International Journal of Security and Networks

ISSN online: 1747-8413 - ISSN print: 1747-8405
https://www.inderscience.com/ijsn

A multi-theory model to evaluate new factors influencing information security compliance

Aatish Chiniah, Feroz Ghannoo

DOI: 10.1504/IJSN.2022.10053519

Article History:

Received:	11 January 2022
Last revised:	13 January 2022
Accepted:	20 January 2022
Published online:	03 April 2023

A multi-theory model to evaluate new factors influencing information security compliance

Aatish Chiniah*

Department of Digital Technologies,
University of Mauritius,
Reduit, Mauritius
Email: a.chiniah@uom.ac.mu
*Corresponding author

Feroz Ghannoo

UoM Trust,
University of Mauritius,
Reduit, Mauritius
Email: ferozghannoo@yahoo.co.uk

Abstract: Many organisations recognise that their employees, who are often considered the weakest link in information security, can also be great assets in the effort to reduce risk related to information security. This research identifies the antecedents of employee compliance with the information security policy (ISP) of an organisation. A survey among computer users of organisations in Mauritius which have established information security policy was carried out. A novel multi-theory model is derived from theory of reasoned action, cognitive evaluation theory and hanoo, and that model is presented to evaluate the data gathered through the survey. The results show that an employee's intention to comply is influenced by attitude, security awareness programs and rewards. Intention to comply in turn influences actual compliance to ISP.

Keywords: information security; compliance behaviour; information security policy.

Reference to this paper should be made as follows: Chiniah, A. and Ghannoo, F. (2023) 'A multi-theory model to evaluate new factors influencing information security compliance', *Int. J. Security and Networks*, Vol. 18, No. 1, pp.19–29.

Biographical notes: Aatish Chiniah is a Senior Lecturer in the Department of Digital Technologies, University of Mauritius. He completed his BEng in Computer Science and Engineering from the Saint-Petersburg Electro-Technical University 'LETI' in 2005. He then obtained his MSc in Computer Systems and Networking from the University of Greenwich, London, UK, in 2007. He worked as a Network Engineer and IT Consultant, before joining the University of Mauritius in 2009. In 2013, he went to the Nanyang Technological University, Singapore to embark on a PhD in Distributed Systems. His areas of interest are cloud computing, networking, mobile computing and technology adoption.

Feroz Ghannoo is a System Administrator at the National Housing Development Co. Ltd., Mauritius. He completed his BSc in Computing and Information System from the London Metropolitan University in 2005. In 2019, he obtained his MBA in IT Enterprise Management from the University of Mauritius and MSc in Enterprise Security and Digital Forensics from University of Technology, Mauritius, in 2022. His areas of interest are artificial intelligence, IT security and digital forensics.

1 Introduction

Today organisations rely more on information systems. It is growingly important for these organisations to manage the threats to information security as information security breaches may have grave consequences for their clients and themselves (Cavusoglu and Raghunathan, 2004; Kritzinger and Smith, 2008). Thus, ensuring security of information has become one among the biggest challenges and priorities for them (Posthumus and Von Solms, 2004). To protect information, organisations are spending increasingly more on technological solutions but incidents are increasing in numbers and severity. Depending only on or more than necessary on technological solutions is rarely adequate to do away with the risks of information security breaches (Cavusoglu et al., 2009; Siponen, 2005). Siponen and Vance (2010) believe that most incidents concerned with information security result directly or indirectly from employees' misuses, inexperience errors or deliberate abuses. Substantial resources are allocated to develop

growingly advanced technologies but it is employees and other organisational factors which are the most important threats to the information security of their organisations. Hence information security built on a comprehension of 'organisational' factors contributes to an important protection against the threats (Hu et al., 2007). To discern information security problems, Dhillon and Backhouse (2001) suggest a 'socio-organisational' point of view as it is employees who design and run the information systems and the technologies. Many literature of information security on insiders have concentrated on unacceptable conduct of employees and considered them as potential threats to information security. However, on the side of the coin it must be recognised that employees can be used to protect the technologies and information of organisations. To encourage employees to act responsibly, organisation create information security policy.

Previous studies (Siponen, 2005) have put forward information security polices for consideration to deal with the rise in security threats. Consequently, spending in both 'socio-organisational' and technical resources is required to raise information security (Bulgurcu et al., 2010). Most companies are conscious of the significance of 'information security' policy. Organisations create ISPs providing employees with instructions on information security to comply with while they utilise information systems to carry out their works. Employees' 'information security' policy compliance still worries organisations in spite of an ISP document (Alotaibi et al., 2016). Compliance with information security may be missing although the defined policies may be very understandable (von Solms and von Solms, 2004; Herath and Rao, 2009a). The existence of policy documents do not de facto means compliance by employees. Information security measures are ineffective if users do not abide by the policies (Puhakainen and Siponen, 2010). Mitnick and Simon (2003) consider employees, in information security, as the weakest link. For that reason employee's information security policy compliance has turned into a very important socio-organisational factor. Consequently, it is very important to understand the user's behaviours which affect to compliance with security policies in establish security programs (Abraham, 2011). Information systems security which is built on the comprehension of organisational factors will cater for a better protection against these threats. Socio-organisational factors are very significant to ensure the security of information system because it is human beings who design and run the information systems and the technologies. Human beings make link the between the technologies and the outside world. Several elements have a direct effect on users' behaviour regarding information security policy. These factors are grouped into human and organisational factors (Alotaibi et al., 2016). Among many others, Von Solms and Von Solms (2004) and Hu and Dinev (2005), have studied these two groups of factors.

1.1 Problem statement

Unfortunately employees rarely abide with information security policies endangering the assets of their organisations [Stanton et al., (2005), p.125]. For that reason employees should not be aware of but also abide by policies for an information security which is effective. Understanding what factors inspire employees to abide by ISP is important so that practitioners can identify the shortages in their information security management endeavour and come up with solutions for the behavioural problems of users. Instead of that, companies concentrate more attacks from outside overlooking the statistics. Moreover, organisations are expending increasingly on technologies but pay less attention to the human aspect of security breaches (Vroom and von Solms, 2004). Vroom and von Solms (2004) state that security breaches result from negligence, ignorance or malicious intentions. These indicate the misfiring of information security administration programs that ignore individual beliefs and values to stimulate abidance by information security policies (Mishra and Dhillon, 2006; Herath and Rao, 2009b). The previous studies do not provide a theoretical and empirical model which explains neither the reason for the non-compliance of employees with information security policies nor the elements that influence their compliance (Alotaibi et al., 2016).

1.2 Proposed solution

A theoretical model which comes from the theory of reasoned action, cognitive evaluation theory and general deterrence theory (GDT) with an objective to provide an insight of how to raise employees' compliance. Other factors (human and organisational) identified by Alotaibi et al. (2016) are added to this model. These theories can help to comprehend how organisations can raise the compliance of their since employees' compliance is a psychological phenomenon. This study will test proposed theoretical model and confirm it empirically to the factors affecting the compliance of employees' with information security policies. This will be helpful for IT professionals who need empirically validated information based on grounded theoretical model. Several studies have tried to pinpoint reasons for the various levels of compliance. Alotaibi et al. (2016) have gone through the literature and categorised the influencing factors have been categorised into two types: organisational and human.

2 Related works

Due to the significance of information security to organisations, there has been a rapidly increasing number of studies on compliance and non-compliance of employees with information security policies. Puhakainen (2006) has analysed 60 different methods developed to improve the information security compliance of employees. These include: criminology-based models (e.g., Siponen and

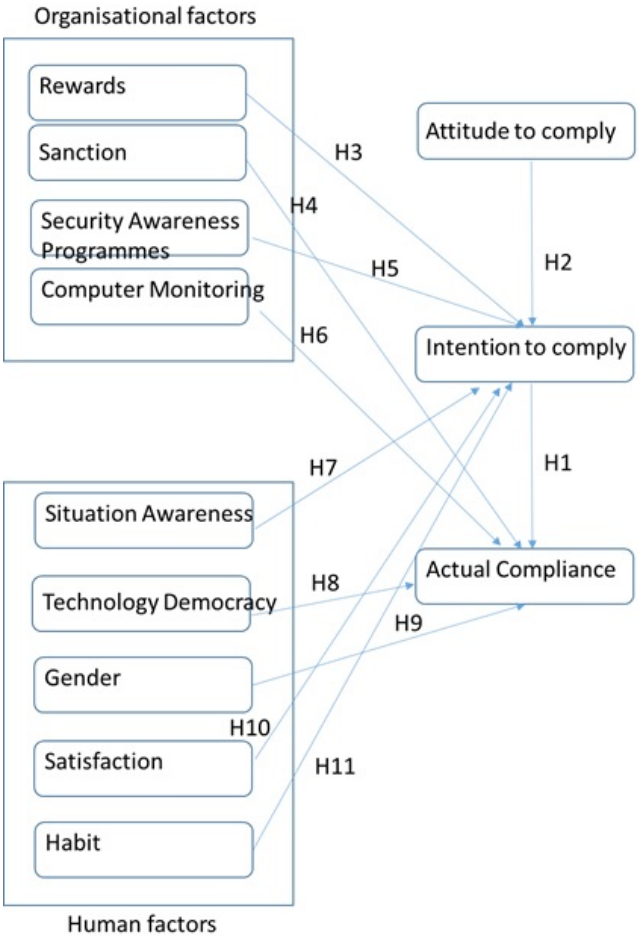
Vance, 2010), security awareness programs and training (Siponen, 2000), social-cognitive models (Siponen et al., 2007; Pahnila et al., 2007). They also encompass GDT to comprehend human behaviour concerning intentional misuse and computer crime (e.g., Straub and Welke, 1998) and those look into abuse by insiders (e.g., Siponen and Willison, 2009). Other studies used protection motivation theory (PMT) in order to comprehend the behaviour of users in the context of security measures. Academics carrying out research on information security problems have built their investigation on different theories, including theory of planned behaviour (Bulgurcu et al., 2010), learning theories (Puhakainen and Siponen, 2010), communication theory, control theory and institutional theory. A high number of studies examined the efficacy of rewards and deterrence (e.g., Herath and Rao, 2009a, 2009b; D'Arcy et al., 2009). They recommended to use deterrent strategy against security policy non-compliance and computer abuse. Other studies recommended rewards to foster improved performance and desirable behaviours. Other psychological and cognitive factors were added in the behaviour models (e.g., Bulgurcu et al., 2010; Siponen and Vance, 2010; Myyry et al., 2009). As single theory centres on individual factors in spite of empirical proof of researches that external factors also are instrumental. Theories that explain and forecast the conduct of employees, may become ineffective by overlooking the external factors and their independencies with the internal factors. In order to reduce the blank space between outcome of conduct, and individual and external, some researches included additional factors, which affect the individual behaviour, in their theoretical models (Lebek et al., 2014). Herath and Rao (2009a) were the first to use several theories. It is expected that a model which is one integrated one will explain better than one obtained based a sole theory. Some academics included theoretical extensions of additional factors which affect the individual behaviour to reduce the rift between behavioural outcome and individual and external factors (Lebek et al., 2014). In other studies other factors (e.g., habit, social influence, environment, personality, etc.) were advanced to influence the behaviour of employees. Organisations count on their employees in addition to the technologies deployed for the protection their information assets. As these employees play some part in protecting these assets, organisations, while developing policy, should concentre their attention on the factors which influence an employee to act responsibly (Bulgurcu et al., 2010). Hence it is important to make further studies on information security. According to Siponen et al. (2014), many approaches of information security compliance have been advanced. However, they do not provide empirical proof to support their principles (Siponen et al., 2010, 2014). This is a major defiency as practitioners are in need of approaches that have been tried and tested to show that the approach works in reality (Siponen and Vance, 2010).

Several significant theoretical models have been proposed. Various individual and organisational factors influencing employee information security behaviour have been established. However, according to Hu et al. (2012) the most influential theoretical models are criminological theories and cognitive theories. Earlier, researches used only unique theory (TRA/TPB, PMT, rational choice model) and theories were brought from criminology and social psychology to information security literature to account for and forecast employees' security-related behaviour (Lebek et al., 2014). However the most regularly used one in the information security studies are TRA/TPB, GDT, PMT and TAM (Lebek et al., 2014). As single theory centres on individual factors in spite of empirical proof of researches that external factors also are instrumental. Theories that account for and forecast employee's behaviour may be ineffective by overlooking these factors and interdependencies (Lebek et al., 2014). Besides, Herath and Rao (2009a), not any of the previous researches were built using several theories. It is expected that a model which is one integrated one will explain better than one obtained based a sole theory. Some academics included theoretical extensions of additional factors which affect the individual behaviour to reduce the rift between behavioural outcome and individual and external factors (Lebek et al., 2014). The present existing literature acknowledges that insiders may constitute a challenge to an organisation because their ignorance, mistakes, and deliberate acts can endanger information security. Hence, studies on factors which drive the compliance of users are emerging.

3 Proposed model

A multi-model theory by integrating three theories which are theory of reasoned action, and cognitive evaluation theory and GDT is being proposed. This model explains the behaviour of employees. The model will help to understand the factors which affect the compliance of employees. Human and organisational factors identified from the studies of Alotaibi et al. (2016) are included in the proposed model. First, we start by adopting three main constructs of the TRA – actual comply, intention to comply and attitude. Then, the model sanction from the GDT and rewards is added. Finally, security awareness program, computer monitoring, technology democracy, situation awareness, gender, satisfaction and habit based on the factors identified by Alotaibi et al. (2016) are also included to derive the final proposed model. Organisations need advice how to foster compliance of information security by their users. Many studies have been carried out in that context and they offer parts of the solution. The study of Alotaibi et al. (2016) has examined many variables taken from important theories and studies in the field of information security. The proposed multi-theory model developed is quite alike to the one used by Siponen et al. (2014). These theories can help to comprehend how organisations can raise the compliance of their since employees' compliance is a psychological phenomenon.

Figure 1 Proposed model (see online version for colours)



3.1 Hypotheses

The constructs actual compliance with policies and intention to comply are derived the theory of reasoned action. Actual behaviour should be included in studies to avoid wrong deduction (Limayem and Hirt, 2003). Intentions pull in the motivational factors that have an influence on behaviour. It points out how seriously people are willing to attempt the required behaviour. Behavioural intention affects an individual's actual intention to carry out the behaviour. Thus, it can be said that the stronger an individual's intention to comply with such policies, the more likely that individual will actually comply.

H1 Employees' intention to comply positively influences their actual compliance.

H2 Employees' attitude positively influences employees' intention to comply.

H3 Rewards positively influences employees' intention to comply.

H4 Sanction positively influences employees' actual compliance.

H5 Security awareness programs positively affect employees' intention to comply.

H6 Computer monitoring positively influences employees' actual compliance.

H7 Situation awareness positively influences employees' intention to comply.

H8 Gender influences employees' actual compliance.

H9 Technology democracy positively influences employees' actual compliance.

H10 Satisfaction positively influences employees' intention to comply.

H11 Habit positively influences employees' intention to comply.

3.2 Survey design and distribution

A questionnaire was designed using appropriate measurement scales from the existing literature. The questionnaire was structured into five sections. Section 1 requested demographic data of the users. In this section, an inclusion-criteria question was included. The answers of respondents working organisations having established information security policy. The computer users were not informed of that criteria. Section 2 was concerned with the constructs (actual compliance, intention to comply and attitude to comply) of the main theory which is the theory of reasoned action. Section 3 captured data about organisational factors and Section 4 was concerned with human factors. In the last section, the respondents were asked an open-ended question.

As there was census available on the number of organisations which have established Information Security Policy, the sample size could not be calculated. For that reason the method of convenient was chosen. The target population of this study was computer users in organisations of Mauritius which have established information security policy. An online questionnaire using Google Form was used to collect data. The hyperlink of the questionnaire was sent to some 675 software companies and individuals in Mauritius by e-mails and messages. Some 75 e-mails were undeliverable. In the end 40 responses were received.

4 Data analysis

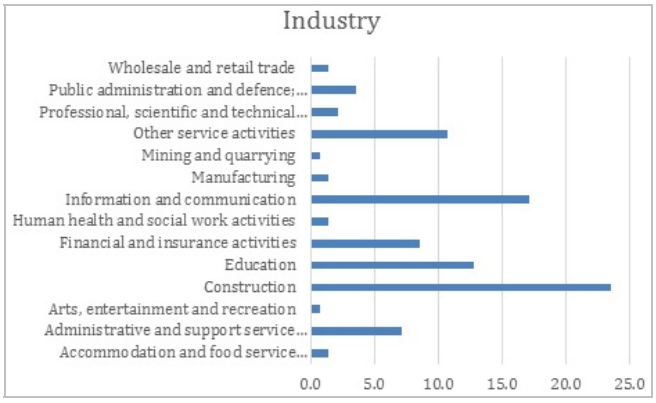
4.1 Demographic information

Female represented a bigger percentage of the sample (63.6%) and the remaining were male (36.4%). The age group was distributed as follows: 18–24 years (22.1%), 25–39 years (47.1%), 40–49 years (20.7%), 50–59 years (8.6%) and 60 or above (1.4%). The sample was well-educated. More than 80% of the respondents have a diploma at least.

The respondents are from a broad range of organisation categories. These are construction (23.6%), information and communication technology (17.1%), education (12.9%), other services activities (10.7%), financial and insurance

activities (8.6%) and administrative and support service activities (7.1%).

Figure 2 Industry of respondents (see online version for colours)



4.2 Descriptive statistics of variables

Table 1 shows the mean, standard deviation, minimum and maximum value of each constructs. The means of construct evaluated by the respondents range from 3.01 to 3.95. As per Likert scale, 1 indicates strongly disagree, 2 disagree, 3 neutral, 4 agree and 5 strongly disagree.

Table 1 Descriptive statistics of variable

Constructs	*Mean*	*Standard deviation*	*Minimum*	*Maximum*
Actual compliance	3.80	0.87	1.0	5.0
Intention to comply	3.73	0.87	1.0	5.0
Attitude to comply	3.95	0.93	1.0	5.0
Rewards	3.01	0.87	1.0	5.0
Sanctions	3.28	0.87	1.0	5.0
Security awareness programs	3.45	1.01	1.0	5.0
Computer monitoring	3.54	0.92	1.0	5.0
Situation awareness	3.53	0.77	2.0	5.0
Technology_Democracy	3.18	0.90	1.0	5.0
Satisfaction	3.73	0.84	1.0	5.0
Habit	3.39	0.73	1.4	5.0

Note: 1 – strong disagree, 2 – disagree, 3 – neutral, 4 – agree and 5 – strongly agree.

4.3 Reliability, validity and multicollinearity of construct

Normally reliability, content validity and construct validity define the standard of measurement model (Straub et al., 2004). Before testing the hypothesised model, the 'psychometric' characteristics of the measures was evaluated. Reliability, convergent and discriminant validity, multicollinearity and common methods bias tests were also done.

4.3.1 Reliability

The factor loadings of the measurement items were above the threshold of 0.50. This additionally demonstrated reliability of the measurement scales (Nunkoo, 2015).

Table 2 Reliability of construct

Constructs	*Items*	*Corrected item-total correlation*	*Cronbach's alpha*
Actual compliance	AC1	0.813	0.904
	AC2	0.846	
	AC3	0.770	
Intention to comply	INT1	0.911	0.950
	INT2	0.917	
	INT3	0.858	
Attitude	ATT1	0.899	0.963
	ATT2	0.930	
	ATT3	0.935	
Rewards	REW1	0.701	0.824
	REW2	0.701	
Sanctions	SAN1	0.831	
	SAN1	0.919	0.923
	SAN1	0.787	
Security awareness programs	SAP1	0.836	0.909
	SAP2	0.836	
Computer monitoring	CM1	0.772	0.871
	CM2	0.772	
Situational awareness	SA1	0.887	0.947
	SA2	0.909	
	SA3	0.875	
Technology democracy	TM1	0.568	0.841
	TM2	0.825	
	TM3	0.754	
Satisfaction	SAT1	0.937	0.968
	SAT2	0.943	
	SAT3	0.941	
	SAT4	0.870	
	SAT5	0.868	
Habit	HAB1	0.793	0.911
	HAB2	0.680	
	HAB3	0.789	
	HAB4	0.791	
	HAB5	0.816	

4.3.2 Convergent

The factor loading of the measurement items of constructs was computed. Hair et al. (2010, 1998) advanced that factor loadings above than 0.5 demonstrate that the convergent validity is acceptable.

Table 3 Correlations

	Constructs	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
1	Actual compliance	1										
2	Intention to comply	0.766**	1									
3	Attitude	0.824**	0.854**	1								
4	Rewards	0.337**	0.410**	0.329**	1							
5	Sanctions	0.443**	0.482**	0.413**	0.337**	1						
6	Security awareness programs	0.445**	0.481**	0.396**	0.366**	0.347**	1					
7	Computer monitoring	0.439**	0.531**	0.601**	0.438**	0.233**	0.459**	1				
8	Situation awareness	0.470**	0.496**	0.520**	0.305**	0.313**	0.662**	0.448**	1			
9	Technology_Democracy	0.178*	0.216*	0.218**	0.186*	0.127	0.429**	0.326**	0.294**	1		
10	Satisfaction	0.469**	0.589**	0.596**	0.264**	0.419**	0.460**	0.418**	0.664**	0.191*	1	
11	Habit	0.585**	0.579**	0.572**	0.323**	0.354**	0.624**	0.498**	0.742**	0.300**	0.613**	1

Notes: **Correlation is significant at the 0.01 level (2-tailed). *Correlation is significant at the 0.05 level (2-tailed).

4.3.3 Discriminant

The discriminant validity of the measurement items was first examined by analysing the item loadings across constructs. Items of a construct loading more on their own construct than on other constructs show discriminant validity. There should be a minimum difference of 0.10 between the item loading on its own construct and its next highest loading (Gefen and Straub, 2005; Bulgurcu et al., 2009).

Moreover, the correlation between all pairs of constructs was computed to test the discriminant validity of the items. In this case the correlations were below 0.9 demonstrating the discriminant validity of the constructs (Pahnila et al., 2007).

Hence, all the constructs of this study have an acceptable degree of reliability and validity which established the correctness of the measuring scales.

4.3.4 Multi-collinearity

In the multi-regression analysis, multi-collinearity was examined by looking at the 'tolerance and variance inflation factor' (VIF) values for each independent (predictor) construct. The value of VIF is calculated as '1/tolerance'. High values of VIF point out high level of multi-collinearity. Only constructs whose VIF are less than limit value of 10 should be kept for further analysis (Hair et al., 1998; Nunkoo, 2015). All VIF values of the two regression models of this study are with the maximum allowable value of 10. Hence, there is no issue of multi-collinearity.

4.4 Hypothesis testing

Using Pearson's correlation analysis, the following is derived:

H1 Intention to comply positively influences actual compliance ($r = 0.766$; $p < 0.001$).

H2 Attitude positively influences intention to comply ($r = 0.854$; $p < 0.001$).

H3 Rewards positively influences intention to comply ($r = 0.410$; $p < 0.001$).

H4 Sanctions positively influences actual compliance ($r = 0.443$; $p < 0.001$).

H5 Security awareness programs positively influences intention to comply ($r = 0.481$; $p < 0.001$).

H6 Computer monitoring positively influences actual compliance ($r = 0.439$; $p < 0.001$).

H7 Situation awareness positively influences actual compliance ($r = 0.496$; $p < 0.001$).

H8 Technology democracy does not influence actual compliance ($r = 0.178$; $p < 0.05$).

H10 Satisfaction positively influences intention to comply ($r = 0.589$; $p < 0.001$).

H11 Habit positively influences intention to comply ($r = 0.579$; $p < 0.001$).

H9 Gender influences employees' actual compliance.

An independent t-test was conducted. It shows that the means of the two groups of gender (male and female) are not different significantly. Mean scores of the males ($m = 4.09$, $sd = 0.85$) while females ($m = 3.64$, $sd = 0.84$) found no significant difference in gender [$t(138) = 3.017$, $p > .05$]. In this study, gender does not influence employees' actual compliance. In other words, the null hypothesis is accepted.

4.5 Model analysis

For this study, multiple regression analysis were conducted to validate the overall research framework, to evaluate on which factors are more important and to proof all hypotheses. Multiple regression analysis which is multivariate technique, is used to investigate the

relationship between a dependent construct and its independent constructs. It establishes a method of predicting values for the dependent variable for all members of a population (Ng et al., 2009; Nathans et al., 2012; Mertler and Reinhart, 2016).

Table 4 Summary of hypotheses

Hypothesis	
H1: Intention to compliance --> Actual compliance	Accepted
H2: Attitude --> Intention to compliance	Accepted
H3: Rewards --> Intention to compliance	Accepted
H4: Sanction --> Actual compliance	Accepted
H5: Security awareness programs --> Actual compliance	Accepted
H6: Computer monitoring --> Actual compliance	Accepted
H7: Situation awareness --> Intention to comply	Accepted
H8: Technology democracy negatively influences --> Actual compliance	Rejected
H9: Gender --> Actual compliance	Rejected
H10: Satisfaction --> Intention to compliance	Accepted
H11: Habit --> Intention to compliance	Accepted

The coefficient R of the multiple regressions indicates the correlation between the dependent construct (criterion) and the weighted sum of the independent constructs (predictor) (Nunkoo and Gursoy, 2012). R^2 expressed as a percentage, explains how much variance in the dependent construct is explained by the independent variables (Nunkoo and Gursoy, 2012). Other components of the multiple regression analysis are the F-test and the t-test. F-test demonstrates the strength of model; the t-test evaluates whether the dependent variable is influenced by the independent variables (Nunkoo and Gursoy, 2012). The standardised beta coefficients present the importance of the predictor variable on the criterion (Hair et al., 2010).

The null hypothesis is rejected when t value is over 1.645 and p value (Sig.) is 0.05 or lesser (Pallant, 2010).

Four multiple regression analyses were performed to test the hypotheses.

Table 5 displays the multiple regression analysis between intention to comply, sanctions, computer monitoring, technology democracy and gender as independent variables and actual compliance as the dependent variable.

The first model ($F = 39.462$, $p < .001$) explained 59.6% ($R^2 = 0.596$) of the variance of the dependent variable. Intention to comply (ß = 0.690, t-value = 9.388, p = 0.001) has a significant direct influence on actual compliance. Sanctions, computer monitoring, technology democracy and gender do not have a significant effect on actual compliance.

Table 5 Multi-regression analysis

Multiple regression model 1								
Model		*Unstandardised coefficients*	*Standardised coefficients*		*t*	*Sig.*	*Collinearity statistics*	
		B	*Std. error*	*Beta*			*Tolerance*	*VIF*
1	(Constant)	0.822	0.354		2.324	0.022		
	Intention to compliance	0.684	0.073	0.690	9.388	0.000	0.560	1.787
	Sanctions	0.097	0.062	0.097	1.551	0.123	0.765	1.308
	Computer monitoring	0.043	0.064	0.045	0.671	0.504	0.658	1.520
	Technology democracy	0.003	0.057	0.003	0.045	0.964	0.863	1.159
	Gender	–0.028	0.106	–0.015	–0.260	0.795	0.875	1.143

Note: Dependent variable: Actual_compliance.

Table 6 Intention to comply

Multiple regression model 2								
Model		*Unstandardised coefficients*	*Standardised coefficients*		*t*	*Sig.*	*Collinearity statistics*	
		B	*Std. error*	*Beta*			*Tolerance*	*VIF*
1	(Constant)	0.110	0.204		0.536	0.593		
	Attitude	0.681	0.052	0.726	13.125	0.000	0.560	1.785
	Rewards	0.108	0.046	0.107	2.344	0.021	0.825	1.212
	Security awareness programs	0.131	0.051	0.151	2.587	0.011	0.500	1.999
	Situation awareness	–0.156	0.082	–0.138	–1.916	0.058	0.329	3.037
	Satisfaction	0.110	0.063	0.106	1.742	0.084	0.464	2.153
	Habit	0.087	0.082	0.072	1.064	0.289	0.370	2.706

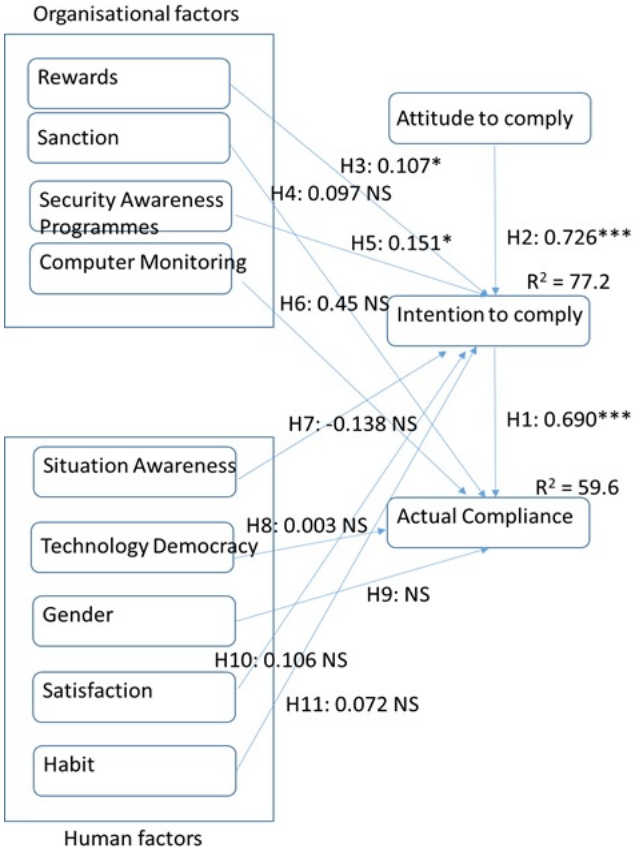
Note: Dependent variable: Intention_to_compliance.

Table 7 Summary of supported or rejected hypotheses

Summary of hypotheses							
	Regression test	R^2	*F*	*Standardised coefficients*	*t*	*Sig.*	*Hypothesis*
				Beta			
1	Actual_Compliance	0.596	39.462***		2.324	0.022	
	Intention to compliance			0.690	9.388	0.000	Supported
	Sanctions			0.097	1.551	0.123	Rejected
	Computer monitoring			0.045	0.671	0.504	Rejected
	Technology democracy			0.003	0.045	0.964	Rejected
	Gender			–0.015	–0.260	0.795	Rejected
2	Intention to compliance	0.772	75.087***		0.536	0.593	
	Attitude			0.726	13.125	0.000	Supported
	Rewards			0.107	2.344	0.021	Supported
	Security awareness programs			0.151	2.587	0.011	Supported
	Situation awareness			–0.138	–1.916	0.058	Rejected
	Satisfaction			0.106	1.742	0.084	Rejected
	Habit			0.072	1.064	0.289	Rejected

Note: ***p < 0.001.

Figure 3 Final model (see online version for colours)



Note: ***p < 0.001, **p < 0.01 and *p < 0.05.

In the second multiple regression analysis the model (F = 75.087, p < .001) explains 77.2% of the variance. Attitude (ß = 0.690, t-value = 9.388, p = 0.001), rewards (ß = 0.690, t-value 9.388, p = 0.001) and security awareness programs (ß = 0.690, t-value = 9.388, p = 0.001) have a significant influence on intention to comply. The effect of situation awareness, satisfaction and habit on intention to comply was not significant.

4.5.1 Summary of hypotheses (multiple linear regression)

A summary of supported or rejected hypotheses is shown in Table 7.

4.5.2 Final result (model)

The research model explained 59.6% of the variance in actual compliance and 77.2% of the variance in Intention to comply.

5 Discussion of findings

The results indicate that 60–70% of the sample respondents agree with actual compliance, 60–75% with intention to comply and 70–80% with attitude to comply. To increase the level of actual compliance, influence the intention and attitude to comply with information security policy, news of cyber-attack even outside the organisation should be shared with the employees to make them aware of severity and celerity for organisation.

This would stimulate employees' attitude. Once behaviour of users' influenced, intention to comply and actual compliance will follow. The findings underline the role of positive incentives on compliance. Rewards were found to exercise an important influence on employee's intention to comply, rewards system is not seen enough in organisation or may be the respondents were unaware of rewards system. It is very important for organisations take into consideration the role of positive incentives.

Organisations should inspire their employees to abide by information security policy. Organisations could show their employees that they trust them. Organisation could set weekly or monthly achievable goals and reward them accordingly. This would galvanise the employees.

Sanctions were found to not have an important influence on actual compliance. Most respondents do not believe that they will sanctioned for not complying with the security policies. It means that practitioners must mention the sanctions for not complying with information security. It is very important to make employees believe that their non-compliance with the security policies will be detected. Consequently severe and quick actions against them will take place.

Information security compliance will be raised by developing a security-aware culture in an organisation. Organisation should organise security awareness campaign and provide appropriate training. Two thirds of the respondents are aware of the security awareness and training campaign. Computer users should be involved in information security development to influence their attitude. Flores et al. (2014) advanced that shortage of information security awareness among staff can be explained by the low level of involvement in information security.

Half of the respondents do not believe that their computing activities at work are monitored. This could have negative impact on their intention to comply with information security policy. Organisations should use monitoring and auditing tools. Monitoring tools will deter unacceptable attitude of employees while ensure that breaches are brought to the attention of the organisations. This should be known to employees so that they adopt acceptable behaviour concerning information security. Studies have proven employees change their conduct once organisation take monitor their activities on information systems and their corporate network.

Guidance and help should be easily available from superior or IT security staff if employees encounter difficulties in understanding the policies. Organisation should strive to simplify the security procedures so that employees easily understand what is expected from them. Both the language used to write and terms used in the information security compliance policy should be easy to understand. Technical terms should be either avoided or explained clearly in the document. This is mainly to ensure that employees truly believe that they can carry out these security policies. Information security policy should be updated as and when required so that it is seen as relevant by employees.

While employees wish innocently to use applications or devices which they use at home they may be unaware of the serious consequence it could have for organisations. Severity of security breaches to the commercial activities of organisations is growing. So this should be emphasised to employees. Incidents related information security divulged should be brought the attention of employees and discussed in organisations so that they become aware of the danger and discern between home and work environment. The consequence of security breaches for organisations will be much greater than for individual at home. Organisations have legal obligations to protect data of its clients. Now more with the Data Protection Act 2017. Interruptions of services as a result of security breaches would be catastrophic for organisations. Most employees would not want their organisations to suffer such consequence as this would endanger the job. Employees are unaware of the importance of importance security at work.

As an unsatisfied employee could hold resentment towards his organisation and neglect information security to punish it, organisations should give employees' satisfaction its due importance. Employees should be treated fairly. Salary compensation would increase job satisfaction but only temporarily. Employees could be given more flexibility over their work schedule to have a better work-life balance. They should be given to the opportunity to create an enjoyable place of work so that they feel at ease with their job. Organisation could consider avoid giving their employees tight deadline. This would make employees satisfied with their job and less prone to error under stressing condition of work.

It is significant for organisation to make it a habit for theirs employees to comply with information security policies. Training sessions and meeting are good places to remind employees of adhering to the security policies. If employees understand the policy document easily, they will most probably take the habit of complying the policies. A visible reward system will motivate employees to take habit of complying in the long run.

6 Conclusions

Former studies advance that most employees do not comply with the information security policy frequently. To solve this issue many suggestions have been made in the extant literature. However, there is a major deficiency in the existing approaches. Academics say these approaches are short of theoretical and empirical proof on their efficacy in practice. It is of utmost significance that employees' compliance or non-compliance is studies using field research since practitioners require empirically validated information.

A survey was conducted to identify the major factors influencing the compliance of employees with information security policy. The theory of reasoned action, cognitive evaluation theory and GDT were added with other factors mentioned in the study of Alotaibi et al. (2016) and empirically tested the proposed model (N = 140). The results suggest that attitude, rewards and security awareness programs have important influence on intention to comply. Intention to comply, in turn, has an important impact on actual compliance. However, sanctions, computer monitoring, technology democracy and gender did not have a significant effect on actual compliance. Satisfaction, habit and situational awareness also did not have an important impact on Intention to comply.

References

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

Alotaibi, M., Furnell, S. and Clarke, N. (2016) 'Information security policies: a review of challenges and influencing factors', in *Internet Technology and Secured Transactions (ICITST), 2016 11th International Conference for*, IEEE, December, pp.352–358.

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.

Cavusoglu, H. and Raghunathan, S. (2004) 'Economics of IT security management: four improvements to current security practices', *Communications of the Association for Information Systems*, Vol. 14, No. 1, p.3.

Cavusoglu, H., Bulgurcu, B. and Benbasat, I. (2009) 'Roles of information security awareness and perceived fairness in information security policy compliance', *AMCIS 2009 Proceedings*, p.419.

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.

Dhillon, G. and Backhouse, J. (2001) 'Current directions in IS security research: towards socio-organizational perspectives', *Information Systems Journal*, Vol. 11, No. 2, pp.127–153.

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

Gefen, D. and Straub, D. (2005) 'A practical guide to factorial validity using PLS-Graph: tutorial and annotated example', *Communications of the Association for Information Systems*, Vol. 16, No. 1, p.5.

Hair, J.F., Anderson, R.E., Tatham, R.L. and Black, W.C. (1998) *Multivariate Data Analysis: With Readings*, 4th ed., Prentice Hall, Englewood Cliffs, New Jersey.

Hair, J.F., Black, W.C., Babin, B.J. and Anderson, R.E. (2010) *Multivariate Data Analysis*, p.7.

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

Herath, T. and Rao, H.R. (2009b) 'Protection motivation and deterrence: a framework for security policy compliance in organisations', *European Journal of Information Systems*, Vol. 18, No. 2, pp.106–125.

Hu, Q. and Dinev, T. (2005) 'Is spyware an internet-age nuisance or public menace?', *Communications of the ACM*, Vol. 48, No. 8, pp.61–66.

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012) 'Managing employee compliance with information security policies: the critical role of top management and organizational culture', *Decision Sciences*, Vol. 43, No. 4, pp.615–660.

Hu, Q., Hart, P. and Cooke, D. (2007) 'The role of external and internal influences on information systems security – a neo-institutional perspective', *The Journal of Strategic Information Systems*, Vol. 16, No. 2, pp.153–172.

Kritzinger, E. and Smith, E. (2008) 'Information security management: an information security retrieval and awareness model for industry', *Computers & Security*, Vol. 27, Nos. 5–6, pp.224–231.

Lebek, B., Uffen, J., Neumann, M., Hohler, B. and Breitner, M.H. (2014) 'Information security awareness and behavior: a theory-based literature review', *Management Research Review*, Vol. 37, No. 12, pp.1049–1092.

Limayem, M. and Hirt, S.G. (2003) 'Force of habit and information systems usage: theory and initial validation', *Journal of the Association for Information Systems*, Vol. 4, No. 1, p.3.

Mertler, C.A. and Reinhart, R.V. (2016) *Advanced and Multivariate Statistical Methods: Practical Application and Interpretation*, Routledge, New York.

Mishra, S. and Dhillon, G. (2006) 'Information systems security governance research: a behavioral perspective', in *1st Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference*, June, pp.27–35.

Mitnick, K.D. and Simon, W.L. (2003) *The Art of Deception: Controlling the Human Element of Security*, John Wiley & Sons, Indianapolis, Indiana.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T. and Vance, A. (2009) 'What levels of moral reasoning and values explain adherence to information security rules? An empirical study', *European Journal of Information Systems*, Vol. 18, No. 2, pp.126–139.

Nathans, L.L., Oswald, F.L. and Nimon, K. (2012) 'Interpreting multiple linear regression: a guidebook of variable importance', *Practical Assessment, Research & Evaluation*, Vol. 17, No. 9, pp.1–19.

Ng, B.Y., Kankanhalli, A. and Xu, Y.C. (2009) 'Studying users' computer security behavior: a health belief perspective', *Decision Support Systems*, Vol. 46, No. 4, pp.815–825.

Nunkoo, R. (2015) 'Tourism development and trust in local government', *Tourism Management*, Vol. 46, pp.623–634.

Nunkoo, R. and Gursoy, D. (2012) 'Residents' support for tourism: an identity perspective', *Annals of Tourism Research*, Vol. 39, No. 1, pp.243–268.

Pahnila, S., Siponen, M. and Mahmood, A. (2007) 'Employees' behavior towards is security policy compliance', *Proceedings of the 40th Annual Hawaii International Conference on System Sciences*, pp.156–166.

Pallant, J. (2010) *SPSS Survival Manual: A Step by Step Guide to Data Analysis using SPSS*, Maidenhead, London.

Posthumus, S. and Von Solms, R. (2004) 'A framework for the governance of information security', *Computers & Security*, Vol. 23, No. 8, pp.638–646.

Puhakainen, P. and Siponen, M. (2010) 'Improving employees' compliance through information systems security training: an action research study', *MIS Quarterly*, Vol. 34, No. 4, pp.757–778.

Puhakainen, P. (2006) *Design Theory for Information Security Awareness*, University of Oulu. Finland.

Siponen, M. (2000) 'A conceptual foundation for organizational information security awareness', *Information Management and Computer Security*, Vol. 8, No. 1, pp.31–41.

Siponen, M. and Vance, A. (2010) 'Neutralization: new insights into the problem of employee information systems security policy violations', *MIS Quarterly*, Vol. 34, No. 3, pp.487–502.

Siponen, M. and Willison, R. (2009) 'Information security management standards: problems and solutions', *Information & Management*, Vol. 46, No. 5, pp.267–270.

Siponen, M., Mahmood, A. and Pahnila, S. (2009) 'Are employees putting your company at risk by not following information security policies?', *Communications of the ACM*, Vol. 52, No. 12, pp.145–147.

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

Siponen, M., Pahnila, S. and Mahmood, A. (2007) 'Employees' adherence to information security policies: an empirical study', in *IFIP International Information Security Conference* Springer, Boston, MA, May, pp.133–144.

Siponen, M., Pahnila, S. and Mahmood, A. (2010) 'Compliance with information security policies: an empirical investigation', *Computer*, Vol. 43, No. 2, pp.64–71.

Siponen, M.T. (2005) 'Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods', *Information and Organization*, Vol. 15, No. 4, pp.339–375.

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

Straub, D., Boudreau, M.C. and Gefen, D. (2004) 'Validation guidelines for IS positivist research', *Communications of the Association for Information Systems*, Vol. 13, No. 1, p.24.

Straub, D.W. and Welke, R.J. (1998) 'Coping with systems risk: security planning models for management decision making', *MIS Quarterly*, pp.441–469.

von Solms, B. and von Solms, R. (2004) 'The 10 deadly sins of information security management', *Computers & Security*, Vol. 23, No. 5, pp.371–376.

Vroom, C. and Von Solms, R. (2004) 'Towards information security behavioural compliance', *Computers & Security*, Vol. 23, No. 3, pp.191–198.