Significant at * $p < 0.05$, *** $p < 0.001$*

Figure 3: Results of Paths analysis

Interestingly, employee's perceptions of benefits of security policies, security awareness, and self-efficacy could not influence user's intention to continue following security policies. In comparison with previous findings, these three factors have widely been found to influence intention to perform a range of security-related behaviours. For instance perceived benefits have been found to influence adoption of computer security software among the users (Ng et al., 2009) and self –efficacy was found to influence protective security behaviours when opening email attachments and adoption of computer security software (Claar & Johnson, 2012; Ng et al., 2009), while security awareness was found to influence password related behaviours (Stanton, Stam, Mastrangelo, & Jolton, 2005). Therefore it is important to find out the reasons that could have contributed to this. Literature informs us that, there is lack of security training among Tanzania government employees (Bakari, Tarimo, & Mutagahywa, 2006). Possibly, lack of adequate security training could, in turn, diminish user's security awareness, confidence, and ability to continue following the security policies.

The primary use of cues is to improve memory capability with regard to the execution of behaviours (Eysenck, 2009; Vu et al., 2007) and stimulate user's intention to continuously execute acceptable security behaviours (Botta, Muldner, Hawkey, & Beznosov, 2011). Perhaps the effect of cues on security behaviours was clear during the initial stages of information security policies inception in the studied organization when the memory on the existence of security policies was low. However, as time goes by, users become familiar with the terms and requirements of the policy may not continue relying on the presence of cues as a motivation for them to continue following security policies. This finding of this study is consistent with (Claar & Johnson, 2012; Ng et al., 2009).

Implications

Our findings suggest that organizations should plan for ways to keep the levels of perceived susceptibility and severity up among the employees in order to motivate continued compliance with security policies. This can be achieved through regular information security training (Whitman, 2003) with regard to malicious online resources and consequences an organization could face if an employee violates security policies. Proper security training could lead to reduced number of security policy violations(Straub & Welke, 1998).

Further, our findings indicate that there is a necessity to reduce barriers that obstruct continued compliance with security policies; because employees who believe security controls such policies could hinder completion of their work are likely to violate the policies (Post & Kagan, 2007). To reduce the barriers, assessment of the barriers should be conducted along with strategies to reduce them. Taking into consideration that, security management is a mutual achievement all multiple parties in an organization (Dourish, Grinter, DeLaFlor, & Joseph, 2004), dialogue between management, security personnel, and the end user can be arranged on aspects that obstruct security policy compliance. For example, dialogue may be needed during the distribution of workloads among the employees and setting of realistic deadlines. In this way, employees may not need to violate security policies to in order to meet the deadlines. Also, security processes can be re-engineered to reduce unnecessary security controls which could be contributing to a violation of security policies. However, careful consideration should be observed during re-engineering of security controls to avoid creation of security loopholes.

With regard to employee's organizational commitment, we recommend promotion of organization mission, vision and values to employees and involving them in the process of decision making. By doing so, employee's commitment to organization goals, and obligation to rules, procedures, and policies will be assured (Randall, 1987; Stanton, Stam, Guzman, & Caledra, 2003). It should be noted that a committed employee is the most ardent supporters of organization goals, policies, and objectives and always strive to accomplish what is committed to (Zimbardo & Leippe, 1991), thus having a cadre of committed employees is crucial for the success of security policies. Further, organizations need to pursue ways to increase employee's self-efficacy when complying with security policies, perceived benefits of continuing to comply with security policies and information security awareness.

Giving feedback on how employees comply or not comply with security policies could help to boost-up confidence and ability of compliant employees and provide room for improvement for the non-compliant employees (Escartí & Guzmán, 1999; Karl, O'Leary, Kelly, & Martocchio, 1993) while information security training could increase employee's perceived benefits of continuing to comply with security policies. Also, sufficient security awareness training should be conducted regularly in order to develop a cadre of secure aware employees who will consciously comply with security policies in the future.

Limitations and Direction for Future studies

Two limitations are facing this study. First, respondents of the study were sourced from only one country, thus findings of this study could not be applicable to other countries due to the difference in work environment and culture of the country. Second, the current study used cross-sectional approach. The results obtained from cross-sectional studies may differ over a period of time if the existing situation changes. Thus, due to rapid changes in ICT and information system field in general, future studies may investigate changes in the intention of the employees to continue to comply with security policies in longitudinal studies. Conducting a similar study by measuring the extent of changes in intention to continue to comply with security policies over time may provide new insights into information security behaviour research.

Conclusion

The present study investigates the intention of employees working in public organizations to continue to comply with information security policy. Given that information security continuance compliance literature is scarce, this study broadens our understanding of the factors that influence users of information systems in the workplace to comply with information security policies. To investigate the factors, the study extended the health beliefs model (HBM) through the inclusion of organizational commitment and security awareness constructs. The study concludes that the extended HBM is useful to explain factors towards continuous compliance with information security policy. Generally, findings of this study imply that organizational commitment, perceived barriers, perceived severity and perceived susceptibility can be used to motivate employees to continue to comply with information security policy as they are the key factors for information security policy compliance continuance intention.

REFERENCES

Amine, A. (1998). Consumers' true brand loyalty: the central role of commitment. *Journal of Strategic Marketing*, *6*(4), 305–319.

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modelling in practice: A review and recommended a two-step approach. *Psychological Bulletin*, *103*(3), 411.

Armitage, C., & Conner, M. (2001). Efficacy of the Theory of Planned Behaviour: A Meta-Analytic Review. *The British Journal of Social Psychology*, *40*(4), 471–499.

Awang, Z. (2015). *SEM Made Simple: A Gentle Approach to Learning Structural Equation Modeling*. Selangor, Kuala Lumpur: MPWS Rich Publication.

Bacon, D., Sauer, P., & Young, M. (1995). Composite Reliability in Structural Equation Modelling. *Educational and Psychological Measurement*, *53*(3), 394–406.

Bagozzi, R., Yi, Y., & Phillips, L. (1991). Assessing Construct Validity in Organizational Research. *Administrative Science Quarterly*, *36*, 421–458.

Bakari, J. K., Tarimo, C. N., & Mutagahywa, B. (2006). Issues and Challenges to be Addressed in e-Government from an Information Security Point of View. In *Proceedings of IST-Africa 2006 Conference, IIMC*.

Bandura, A. (1977). Self-efficacy: Toward a Unifying Theory of Behavioral Change. *Psychological Review*, *84*(2), 191.

Bhattacherjee, A. (2001). Understanding information systems continuance: an expectation-confirmation model. *MIS Quarterly*, 351–370.

Botta, D., Muldner, K., Hawkey, K., & Beznosov, K. (2011). Toward understanding distributed cognition in IT security management: the role of cues and norms. *Cognition, Technology & Work*, *13*(2), 121–134.

Bowen, P., Chew, E., & Hash, J. (2007). Information Security Guide For Government Executives. Gaithersburg: NIST.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, *34*(3), 523–548.

Chang, S.-J., Van Witteloostuijn, A., & Eden, L. (2010). From the editors: Common Method Variance in International Business Research. *Journal of International Business Studies*, *41*(2), 178–184.

Claar, C. (2011). *The Adoption of Computer Security: An Analysis of Home Personal Computer User Behavior Using the Health Belief Model.* Utah State University, USA.

Claar, C., & Johnson, J. (2012). Analyzing Home PC Security Adoption Behavior. *Journal of Computer Information Systems*, *52*(4), 20–29.

Cochran, W. (1977). *Sampling Techniques* (3rd Ed). New York: John Wiley & Sons.

Çokluk, Ö., & Yılmaz, K. (2010). The relationship between leadership behaviour and organizational commitment in Turkish primary schools. *Bilig*, *54*, 75–92.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–98.

Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. *Computers in Human Behavior*, *26*(6), 1739–1747.

Dhillon, G. (1999). Managing and controlling computer misuse. *Information Management & Computer Security*, *7*(4), 171–175.

Dhillon, G., & Moores, S. (2001). Computer crimes: theorizing about the enemy within. *Computers & Security*, *20*(8), 715–723.

Dignan, L. (2016). Security spending to top $100 billion by 2020: Are we any cyber safer? Retrieved April 1, 2017, from http://www.zdnet.com/article/security-spending-to-top-100-billion-by-2020-are-we-any-cyber-safer/

Dourish, P., Grinter, R. E., DeLaFlor, J., & Joseph, M. (2004). Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, *8*(6), 391–401.

Eisenberger, R., Huntington, R., Hutchison, S., & Sowa, D. (1986). Perceived Organizational Support. *Journal of Applied Psychology*, *71*, 500–507.

Escartí, A., & Guzmán, J. F. (1999). Effects of feedback on self-efficacy, performance, and choice in an athletic task. *Journal of Applied Sports Psychology*, *11*(1), 83–96.

Eysenck, M. W. (2009). Improving your memory. In A. Baddeley, M. Eysenck, & M. Anderson (Eds.), *Memory* (pp. 357–380). New York, USA: Psychology Press.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology*, *30*(2), 407–429.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39–50.

Fry, M., Drennan, J., Previte, J., White, A., & Tjondronegoro, D. (2014). The role of desire in understanding intentions to drink responsibly : an application of the Model of Goal-Directed Behaviour. *Journal of Marketing Management*, *30*(6), 551–570.

Hair, J., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate Data Analysis : Multivariate data analysis: A Global Perspective* (7th Ed). London, UK: Prentice-Hall.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). *Multivariate data analysis* (6th Ed). Upper Saddle River, NJ: Pearson Prentice Hall.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2015). PLS-SEM : Indeed a Silver Bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139–152.

Hardy, C. a, & Williams, S. P. (2010). Managing information risks and protecting information assets in a web 2.0 era. In *Proceedings of the 23rd Bled e- Conference e-Trust: Implications for the Individual, Enterprises and Society* (Vol. 2006, pp. 234–247).

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modelling. *Journal of the Academy of Marketing Science*, *43*(1), 115–135.

Hentea, M., Dhillon, H. S., & Dhillon, M. (2006). Towards Changes in Information Security Education. *Journal of Information Technology Education*, *5*, 221–233.

Herath, T., & Rao, H. R. (2009a). Protection Motivation and Deterrence: a Framework for Security Policy Compliance in Organisations. *European Journal of Information Systems*, *18*(2), 106–125.

Herath, T., & Rao, H. R. (2009b). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. *European Journal of Information Systems*, *18*, 106–125.

Ho, R. (2006). *Handbook of univariate and multivariate data analysis and interpretation with SPSS*. New York: Chapman.

Hochbaum, G. M. (1958). *Public Participation in Medical Screening Programs: A Socio-Psychological Study.* Washington, USA: US Department of Health, Education, and Welfare, Public Health Service, Bureau of State Services, Division of Special Health Services, Tuberculosis Program.

Hong, K.-S., Yen-Ping, C., Chao, L. R., & Tang, J.-H. (2003). An Integrated System Theory of Information Security Management. *Information Management & Computer Security*, *11*(5), 243–248.

Hox, J., & Bechger, T. (1998). An Introduction to Structural Equation Modeling. *Family Science Review*, *11*, 354–373.

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, *6*(1), 1–55.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture* Managing

Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational... *Decision Sciences*, *43*(4), 615–660.

Ifinedo, P. (2012). Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. *Computers and Security*, *31*(1), 83–95.

Ifinedo, P. (2014). Information Systems Security Policy Compliance: An Empirical Study of the Effects of Socialisation, Influence, and Cognition. *Information and Management*, *51*(1), 69–79.

Jafri, M. H. (2010). Organizational Commitment and Employee's Innovative Behavior. *Journal of Management Research*, *10*(1), 62–68.

Johnson, C. W. (2015). Barriers to the use of intrusion detection systems in safety-critical applications. In *International Conference on Computer Safety, Reliability, and Security* (pp. 375–384).

Karl, K. A., O'Leary-Kelly, A. M., & Martocchio, J. J. (1993). The impact of feedback and self-efficacy on performance in training. *Journal of Organizational Behavior*, *14*(4), 379–394.

Kline, B. (2015). *Principles and Practice of Structural Equation Modeling* (4th ed.). New York: Guilford Press.

Kothari, C. R. (2011). *Research Methodology: Methods and Techniques* (2nd Ed). New Delhi, India: New Age International.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security*, *10*(2), 57–63.

Lee, M. (2013). *Exercise Barriers in Cancer Survivors: A Multi-Dimensional Approach.* University of South Florida, USA.

Lee, Y., & Larsen, K. (2009). Threat or Coping Appraisal: Determinants of (SMB) Executives Decision to Adopt Anti-malware Software. *European Journal of Information Systems*, *18*(2), 177–187.

Lewis, J. (2003). Cyberterror: Missing in action. *Knowledge, Technology & Policy*, *16*(2), 34–41.

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding Compliance with Internet Use Policy from the Perspective of Rational Choice Theory. *Decision Support Systems*, *48*(4), 635–645.

Liang, H., & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage : A Threat Avoidance Perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413.

Mahabi, V. (2010). *Florida State University Libraries Information Security Awareness : System Administrators and End-User Perspectives at Florida State University.* Florida State University.

McKnight, D. H., Lankton, N., & Tripp, J. (2011). Social networking information disclosure and continuance intention: A disconnect. In *System Sciences (HICSS), 2011 44th Hawaii International Conference on* (pp. 1–10). IEEE.

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory. *Journal of Applied Social Psychology*, *30*(1), 106–143.

Mowday, R. T. (1999). Reflections on the study and relevance of organizational commitment. *Human Resource Management Review*, *8*(4), 387–401.

Ng, B., Kankanhalli, A., & Xu, Y. (2009). Studying Users' Computer Security behaviour: A health Belief Perspective. *Decision Support Systems*, *46*(4), 815–825.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Which Factors Explain Employees' Adherence to Information Security Policies? An Empirical Study. In *Pacis 2007 Proceedings* (pp. 438–439). Aukland, USA.

Paine, L. S. (1994). Managing for organizational integrity. *Harvard Business Review*, *72*(2), 106–117.

Perry, J. L. (1996). Measuring Public Service Motivation: An Assessment of Construct Reliability and Validity. *Journal of Public Administration Research and Theory*, *6*(1), 5–22.

Peyman, N., Hidarnia, A., Ghofranipour, F., Kazemnezhad, A., Oakley, D., Khodaee, G., & Aminshokravi, F. (2009). Self-efficacy: Does it Predict the Effectiveness of Contraceptive Use in Iranian Women? *Eastern Mediterranean Health Journal*, *15*(5), 1254–1262.

Podsakoff, P. M., Mackenzie, S. B., Lee, J., & Podsakoff, N. P. (2003). Common Method Biases in Behavioral Research : A Critical Review of the Literature and Recommended Remedies. *Journal of Applied Psychology*, *88*(5), 879–903.

Posey, C., Roberts, T. L., Lowry, P., & Bennett, R. (2013). Insiders' Protection of Organizational Information Assets: Development of a Systematics-based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors. *MIS Quarterly*, *37*(4), 1189–1210.

Post, G. V, & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security*, *26*(3), 229–237.

PWC. (2015). *Information Security Breaches Survey 2015: Technical Report.* Retrieved from /www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf

Rahman, S., & Donahue, S. (2010). Convergence of Corporate and Information Security. *International Journal of Computer Science and Information Security*, *7*(1), 63–68.

Randall, D. M. (1987). Commitment and the organization: The organization man revisited. *Academy of Management Review*, *12*(3), 460–471. http://doi.org/10.5465/AMR.1987.4306561

Reiser, L. M. (2007). *Health Beliefs and Behaviors of College Women.* University of Pittsburgh, USA.

Rosenstock, I. M. (1974). Historical Origins of the Health Belief Model. *Health and Behaviour*, *2*(4), 328–335.

Schwab. (1980). Construct validity of organizational behaviour. In B. Staw & L. Cummings (Eds.), *Research in organizational behaviour* (pp. 3–43). Greenwich: JAI Press.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2009). Technical Opinion Are employees putting your Company at Risk by not Following Information Security Policies? *Communications of the ACM*, *52*(12), 145–147.

Siponen, M., Mahmood, M., & Pahnila, S. (2014). Employees' Adherence to Information Security policies: An Exploratory Field Study. *Information and Management*, *51*(2), 217–224.

Stanton, J. M., Stam, K. R., Guzman, I., & Caledra, C. (2003). Examining the Linkage Between Organizational Commitment and Information Security. In *Systems, Man and Cybernetics, 2003. IEEE International Conference on* (Vol. 3, pp. 2501–2506).

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of End User Security Behaviors. *Computers and Security*, *24*(2), 124–133.

Straub, D. W., & Welke, R. J. (1998). Coping With Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, *22*(4), 441–469.

Tabachnick, B. G., & Fidell, L. S. (2007). *Using multivariate statistics.* (Fifth). Boston, USA: Allyn & Bacon/Pearson Education.

Vervloet, M., Linn, A. J., van Weert, J. C., de Bakker, D. H., Bouvy, M. L., & van Dijk, L. (2012). The effectiveness of interventions using electronic reminders to improve adherence to chronic medication: a systematic review of the literature. *Journal of the American Medical Informatics Association*, *19*(5), 696–704.

Vu, K.-P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B.-L. B., Cook, J., & Schultz, E. E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies*, *65*(8), 744–757.

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of Protective Security Behavior: A Longitudinal Study. *Decision Support Systems*, *92*(September), 25–35.

Whitman, M. E. (2003). Enemy at the Gates: Threats to Information Security. *Communications of the ACM*, *46*(8), 91–95.

Whitman, M. E., Townsend, A. M., & Aalberts, R. J. (2001). Information systems security and the need for policy. In *Information security management: Global challenges in the new millennium* (pp. 9–18). IGI Global.

Wood, C., & Banks, W. (1993). Human Error: An Overlooked but Significant Information Security Problem. *Computers & Security*, *12*(1), 51–60.

Woon, I., Tan, G., & Low, R. (2005). A Protection Motivation Theory Approach to Home Wireless Security. In *Proceedings of the Twenty-Sixth International Conference on Information Systems* (pp. 367–380). Las Vegas, USA.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security Lapses and the Omission of Information Security Measures: A threat Control Model and Empirical Test. *Computers in Human Behavior*, *24*, 2799–2816.

Yaojun, H., & Yongliang, W. (2015). Modeling and Empirical Study of Users ' Continuance Intention Toward Location Based Service. *International Business and Management*, *11*(2), 8–15.

Zhao, K., Stylianou, A. C., & Zheng, Y. (2013). Predicting users' continuance intention in virtual communities: The dual intention-formation processes. *Decision Support Systems*, *55*(4), 903–910.

Zimbardo, P. G., & Leippe, M. R. (1991). *The psychology of attitude change and social influence.* New York: Mcgraw-Hill Book Company.