View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by The International Islamic University Malaysia Repository

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 72 (2015) 361 – 373

Procedia Computer Science

The Third Information Systems International Conference

Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures

Abdul Rahman Ahlan [a], Muharman Lubis [a]*, Arif Ridho Lubis [b]

[a]*International Islamic University Malaysia, Jalan Gombak, 50728 Kuala Lumpur, Malaysia*
[b]*Politeknik Negeri Medan, Jalan Almamater No. 1, Kampus USU, 20155, Medan, Indonesia*

Abstract

Information security awareness (ISA) is referred to as a state of consciousness where user ideally committed to the rules, recognize the potentiality, understand the importance of responsibilities and act accordingly. Despite the number of case occurred in information security breaches, especially at knowledge-based institution result from the reluctance of user's failure to comply with security guidelines, such effective measure should take place to anticipate the negative effect. Therefore, more attention is required to understand the roles of individual, institutional and environmental antecedent for optimization in raising the information security awareness. This paper elucidated the roles of its antecedent and measure in influencing ISA of user using survey method that contributes for better understanding by analyzing user perception. From the result, this study identified several important factor impacts to the awareness and its relationship to other factor such as religious indicator can influence peer performance but also social pressure. Thus higher education can focus the policy for encouraging them to have proper response from student and staff in avoiding security incident.

© 2015 Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).
Peer-review under responsibility of organizing committee of Information Systems International Conference (ISICO2015)

Keywords: Awareness; Antecedent; Measure; Information Security; Perception

1. Introduction

Information Security (IS) incidents eventually are still occurring despite the security procedure that is designed by many organizations refer to specific guideline to counter the negative effect, at least to avoid loss. In the end, the organization often struggle from the after effect of an incident which may cause severe damage to the reputation and finances, even it has the potentiality to harm the state of emotion from its staff and customer. Therefore, a series of solution offered by some researchers for this problem to

* Corresponding author. Tel.: +6017-3303-514
E-mail address: muharman.lubis@gmail.com

1877-0509 © 2015 Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).
Peer-review under responsibility of organizing committee of Information Systems International Conference (ISICO2015)
doi:10.1016/j.procs.2015.12.151

provide certain degree of assurance of the expected results by developing incorporated policy for training program, campaigning and reward system [1][2][3][4]. However, assessing the effectiveness of information security policy and procedure conducted with the workforce is difficult, at certain aspect is complicated. Meanwhile, organizations also have doubt the return on investment of formal security awareness strategy entangled with training, campaigning and reward system [5]. Formal security awareness training may improve the ethical and unethical perceptions of users concerning information technology but as these perceptions are often blurred, the effectiveness of their practice is difficult to monitor. In knowledge-based institution that involved intangible asset to favor specialization, research, innovation and learning, the indicators for evaluation to determine the security awareness strategy meet with expectation become more difficult. But, the effectiveness of these attempts to raise security awareness is questionable, as most employees do not fully comply with organizational security policies and procedure while the organization at certain aspect unwilling to put security awareness strategy in practice properly [6]. Likewise, users often practice unsafe computing behaviors, although it is not with the intention of causing harm. In one study, 49% of the research participants occasionally engaged in risky behavior and 28% did so frequently [7]. Meanwhile, according to a quantitative survey of 435 higher education institutions in the US, only 39% of the examined institutions had applied IS security awareness program, whereas 75% of them view IS security as one of the top three issue confronting the institution activities contradictory [8].

Another study [9] suggest that both the narcissistic individual and organization develop the identities that are reflected in their policies, procedures, behaviors, values, and beliefs, lead to have certain impacts on the intentions and actions of the employees. These individuals and organizations tend to be self-absorbed, feel self-important, are obsessed with success and power, lack empathy and exploit others. Based on the analysis of the extant literature [6][10][11], it is evident that existing theoretical developments have been effective in defining the factors that enhance compliance or prevent system abuse. Nevertheless, one of the major limitations of the research thus far is that it addresses the research problem only from an organizational perspective but it has lack in considering the users' perspective. To explain this phenomenon, a study [10] examined the uncertainty college students have concerning what constitutes ethical and unethical behavior using corporate information systems. The results are consistent with expectations for the most part; the students identified most unethical situations correctly. However, they had problems identifying misuse of corporate information technology assets even when proper polices are in place. As a result, the security policy should be aligned with the readiness of user state of perception and emotion, as well as observed the user environment. This study is the continuation of research on implication of roles responsibility in ISA that has technical error and data changes in collection stage [16]. However, this study have objective to improve previous findings by using new data collection in Indonesia let alone Malaysia based on prior experience. This study has purpose to develop new model based on current model to emphasize the importance of individual, institutional and environmental antecedent so it will contribute to explain further the relationship between antecedent and measures for developing information security awareness especially in knowledge based institution.

2. Hypotheses Development

The following hypotheses were formed based on relevant theories in the literature review, which are TPB and TRA [14][15][19], Triparte Model [17][18][20] and Relationship Awareness [21][22][23] to examine the relationship of towards information security awareness. These hypotheses are derived from understanding the previous study to implement new developed model with the purpose to establish multi-level ISA theory model of awareness that focus on three antecedents consist of individual: Self Attitude (AT), Self Behavior (BV) and Self Cognitive (CT), institutional: Policy Compliance (PC) and Training Program (TP) and environmental: Peer Performance (PP) and Social Pressure (SP) connected directly but

separately to three measures are intention to comply (IC), perceived threat (RT) and religious indicator (RI) respectively that have positive impact towards information security awareness in higher education process of teaching and learning.

2.1. Individual Antecedents

Commonly, attitudes can be changed through persuasion as a response to communication [24]. Theoretically, a positive attitude towards a behavioral change can be achieved if the driving forces are greater than the resisting forces and vice versa [25]. For example, if an employee starts showing a positive attitude towards various issues in information security, then that employee could be initially rewarded. Next time, only when that employee shows more than a positive attitude and starts showing a part of the desired behavior, then the employee is rewarded again and again. Meanwhile, Skinner [26] points out that even though it might be unlikely to demonstrate that a displayed behavior could be the result of the stimulating environment as a whole, he asserts that it is possible to induce part of the displayed behavior according to certain laws. From empirical evidence shows the positive impact of security policy compliant behavior of peers on the security behavior of others [27]. It has also been shown that direct supervisory security practices and direct co-workers socialization, including conversations and observing the behavior of co-workers increase an employee's attention for organizational policy, which in turn positively affects security compliant behavior [11]. Moreover, if co-workers disapprove of policy violations employees are found to be less likely to do so [20]. Also in the private context it could be empirically proven that family members and peers significantly affect users' intention to behave responsible with regard to computer security [28]. Thus, there is strong evidence that peers affect employees' security behavior. However, we argue that interactions with peers initiate knowledge transfers [29] and consequently increase security strategy-related knowledge.

Cognitive perspectives focus on both trainee knowledge and the processes of knowledge acquisition, organization, and application [30]. All individuals must be trained on how to handle information carefully according to the guidelines and must be trained to become aware of the possible consequences of their actions [31]. Lubinski and Humphreys [32] noted a neglected aspect does not cease to operate because it is neglected and there is no good reason for ignoring the possibility that general intelligence or various more specific cognitive abilities are important causal determinants of decision-making. As reviewed in literature above, intention to comply was strongly related to actual compliance behavior and it is sufficient in predicting behavior because if one's intention to comply is high, that person will comply [6][11]. Meanwhile, Bulgurcu et al [33] found that the effect of attitude on an employee's intention to comply, explaining 23% of the variance in intentions in both individual and organizational model of compliance.

H1. User with a more positive self-attitude towards following security precautions has positive impact towards information security awareness.

H2. User with a more positive self-behavior towards following security precautions has positive impact towards information security awareness.

H3. User with a more positive self-cognitive towards following security precautions has positive impact towards information security awareness.

H4. User with a more positive intention to comply with security mandatory has positive effect towards individual antecedent of information security awareness.

2.2. Institutional Antecedents

The development of corporate information security policies (ISPs) is a primary resource of ISS management practices [11]. An ISP can be broadly defined as statements by an organization providing

guidance about ISS related responsibilities, rules, and guidelines which prescribe how the IS resources are used properly and in a secure way [35]. Meanwhile, prior research offers contradicting results with regard to the effect of ISPs (Information Security Policies) found that the existence of corporate ISPs to be effective for preventing IS misuse behavior and ascribe this effect to deterrence mechanisms, Lee et al. [35] found that ISPs had no influence on IS misuse behavior. Literature argues that the inconsistent results are due to employees' lack of awareness of security policies [36][37]. Meanwhile, Marks and Rezqui [1] suggested training and campaign as the best methods to increase understanding about ISA accommodates the uniqueness of specific location and durable of time. The establishment of training also be encouraged to ensure that users are informed and can be accounted liable for IS misconduct. One way to make people become security-conscious is through security awareness training by removing vulnerabilities associated with human behavior [38]. If the workforce has a clearer concept of the damage the organization might sustain in the event of an information security compromise, there should be an improvement in their attitudes toward following policies [19].

Since people represent one of the biggest threats for the business information, the less trusted people involved in security decisions, the better, because the more trusted people is involved in security decisions, the more weak the system becomes [39]. According to the Information Security Breaches survey [12] almost two thirds of the respondents reported that the worst security incident had an internal cause particularly staff misuse of information systems (47%) in large business. These results are consistent with what is observed in other surveys. For example, according to the CSI survey [13] the top three types of attacks detected in 2007 were insider abuse of Net access (59%) and Virus (52%) and Laptop/Mobile device theft (50%). Perceived severity of the threats to the information system had no role in intended behavior of the information system users. Thus, perceived threat is not viewed as risk that involves both the vulnerability and amount of damage the attack could incur but one dimension ally only in terms of likelihood of an attack [19].

H5. User who perceived policy compliance positively in institution has positive influence towards information security awareness.

H6. User who perceived training program positively in institution has positive influence towards information security awareness.

H7. User who perceived a security threats higher towards security system has positive effect to institutional antecedent within ISA.

2.3. Environmental Antecedents

Researchers have called for the creation of policy to help organizations to influence employee performance in order to better protect organizational information [40]. It is also important that the message and materials of IS training are the same regardless of who the trainer is [41] as well as regularly and continuity to increase the awareness in security performance. Unfortunately, performance is recognized as a major problem in the implementation of information security practices in institution. The engagement of IT knowledge-based institution such as library, human resource or IT division together will strengthen the goals of ISA initiative with detailed responsibilities and plan to obtain the target in developing ISP. However, ISP cannot guarantee a recipe for correct decisions but it provides an integrated perspective on goals, targets, and measures of progress. Therefore, the evaluation from feedback and learning experience is required to measure the performance for the future function such as revise the plan and develop credible measure [16].

Social environment can influences the shape of person practices, judgment, opinion and belief, whereby it occurs when individual's opinion and action that was affected by other people [42]. It is commonly believed that the close proximity peers, such as friends and friends of friends, have social influence on the joining of a certain group of that node, the effect can also be the other way around, when

people get to know others by virtue of their common interests and memberships in the same groups. The final outcome of an idea of social influence in a group of actors is the result of the interpersonal influences between these actors and also actors' susceptibilities to interpersonal influence. Meanwhile, in the context of social network, a qualitative study [43] found that there is strong direct social pressure to join online among American teenagers in addition to their own feeling of being left out if they do not join. Recently, Murray [44] conducted a quantitative study, which was carried out by online survey to investigate the practices and perceptions of students in a Catholic high school about using Internet, it was found that 8 out of 10 aware that information posted online might have an negative effect on their future. Meanwhile, other researcher established an inverse relationship between church attendance and Internet pornography use with persons associated with greater levels of religiosity were found less involved with behavior regarding to sexual addiction [45][46].

H8. User who has a greater peer performance in environment has greater information security awareness.

H9. User who has a greater social pressure in environment has greater information security awareness.

H10. User who has a greater religious indicator in environment has positive effect to environmental antecedent of ISA.

3. Analysis & Result

3.1. Instrument

This study will use quantitative methodology, which was survey questionnaire through manual approach as the data collection method by distribution a question paper to student, staff and lecturer with 5 demographic question related to the position, marriage status, age, races and gender with 103 people from Harapan University and North Sumatera University in Medan. Previously, pre-test towards 2 experts has been conducted to evaluate the quality of questionnaire form in term of clarity and simplicity of message. The questionnaire has been divided into 3 categories consist of individual, institutional and environmental context. For individual context has 14 questions, institutional context has 13 questions and environmental context has 12 questions that focused on their antecedent and measure model. It has used Indonesian language to make ease conveying the message for the question statement and 5-likert scales with ticking box for answer method. The question statement (*appendix A*) in each construct from this survey questionnaire was designed by referring to previous work [27][47]. The survey results were generated analyzed using smartPLS v2 [49] for the hypothesis model testing and examined for validity and reliability.

3.2. Measurement Model Result

Using a two tailed test with significant level of 5%, the path coefficient will be significant if the t-value is larger than 1.96. From the list of indicator from all constructs (table 2), they are total 13 out of 39 with three constructs (PC, RI & IS) have all of three highly significant indicator of outer loadings. Therefore, as the standard of significance p-value that above 0.10 as non-significant (NS) while below 0.10 as weak (*) and then below 0.05 as medium (**) and below 0.01 as strong (***). From the result (*appendix B)*, it listed 9 out of 39 indicators that have non-significant (label 'NS') relationship with the constructs reflectively. Meanwhile, 19 reflective indicators have strong significant influence to their construct as well as 3 weak and 8 medium significant indicators respectively. To find the indicator of reliability value through checking square each of the outer loadings which preferable value more or equal to 0.7, therefore if it is an exploratory research, 0.4 or higher is acceptable [50]. From the result, there are 7 outer loading values that have not met the standard, which has lower value consist of BV3 (0.152), CT1 (0.064), IC1 (-0.052), IC3 (0.222), PP4 (0.200), SP2 (0.234) and SP5 (0.380).

3.3. Structured Model Result

The result (*appendix C*) shows that the interrelationship of AT to IS has non-significant value (p=0.2773), so the other two individual antecedent those are BV (p=0.2343) and CT (p=0.195) with table value of 1.96 (95% CI) and degree of freedom > 100. Likewise, they posits the indication that individual antecedent has direct insignificant on Information Security Awareness. Manually, t value can be calculated with path coefficient divided by the standard errors. Based on t value, AT changes in direct proportion to IS with coefficient of 0.1282, which indicates that a 100 points change in AT will bring 12.82 changes in IS positively. In contrast, BV has coefficient of -0.1285, which indicates that a 100 points changes in BV will bring 0 points changes in IS as it have no impact at all due to negative value. Besides that, SP also has negative direction with coefficient of -0.089 and p value of 0.49 that clearly indicated insignificant relationship as well as has no impact to point changes in IS. On the other hand, last construct in individual antecedent CT has coefficient of 0.1761 has the indication that a 100 points change in CT will be bring 17.61 changes in IS positively. As shown in table 2, four constructs relationship has a strong significant influence wherein RI has p value of 0.004 to PP and 0.0006 to SP. Further, PP and TP also has a strong significant influence to IS with p value 0.012 and 0.001 respectively. Only two constructs relationship has weak significant influence, which are IC to BV with p value of 0.05 and RT to PC with p value of 0.08 while IC to AT has medium significant influence with p value of 0.049.

3.4. Validity and Reliability

The coefficient of determination (R^2) is 0.3795 for the IS endogenous latent variable meant that the antecedent (individual, institutional and environmental) slightly explain 37.95% of the variance in IS. The discriminate validity is adequate when constructs have an AVE loading greater than 0.5 meaning that at least 50% of measurement variance was captured by the construct, while for composite reliability should be 0.7 or higher, while in exploratory research 0.6 or higher is acceptable [51]. On the other hand, to establish discriminant validity, Fornell and Larcker [52] suggest the square root of AVE in each latent variable should be higher than other correlation values among the latent variable. From the result (*appendix E)*, it listed that all the square root of AVE construct has larger value than those in row and column of correlation values with RI (0.772) has highest number above all, while IC (0.507) became the lowest. It means that the table result indicates that discriminant validity is well established. For the effect size of each construct IS is the large impact with r more than 0.5 while SP and AT are medium impact with r more than 0.3. Meanwhile, goodness of fit has been developed as an overall measure of model fit for PLS-SEM, but it cannot reliably distinguish valid from invalid models and since its applicability is limited to certain model setup, researcher should avoid its use [53].

3.5. Research Hypothesis

From the result, surprisingly, individual antecedent does not appear to be a valid reflective construct in this research and was found insignificant contributor to the latent variable information security awareness (IS). Meanwhile, the other antecedent relationships of exogenous construct to IS variable partially consistent with Haeussinger and Kranz [47] work, even though policy compliance (PC) and social pressure (SP) have non-significant relationship with IS but training program (TP) and peer performance (PP) have strong significant relationship. Despite the non-significant individual antecedent on IS, intention to comply as a measure has medium significant influence with self-attitude (AT) and weak significant influence to behavior (BV) but not with self-cognitive (CT).

H1. The effect of AT on IS has path coefficient 0.13 (p=0.28), 95% CI [0.36, -0.1] which does not significant but positively influence so null hypotheses 1 can be rejected.

H2. The effect of BV on IS has path coefficient -0.13 (p=0.23), 95% CI [0.08, -0.34] which does not significant but negatively influence so it failed to reject null hypotheses 2.

H3. The effect of CT on IS has path coefficient 0.18 (p=0.19), 95% CI [0.44, -0.08] which does not significant but positively influence so null hypotheses 3 can be rejected.

H4. The effect of IC on individual antecedents has path coefficient for AT 0.42 (p=0.04), 95% CI (0.83, 0.006) which does significant positively in moderate level, while for BV 0.37 (p=0.05), 95% CI (0.74, -0.007) also does significant positively but in weak level and for CT 0.09 (p=0.7), 95% CI (0.57, -0.39) does not significant but positively influence so null hypotheses 4 can be rejected.

H5. The effect of PC on IS has path coefficient 0.03 (p=0.77), 95% CI [0.29, -0.21] which does not significant but positively influence so null hypotheses 5 can be rejected.

H6. The effect of TP on IS has path coefficient 0.35 (p=0.001), 95% CI (0.51, 0.06] which does significant positively in very strong level so null hypotheses 6 can be rejected.

H7. The effect of RT on institutional antecedents has path coefficient for PC 0.3 (p=0.08), 95% CI (0.64, -0.04) which does significant positively in weak level while for TP 0.22 (p=0.17), 95% CI (0.53, -0.09) does not significant but positively influence so null hypotheses 7 can be rejected.

H8. The effect of PP on IS has path coefficient 0.29 (p=0.01), 95% CI (0.51, 0.06] which does significant positively in strong level so null hypotheses 8 can be rejected.

H9. The effect of SP on IS has path coefficient -0.09 (p=0.49), 95% CI (0.16, -0.34) which does not significant but negatively influence so it failed to reject null hypotheses 9.

H10. The effect of RI on environmental antecedent has path coefficient for PP 0.31 (p=0.004), 95% CI (0.51, 0.07) which does significant positively in very strong level while for SP 0.43 (p=0.0006), 95% CI (0.66, 0.19) also does significant positively in very strong level so null hypotheses 10 can be rejected.

4. Conclusion

This study investigates the possibility of the incorporation of individual, institutional and environmental as reflective construct that connect to information security awareness. To shape the human perception to meet the goal and expectation to have good quality of security state that have principle of transferability and readability; set of strategy should be developed and preferable environment should be prepared. Importantly by understanding the human factor within the framework, their perceptions of and motives for compliance in management of information security can help the user to know the type of preventative actions taken and reduce the number of security related incidents. The intention of having security policy was not to persuade users but to convince them, by letting the users reflect, on their own terms, on why information security is important and on how to react in certain circumstances. Emphasizing the role and responsibility the individual user has in information security should personalize information security awareness and encourage personal ownership the information systems integrity and security and increase overall vigilance [19]. Interestingly, the religious indicator and training program factor based on user perspective play important role to increase ISA in higher education.

Appendix A. Survey List Simple Translated Questions in English

Self Attitude (AT)	Self Behavior (BV)	Self Cognitive (CT)
1. Personal data can be used for personal interest. 2. It is common to see somebody's personal data. 3. Prefer to use pirated software. 4. Feel safe with no antivirus.	1. Often access email from Internet cafes. 2. Prefer to learn based on experience than textbooks. 3. Regularly check document for anticipating virus infection.	1. Often ask for friend's advice on computer problem. 2. Glad to read Internet article on privacy protection. 3. Technology advancement has double edge sword.
Intention to Comply (IC)	**Policy Compliance (PC)**	**Training Program (TP)**
1. It does not matter to violate the IS rule as long as no impact at all. 2. Still obey the IS rule though limited access to certain website. 3. Trust to management campus to protect personal data. 4. Intent to fulfill campus role of responsibility.	1. It is easy to understand general written IS rule of campus. 2. Quick access for related privacy protection. 3. It is necessary to arrange campus IS rule refer to corporation standard.	1. No possibility of occurrence on leaking answered-key in campus. 2. Campus gave counseling on regular basis for IS issues. 3. It is necessary for campus teach the related IT regulation. 4. Campus has explained the consequences of violation.
Perceived Threats (RT)	**Inf. Security Awareness (IS)**	**Peer Performance (PP)**
1. Motivation got through the awareness on the danger of negligence. 2. Current system susceptible from external/internal attack. 3. Inf. system damage can disrupt teaching learning activities.	1. Concern for the impact will be borne for incident. 2. Potential damage to information system by hacker threats. 3. Student role for escalate information security.	1. Every user in campus network will obey the rule. 2. Every related party has work in maximum capacity. 3. Campus accommodated the importance of data protection. 4. Campus should evaluate the performance of staff and student periodically.
Social Pressure (SP)		**Religious Indicator (RI)**
1. Student can satisfy the planned target in general. 2. Mostly staffs often face the affected situation. 3. It is common to share password with wife or close friend. 4. Some of students have difficulty to focus due to workload. 5. It will severe penalties for the one who violate the IS rule.		1. Campus provides good facilities for praying. 2. Campus often promotes the religious program. 3. Religious organization gives positive impact to my productivity.

Appendix B. Outer Model Statistic Result

Reflective Constructs	Reflective Indicators	Outer Loadings	t Value	p Value	95% CI Upper ---------- Lower		Sig. Level
AT	AT1	0.455526	1.592959	0.114263714	0.77874288	-0.14785888	*
	AT2	0.436517	1.386368	0.16865753	0.78445368	-0.32297768	NS
	AT3	0.728783	2.035233	0.044420948	1.0940072	-0.0680572	**
	AT4	0.731272	2.700343	0.008111181	0.9631092	0.0809328	***
BV	BV1	0.600884	1.300338	0.19641563	1.35878704	-0.24919304	NS
	BV2	0.834516	2.107779	0.037501069	1.52512104	0.02023696	**
	BV3	0.151971	0.351456	0.72597124	0.87622484	-0.58908684	NS
CT	CT1	0.064243	0.144742	0.885200193	0.60464372	-1.07549572	NS
	CT2	0.852737	3.278983	0.001425574	1.34533696	0.26233504	***
	CT3	0.618599	2.243332	0.02703768	1.06983848	-0.00399848	**
IC	IC1	-0.051846	0.129162	0.897483814	0.57427684	-0.63750884	NS
	IC2	0.879570	2.241597	0.027153513	1.56107788	0.16378212	**
	IC3	0.222051	0.554663	0.580339405	0.73502636	-0.49866036	NS
	IC4	0.448327	1.104846	0.271825724	1.16096676	-0.20831276	NS
PC	PC1	0.811580	5.757699	9.04727E-08	0.94739024	0.41262776	***
	PC2	0.543678	2.097006	0.038465828	0.63527056	-0.38083656	**
	PC3	0.684765	4.298541	3.94E-05	0.88858268	0.21823132	***
TP	TP1	0.459110	1.683819	0.095274724	0.78872108	-0.07465108	*
	TP2	0.718538	6.357055	5.85903E-09	0.54656896	0.10556504	***
	TP3	0.631879	3.743173	0.000300795	0.75677344	0.13157656	***
	TP4	0.646837	4.334185	3.43773E-05	0.79675444	0.19615556	***
RT	RT1	0.757862	2.570634	0.011594961	1.26415456	0.06635544	***
	RT2	0.513764	1.379940	0.170622416	1.08357532	-0.21391332	NS
	RT3	0.622264	2.283503	0.024474156	1.01149496	-0.13589296	**
PP	PP1	0.778243	10.209661	2.7967E-17	0.52457648	0.24012952	***
	PP2	0.847155	12.715224	9.20708E-23	0.57368584	0.25566016	***
	PP3	0.755333	9.662183	4.5573E-16	0.64451444	0.26990356	***
	PP4	0.200913	0.948089	0.345324977	0.3455216	-0.2877936	**
SP	SP1	0.840398	4.339328	3.37056E-05	1.10692868	0.32985532	***
	SP2	0.233697	0.822335	0.412804493	0.54858636	-0.35376236	NS
	SP3	0.558599	2.692955	0.008280664	0.61902708	0.03230892	***
	SP4	0.430839	2.006186	0.047483731	0.52627544	-0.10617344	**
	SP5	0.379836	1.625620	0.10711643	0.61397016	-0.08171616	*
RI	RI1	0.720455	7.352038	5.02403E-11	0.49822176	0.16274424	***
	RI2	0.730646	5.443917	3.60955E-07	0.54237	0.130966	***
	RI3	0.856920	13.228158	7.36731E-24	0.83300092	0.37111908	***
IS	IS1	0.735951	8.029586	1.76233E-12	0.6827336	0.3313644	***
	IS2	0.723662	9.526822	9.08382E-16	0.57293532	0.21369868	***
	IS3	0.707737	4.086460	8.74262E-05	0.7485694	0.2186246	***

Appendix C. Inner Model Statistic Result

	Path Coefficients	STERR	t-Value	p-Value	95% CI Upper	95% CI Lower	Sig. Value
AT -> IS	0.128247	0.117423	1.092183	0.277325663	0.35839608	-0.10190208	NS
BV -> IS	-0.128501	0.107426	1.196185	0.234397583	0.08205396	-0.33905596	NS
CT -> IS	0.176177	0.135066	1.30438	0.195039664	0.44090636	-0.08855236	NS
IC -> AT	0.420396	0.21129	1.989665	0.049304827	0.8345244	0.0062676	**
IC -> BV	0.366122	0.190749	1.919398	0.057728435	0.73999004	-0.00774604	*
IC -> CT	0.094141	0.244454	0.385105	0.700961497	0.57327084	-0.38498884	NS
PC -> IS	0.037462	0.130288	0.28753	0.774289892	0.29282648	-0.21790248	NS
PP -> IS	0.289408	0.114155	2.535225	0.012755833	0.5131518	0.0656642	***
RI -> PP	0.307751	0.105433	2.918938	0.004322165	0.51439968	0.10110232	***
RI -> SP	0.426002	0.120978	3.521333	0.000643608	0.66311888	0.18888512	***
RT -> PC	0.301605	0.173305	1.740313	0.08481997	0.6412828	-0.0380728	*
RT -> TP	0.218918	0.158596	1.380347	0.170497492	0.52976616	-0.09193016	NS
SP -> IS	-0.088912	0.128261	0.693212	0.489751997	0.16247956	-0.34030356	NS
TP -> IS	0.352047	0.110266	3.19269	0.001874656	0.56816836	0.13592564	***

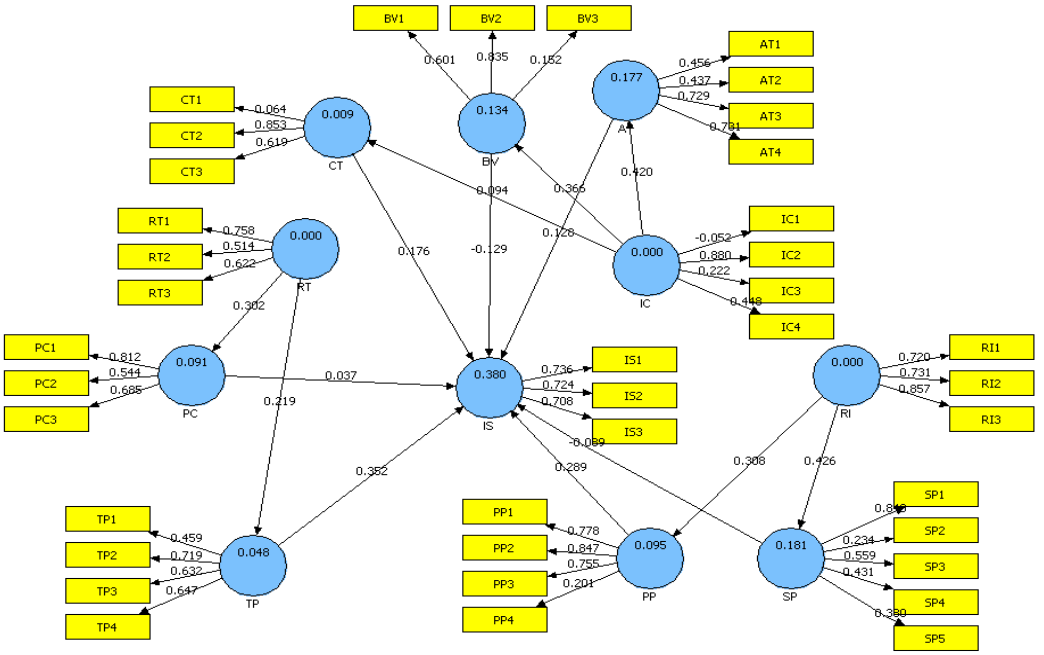
Appendix D. Latent Variable Quality Overview

	AVE	Composite Reliability	R Square	Cronbachs Alpha	Communality	Redundancy	LV Index Values
AT	0.365984	0.685680	0.176733	0.429731	0.365984	0.064225	3.001355
BV	0.360191	0.567616	0.134046	0.055685	0.360191	0.048274	2.494827
CT	0.371317	0.555602	0.008862	0.448860	0.371316	0.004551	1.942310
IC	0.256659	0.430136		0.163739	0.256659		2.852153
PC	0.474384	0.725218	0.090965	0.524019	0.474383	0.031333	2.057432
TP	0.386187	0.710772	0.047925	0.461790	0.386187	0.021625	2.008342
RT	0.408507	0.669021		0.285197	0.408507		2.248250
PP	0.483557	0.763389	0.094711	0.623081	0.483557	0.046950	1.919067
SP	0.280563	0.624010	0.181478	0.427251	0.280563	0.046333	1.904642
RI	0.595737	0.814551		0.681701	0.595737		2.292448
IS	0.522019	0.766113	0.379518	0.546216	0.522019	0.020148	2.038300

Appendix E. Discriminant Validity

	AT	BV	CT	IC	PC	TP	RT	PP	SP	RI	IS
AT	**0.605**										
BV	0.216	**0.600**									
CT	0.189	-0.051	**0.609**								
IC	0.420	0.366	0.094	**0.507**							
PC	0.223	-0.048	0.347	0.090	**0.689**						
TP	0.051	0.088	0.246	-0.059	0.316	**0.621**					
RT	0.112	0.129	0.214	0.213	0.417	0.420	**0.639**				
PP	0.099	0.105	0.136	0.159	0.284	0.182	0.308	**0.695**			
SP	0.007	-0.108	0.187	-0.109	0.210	0.302	0.265	0.144	**0.530**		
RI	0.350	0.160	0.182	0.213	0.181	0.044	0.267	0.426	-0.004	**0.772**	
IS	0.245	0.100	0.243	0.112	0.475	0.348	0.284	0.290	0.219	0.381	**0.723**

Appendix F. Research Model Result



References

[1] Mark A, Rezgui YA. Comparative study of information security awareness in higher education based on the concept of design theorizing. *International Conference on Management and Service Science (MASS)* 2009; 1-7.

[2] Furnell S, Sanders PW, Warren MJ, Addressing IS security training and awareness within the European healthcare community. *Studies in health technology and informatics* 1997; **43**: 707-711.

[3] Pahnila S, Siponen M & Mahmood A. Employees' behavior towards IS security policy compliance. *International Conference on System Sciences 2007*; 156-166.

[4] Pihakainen PA. *Design theory for information security awareness*. Doctoral Disertation. Faculty of Science, Department of Information Processing Science, University of Oulu; 2006.

[5] Schultz E. Security training and awareness – fitting a square peg in a round hole. Computers & Security 2004; **23**: 1–2.

[6] Siponen M, Mahmood MA, Pahnila S. Are employees putting your company at risk by not following information security policies? *Communications of the ACM* 2009; **52**: 145–147.

[7] Aytes K, Connolly T. Computer security and risky computing practices: A rational choice perspective. *Journal of Organizational and End User Computing* 2004; **16**: 22–40.

[8] Updegrove D, Gordon W. Computers and Network Security in Higher Education. *EDUCAUSE* 2003.

[9] Duchon D, Burns M. Organizational narcissism. *Organizational Dynamics* 2008; **37**: 354–364.

[10] Calluzzo VJ, Cante CJ. Ethics in information technology and software use. *Journal of Business Ethics* 2004; **51**: 301–312.

[11] Chan M, Woon I, Kankanhalli A. Perceptions of information security at the workplace: linking information security climate to compliant behavior. *Journal of Information Privacy and Security* 2005; **1**(3): 18-41.

[12] Price Water House Coopers. *2008 Information Security Breaches Survey*. Department for Business, Enterprise & Regulatory Reform, Technical Report. United Kingdom,.

[13] Computer Security Institute. CSI Survey 2007. *The 12th Annual Computer Crime and Security Survey* 2008. United States of

America.

[14] Ajzen I. The theory of planned behavior. *Organizational Behavior and Human Decision Processes* 1991; **50**: 179-211.

[15] Fishbein M, Ajzen I. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Massachusetts: Addison-Wesley; 1975.

[16] Ahlan Abd. Rahman & Lubis M. Information Security Awareness in University: Maintaining Learnability, Performance and Adaptability through Roles of Responsibility. IEEE 7th International Conference on Information Assurance and Security (IAS) 2011; 246-250.

[17] Rosenberg MJ, Hovland CI. Cognitive, Affective and Behavioral Components of Attitudes. In Rosenberg MJ, Hovland CI, editor. *Attitude Organization and Change: An Analysis of Consistency Among Attitude Components*. New Haven: Yale University Press; 1960.

[18] Petty RE, Fazio, RH, Briñol P. *Attitudes: Insights from the new implicit measures*. New York: Psychology Press; 2009

[19] Cox J. Information systems user security: A structured model of the knowing gap. *Computer in Human Behavior* 2012; **28**: 1849-1858.

[20] Siponen M, Vance A. Neutralization: New insight into the problem of employee information systems security policy violations. *MIS Quarterly* 2010; **34**(3): 487-502.

[21] Porter EH. *Relationship Awareness Theory. Manual of Administration and Interpretation*. CA: Personal Strengths Publishing, Inc: Carlsbad; 1973.

[22] Duval TS, Wicklund RA. Effects of objective self-awareness on attributions of causality. *Journal of Experimental Social Psychology* 1973; **9**: 17-31.

[23] Silvia PJ, Duval TS. Objective self-awareness theory: Recent progress and enduring problems. *Personality and Social Psychology Review* 2001*;* **5**: 230-241.

[24] Micki K, Harold FT. *Handbook of Information Security Management*. CRC Press LLC; 2007.

[25] Corona CO. *Information security awareness: an innovation approach*. Research Thesis. Royal Holloway, University of London; 2009.

[26] Skinner BF. *The Behaviour of Organisms: An Experimental Analysis*. Prentice- Hall; 1938.

[27] Herath T, Rao HR. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems* 2009; **47**(2): 1-12.

[28] Ng BY, Rahim MA. A socio-behavioral study of home computer users' intention to practice security. *9th Pacific Asia Conference on Information Systems* 2005.

[29] Spears J. The effects of user participation in identifying information security risk in business processes. *ACM SIGMIS CPR* 2006; 351-352.

[30] Kraiger K, Ford JK, Salas E. Application of Cognitive, Skill-Based and Affective Theories of Learning Outcomes to New Methods of Training Evaluation. *Journal of Applied Psychology* 1993; **78**(2): 311-328.

[31] Wipawayangkool K. Security Awareness and Security Training: An Attitudinal Perspective. *SWDSI* 2009; 266-273.

[32] Lubinski D, Lloyd H. Incorporating General Intelligence into Epidemiology and the Social Sciences. *Intelligence* 1997; **24**(1): 159–201.

[33] Bulgurcu B, Cavusoglu H, Benbasat I. Effects of Individual and Organization Based Belief and the Moderating Role of Work Experience on Insiders' Good Security Behavior. *IEEE International Conference on Computational Science and Engineering* 2009.

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

[35] Lee SM, Lee SG, Yoo S. An integrative model of computer abuse based on social control and general deterrence theories. *Information Management* 2004; **41**(6): 707-718.

[36] Thomson ME, von Solms R. Information security awareness: Educating your users effectively. *Information Management and Computer Security* 1998; **6**(4): 167-173.

[37] Siponen M. A conceptual foundation for organizational information security awareness. *Information Management and Computer Security* 2000; **8**(1): 31-41.

[38] Abawajy J & Kim, T. Performance Analysis of Cyber Security Awareness Delivery Methods. *Security Technology, Disaster*

Recovery and Business Continuity Communications in Computer and Information Science 2010; **122**: 142-148.

[39] Schneier B. Beyond Fear: Thinking Sensibly about Security in an Uncertain World. Springer-Verlag New York, Inc, Secaucus, NJ, USA; 2003.

[40] Veiga AD, Eloff JHP. A Framework and Assessment Instrument for Information Security Culture. *Computers & Security* 2009*,* **29**(2), 196-207.

[41] Rezgui Y, Marks A. Information security awareness in higher education: An exploratory study. *Computers & Security* 2008; **27**(7-8): 241-253.

[42] Hui P, Buchegger S. Groupthink and Peer Pressure: Social Influence in Online Social Network Group. *IEEE Advances in Social Network Analysis and Mining 2009.*

[43] Danah B. *Taken out of context: American teen sociality in networked publics*. . Doctoral DIssertation. University of California, Berkeley; January 2009.

[44] Murray DL. *A Survey of the Practices and Perceptions of Students in One Catholic High School on the Use of the Internet in Relation to Safety, Cyberbullying and Sexting*. Doctoral DIssertation. University of San Fransisco; 2014.

[45] Abell JW, Steenbergh TA, Schouten A, Boivin MJ. Cyperporn use in the context of religiosity. *Journal of Psychology and Theology* 2006; **34**(2): 165-171.

[46] Hoffman AL. *The relationship between the practice of Christian spiritual disciplines and Internet pornography use among Christian college students*. The Southern Baptist Theological Seminary. Doctoral Dissertation. Proquest; 2009.

[47] Haeussinger FJ, Kranz, JJ. Information Security Awareness: Its Antecedents and mediating effects on security compliant behavior. *34th International Conference on Information Systems 2013*.

[48] Harrison DA, Newman, DA, Roth PL. How important are Job Attitudes? Meta-Analytic Comparisons of Integrative Behavioral Outcomes and Time Sequences. *Academy of Management Journal* 2006; **49**(2): 305-325.

[49] Ringle CM, Wende S, Will A. SmartPLS 2.0.M3. Hamburg: SmartPLS 2005. Retrieved from http://www.smartpls.com

[50] Hulland J. Use of partial least squares (PLS) in strategic management research: a review of four recent studies. *Strategic Management Journal* 1999; **20**(2): 195-204.

[51] Bagozzi RP, Yi Y. On the evaluation of structural equation models. *Journal of the Academy of Marketing Science* 1988; **16**(1): 74-94.

[52] Fornell C, Larcker, DF. Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research* 1981; **18**(1): 39-50.

[53] Henseler J, Sarstedt M. Goodness-of-Fit Indices for Partial Least Squares Path Modelling. *Computational Statistics* 2013; 28:565-580.