Exploring the Relationship of Individual Indicator as the Critical Factor in Information Security Awareness

Pipit Liandani[1], Muharman Lubis[2], Wahjoe Witjaksono[3]
{pipitliandani41@gmail.com[1], muharmanlubis@telkomuniversity.ac.id [2],
wahyuwicaksono@telkomuniversity.ac.id [3]}

School of Industrial Engineering, Telkom University, Ters. Buah Batu No.1, Bandung, 40257,
Indonesia

Abstract. Awareness is a starting point for employees to perform well within the organization because they can anticipate numerous problems or threats that might occurred, which often disrupt the flow of activity. At certain occasion, organization have been made guidelines and policy to help achieving the objectives and monitor the employee performances. However, the degree of successes cannot be guaranteed by them due to intervention, changes approach, realization, and constraint lead to certain employees do not comply respectively. Therefore, understanding what factors motivate employees in increasing their awareness of information security (IS) is important to help IS managers diagnose deficiencies in their IS management. It also can provide clear direction to align with training programs and workshop with organization requirement. Thus, this study wants to measure the role of individual antecedent in influencing IS awareness using quantitative method by identifying several critical factors and its relationship. Meanwhile, this study uses one moderating factor namely intention comply, five exogenous constructs consist of self-attitude (AT), self-behaviour (BV), self-cognitive (CT), self-motivation (SM), and self-responsibility (SR); and one endogenous construct namely Information Security Awareness (ISA). The results indicated two factors have significance influence to the outcome positively which are AT with t-value 1.671 (p=0.095) and CT with t value 2,264 (p=0.024) while IC as moderating factor have significant influence to BV, CT, SM, and SR positively and AT negatively as exogenous constructs.

Keywords: Information Security Awareness, Individual Antecedent, Measure

1 Introduction

Information technology systems have increasingly become important for various organizations. In today's digital world, which is characterized by a strong reliance on information systems (IS), organizations continuously aim to uphold their information security. To protect IS and organizational information assets at the individual level, information security awareness (ISA) is considered a crucial factor in influencing secure behavior. In general, ISA considers an individual's knowledge and understanding of topics related to

ICONISTECH-1 2019, July 11-12, Bandung, Indonesia

DOI 10.4108/eai.11-7-2019.2297836

information security (e.g., security risks and threats, organizational security objectives, procedures, and policies). Increased awareness should minimize “user-related faults”, nullify them in theory and maximize the efficiency of security techniques and procedures from the user point of view [1] [24]. At present, the risks associated with information security are a major challenge for many organizations, because these risks may have terrible consequences, including corporate responsibility, loss of credibility, and monetary damage [2]. Thus, ensuring information security has become one of the main managerial priorities in many organizations [3]. Raising public awareness involves creating a private and public message campaign about a specific problem, which is an important part of developing community support for change in the informal and formal sector to change knowledge and attitudes about certain aspects that want to achieve based on requirement, objective and strategy [1] [25] [26].

When the focus shifts on information security to the perspective of individuals and institutions, the employee's compliance with information security policies has emerged as the organization's main social resource because employee are often the weakest link in information security [4]. According to a recent survey of IT security practitioners by the Ponemon Institute, information and privacy management research institutions, employee negligence or laziness are the main causes of many data violations. Surveys show that 78% of respondents reported that their company experienced data violations as a result of negligent employees or employees who misused their power. Information security violations can result in loss of direct costs (e.g. intellectual property loss) and indirect costs (e.g. loss of reputation and potential loss in market share). Therefore, organizations make guidelines to employees on how to ensure information security when they use information systems when they do their work [5]. However, while making guidelines and policies an important starting point, it is not enough to ensure employee compliance. Therefore, understanding what factors motivate employees in increasing their awareness of information security is important to help information security managers diagnose deficiencies in their efforts to manage information security and provide appropriate training programs for employees. This study select the SADAR as the framework to be carried out to analyze the performance from the employee for the perspective company in Indonesia which has been developed previously [1]. The development of the SADAR framework in this study discusses information security awareness on individual antecedents in the context of banking companies.

2 Literature Review

Some literature recognizes that employees who are authorized to use certain systems or facilities can pose challenges for organizations due to their ignorance, mistakes, and intentional actions that can harm the information security [6] [7] [8]. Therefore, employees take a role and are responsible for protecting organizational resources. It is important to know what factors encourage employees to carry out these roles and fulfil their responsibilities. This study was supported by Theory Planned Behaviour (TPB) of Ajzen and Fishbein which explained that the intention to perform various types of behaviour can be predicted from attitudes toward behaviour, subjective norms, and perceived behavioural control. The theory assumes that behavior can be explained by behavioral beliefs, normative beliefs, and self-efficacy as a background to attitudes, subjective standards and control of perceived behavior, respectively [9]. Although these beliefs all influence the intention to perform behaviours, the large majority of the existing literature in the IS field, such as study on the technology acceptance model (TAM), has focused on investigating attitude and its antecedents (behavioural beliefs) because these beliefs can be reshaped by external interventions (e.g. training or policy) in the form of objective information concerning information technologies and their design to influence those behavioural beliefs and, in turn, improve attitude toward behaviour [10]. In addition to TPB, the theory behind this research is the rational choice theory (RCT), which argues that the individual determines how he will act by balancing the costs and benefits his choice [11]. In the case of IS, one can determine how he acts in fulfilling his roles and responsibilities towards IS by balancing the risks and benefits obtained from these actions. The solutions regarding antecedents of information security awareness (ISA) which had been did before trough development of SADAR Framework (Appendix B). Ahlan explained three antecedents related to ISA namely individual, institutional and environmental [1]. The study explains the role of antecedents and measures in influencing ISA, users use survey methods by analysing user perceptions. The results of the study identified several important factors that have an impact on awareness and its relationship with other factors such as religious indicators that can influence social preasure and peer performance. Furthermore, the Bulgurcu study explores the antecedents of employee compliance with an information security policy (ISP) of an organization and the impact of information security awareness (ISA) on results and employee attitudes towards compliance with ISPs [10]. Meanwhile, Kaur and Mustafa explained that a person's information security awareness is influenced by three things, namely, knowledge, attitudes, and behaviour. The study reported information security awareness on SMEs in Malaysia, the study aimed to see the relationship between knowledge, attitudes and behaviour towards the ISA. As a result, only the attitudes and behaviour of employees affect the ISA significantly [12]. Furthermore, Wahyudiwan et al found the role of the Ministry of Research, Technology, and Higher Education (MRTHE) on the knowledge, attitudes and positive behaviour about information security. In addition, the study shows a positive influence between attitude and behaviour [13]. Furthermore, effective training programs play a role in cognitive perspective in providing knowledge about information security to users [14]. The cognitive perspective focuses on the knowledge of trainees and the process of acquiring knowledge, organization, and application [15].

In addition, there are studies that explore factors of motivation and responsibility for ISA, for senior executives, information security is a basic requirement for business success. However, despite being well motivated, top managers often only have a superficial understanding of information security, which can cause them to make decisions that are not conducive to increasing the level of security of the organization. Increasing information security awareness among all employees has been deemed necessary, but the key to success is increasing the level of awareness of senior management. Playing a decisive role, they must assume overall responsibility for information security [16]. Meanwhile, Organizational literature has focused on the role of incentives in encouraging expected employee behavior [17]. Since employees' compliance to organizational policies is essential to successful organizational work [18], organizations often deploy instrumental strategies to achieve better organizational performance [19]. However, an employee's willingness to follow the rules is not necessarily motivated by such strategies. While rewards (to encourage desired behaviour) and punishments (to discourage undesirable behaviour) provide external motivations, the intrinsic desires of employees provide the internal motivation to respect (follow or not to follow) rules and regulations [20]. Based on the review literature, the hypothesis developed in this study is:

H1. User who has positive self-attitude on security prevention will positively impact towards information security awareness.
H2. User who has positive self-behaviour on security prevention will positively impact towards information security awareness.
H3. User who has positive self-cognitive on security prevention will positively impact towards information security awareness.
H4. User who has positive self-motivation on security prevention will positively impact towards information security awareness.
H5. User who has positive self-responsibility on security prevention will positively impact towards information security awareness.
H6. User who has positive intention to comply with regulation will positively impact towards self-attitudes.
H7. User who has positive intention to comply with regulation will positively impact towards self-behaviour.
H8. User who has positive intention to comply with regulation will positively impact towards self-cognitive.
H9. User who has positive intention to comply with regulation will positively impact towards self-motivation.
H10. User who has positive intention to comply with regulation will positively impact towards self-responsibility.

3 Research Method

The first is for the literature review to strengthen the ideas in this study through journals or books available on online databases such as IEEE Xplore, Science Direct, and Springer Link. The researchers found 177 studies related to IS Awareness in the past five years. After that, make a research instrument in the form of a survey that distributed to two banks in Bandung using a simple random sampling technique. The number of samples obtained is 56. Therefore this study uses PLS-SEM because the PLS-SEM procedure does not require a large number of samples (N > 100) so that it is suitable for explorative research [21]. The next step is inferential analysis based on the data obtained. In this step, smart PLS v3 is used to test hypotheses. The method used in smart PLS is PLS algorithm, bootstrapping and blindfolding. Finally, draw conclusions based on the results hypothesis testing in general to measure the properness that aligned with the framework.

4 Disscussions

4.1 Instrument

This study uses a quantitative method, where questionnaires are distributed manually to 56 bank employees in Bandung, using demographic questions about age, sex, position, work experience and how long time using an ERP system. Question of the questionnaire were 75 which were divided into four antecedents, namely individual, institutional, environment and activity. However, this study only explores the development of models on individual antecedents of SADAR, consisting of self-attitude, self-behavior, and self-cognitive as the addition of two new variables namely self-motivation and self-responsibility because according to Kajava, a person's motivational and responsibility factors can play a role in improving employee performance to achieve the desired goal (e.g. ISA and compliance) [16]. Survey list can be seen in appendix A. The questionnaire has tested to test its quality through pilot studies. Likert scale is used to measure attitudes, opinions and perceptions of a person. Respondents answer questions through a defined scale, 1 = Strongly Disagree, 2 = Disagree, 3 = Agree, 4 = Strongly Agree. Some of the research variables refer to previous studies [1]. The survey results were analyzed using SmartPLS v3 software [15] to measure validity and reliability and hypothesis testing of this research model.

4.2 Measurement Model

Using a two-way t test and 10% significance level, path coefficient is declared statistically significant if the t-value is greater than 1.62 or if the p-value is greater than 0.10 then a relationship is categorized as non-significant (NS) while the p-value smaller than 0.10 is categorized as weak (*), the value below 0.05 is categorized as medium (**), and the value below 0.01 is categorized as strong (***). Furthermore, to determine the reliability of the indicator can be seen from square each of the outer loading, an indicator is stated to have reliability indicators if the outer loading value is more than 0.7 [21], but for explorative research the value of 0.4 can be accepted [22]. The results of table 1 show that all indicators have a p-value of less than 0.01. This can be interpreted as all indicators having a strong significance of outer loadings.

Table 1. Outer Model

Reflective Variable	Reflective Indicator	Outer Loadings	t-value	p-value	90% Confidence Level		Sig. Level
					Upper	Lower	
AT	AT1	0.825	14.248	0.000	14.2558	14.24	***
	AT2	0.894	24.613	0.000	24.6178	24.608	***
	AT3	0.702	6.011	0.000	6.02663	5.9954	***
BV	BV1	0.841	16.475	0.000	16.4818	16.468	***
	BV2	0.824	12.813	0.000	12.8216	12.804	***
	BV3	0.624	4.384	0.000	4.40298	4.365	***
CT	CT1	0.613	3.753	0.000	3.77478	3.7312	***
	CT2	0.773	10.993	0.000	11.0024	10.984	***
	CT3	0.737	8.422	0.000	8.43363	8.4104	***
	CT4	0.633	5.789	0.000	5.80357	5.7744	***
	CT5	0.644	6.812	0.000	6.82469	6.7993	***
SM	SM1	0.805	12.483	0.000	12.4917	12.474	***
	SM2	0.652	5.344	0.000	5.3603	5.3277	***
	SM3	0.785	12.334	0.000	12.3426	12.325	***
	SM4	0.677	8.048	0.000	8.05922	8.0368	***
SR	SR1	0.826	13.877	0.000	13.8849	13.869	***
	SR2	0.889	29.091	0.000	29.0951	29.087	***
	SR3	0.724	6.397	0.000	6.4121	6.3819	***
IC	IC1	0.768	8.977	0.000	8.98849	8.9655	***

Reflective Variable	Reflective Indicator	Outer Loadings	t-value	p-value	90% Confidence Level		Sig. Level
					Upper	Lower	
ISA	IC2	0.819	14.952	0.000	14.9593	14.945	***
	IC3	0.685	6.944	0.000	6.95723	6.9308	***
	ISA1	0.673	5.886	0.000	5.90123	5.8708	***
	ISA2	0.774	13.137	0.000	13.1449	13.129	***
	ISA3	0.644	6.261	0.000	6.27476	6.2472	***
	ISA4	0.673	5.549	0.000	5.56517	5.5328	***

4.3 Structural Model

Table 2 shows the path coefficient of the PLS algorithm using the bootstrapping method. The results show that interrelationship of CT and ISA has strong significant value (p = 0.024). Whereas interrelationship among BV (p = 0.530), SM (p = 0.391), and SR (p = 0.360) have non-significant value to ISA, because the t-value is below 1.62 and the p-value is above 0.010. Meanwhile, interrelationship of AT and ISA weak significant (p = 0.095). In addition, IC has strong significant on the AT variable (p = 0.000), BV (p = 0.000), CT (p = 0.000), SM (p = 0.000), and SR (p = 0.000). The t-value is calculated by the path coefficient divided by the standard error. Based on t-value, AT has a direct contribution to ISA with a coefficient of 0.255 its means that 100 points of AT change will bring 25.5 points of positive changes to the ISA. BV has a direct contribution to ISA with a coefficient of 0.079, which means that 100 points of change in BV will carry 7.9 points of small positive changes to the ISA. CT has a direct contribution to the ISA with a coefficient of 0.310 which means that 100 points of change in CT will bring 31 points of positive changes to the ISA. SM has a direct contribution to the ISA with a coefficient of 0.122 which means that 100 points of change in SM will bring 12.2 positive changes to the ISA. Otherwise, SR has a coefficient of -0.134 which means that 100 points of change in SR will bring 13.4 points of negative changes to the ISA.

Table 2. Inner Model

Relationship	Path Coefficient	STERR	t-value	p-value	90% Confidence Level		Sig. Level
					Upper	Lower	
AT --> ISA	0.255	0.020445485	1.671	0.095	1.691445485	1.650554515	*
BV --> ISA	0.079	0.016837458	0.629	0.530	0.645837458	0.612162542	NS
CT --> ISA	0.31	0.018307395	2.264	0.024	2.282307395	2.245692605	**
SM --> ISA	0.122	0.019109179	0.857	0.391	0.876109179	0.837890821	NS
SR --> ISA	-0.134	0.019643701	0.916	0.360	0.935643701	0.896356299	NS
IC --> AT	-0.645	0.010289558	8.351	0.000	8.361289558	8.340710442	***
IC --> BV	0.58	0.011224972	6.928	0.000	6.939224972	6.916775028	***
IC --> CT	0.605	0.011358603	7.104	0.000	7.115358603	7.092641397	***
IC --> SM	0.595	0.012294017	6.437	0.000	6.449294017	6.424705983	***
IC --> SR	0.48	0.014565738	4.408	0.000	4.422565738	4.393434262	***

4.4 Validity and Reliability

A test is valid if the measurement used is appropriate based on the requirement while the reliability related to the consistency of the result in different context. ISA has R2 = 0.811 which means that the individual antecedents explain 81.1% of the changes variation in ISA variable. Cronbach's alpha and Composite Reliability are commonly used to measure internal consistency reliability. Variables can be stated as reliable if they have a Cronbach‘s Alpha value or composite reliability greater than 0.7 [17]. But for explorative research, variables that have Cronbach‘s Alpha values and Composite Reliability above 0.6 can be accepted [18]. Table 3 shows that of the 7 variables tested, all of them have Cronbach Alpha‘s and Composite Reliability values above 0.6. So that it can be stated that all variables have good reliability and provide stable measurement results. Furthermore, to measure convergent validity can be examined using the AVE value. Variables can be stated valid if they have AVE values of more than 0.5 [15]. 5 of the 7 variables showed good results because they had AVE values greater than 0.5, only CT and ISA that do not meet.

Table 3. Latent Variable Quality

Latent Variable	AVE	Composite Reliability	R^2	Cronbach’s Alpha	Communality	Redundancy	LV Index Value	Q^2
AT	0.658	0.851	0.416	0.743	0.658	0.273728	1.496	0.233
BV	0.592	0.810	0.319	0.655	0.592	0.188848	3.195	0.177
CT	0.467	0.813	0.366	0.717	0.467	0.170922	3.446	0.133
SM	0.537	0.822	0.354	0.712	0.537	0.190098	3.500	0.171
SR	0.665	0.856	0.23	0.749	0.665	0.15295	3.458	0.133
IC	0.577	0.802		0.631	0.577		3.519	
ISA	0.48	0.786	0.811	0.637	0.48	0.38928	3.491	0.268

4.5 Discriminant Validity

It is the test of validity from the differentiated discrimination or validity whether the concepts or measurements that should not be relevant are not actually linked. Fornell and Lacker [23] suggest that discriminant validity can be measured using AVE square root of each latent variable. A variable can be stated as having good discriminant validity if the AVE square root value is greater than its correlation value with other variables. Table 4 shows that the AVE square root of each latent variable has a value greater than its correlation value with other latent variables. AT variable has AVE square root value of 0.811 and this value is greater than the values below which is the correlation value between AT variables with variables BV, CT, SM, SR and IC. The same thing with the variables BV, CT, SM, SR, IC which have squared AVE values that are greater than the values below.

Table 4. Discriminant Validity

Latent Variable	AT	BV	CT	SM	SR	IC	ISA
AT	0.811						
BV	0.569	0.769					
CT	-0.728	0.408	0.683				
SM	-0.643	0.522	0.541	0.733			
SR	-0.593	0.637	0.485	0.524	0.816		
IC	-0.645	0.58	0.605	0.595	0.48	0.759	

Latent Variable	AT	BV	CT	SM	SR	IC	ISA
ISA	-0.583	0.553	0.6	0.574	0.521	0.556	0.693

4.6 Hypothesis Testing

It is used to infer the hypothesis results of the sample data from a larger population, which this test tells the analyst whether the main hypothesis is true or not. Statistical analysts test hypotheses by measuring and examining random samples from the analyzed population. Interestingly, testing hypotheses based on statistical significance is another way of expressing confidence intervals while the process of distinguishing between the null hypothesis and the alternative hypothesis is supported by considering two types of conceptual errors, which occurs when an empty hypothesis is rejected or is not rejected. Based on the result above, it can be said that the exogenous variables (AT, BV, CT, SM and SR) can explain the variations in changes of 81.1% towards ISA (R2 = 0.811). The IC variable can explain the variations in changes in AT, BV, CT, SM and SR, respectively by 41.6%, 31.9%, 36.6%, 35.4%, and 23%.

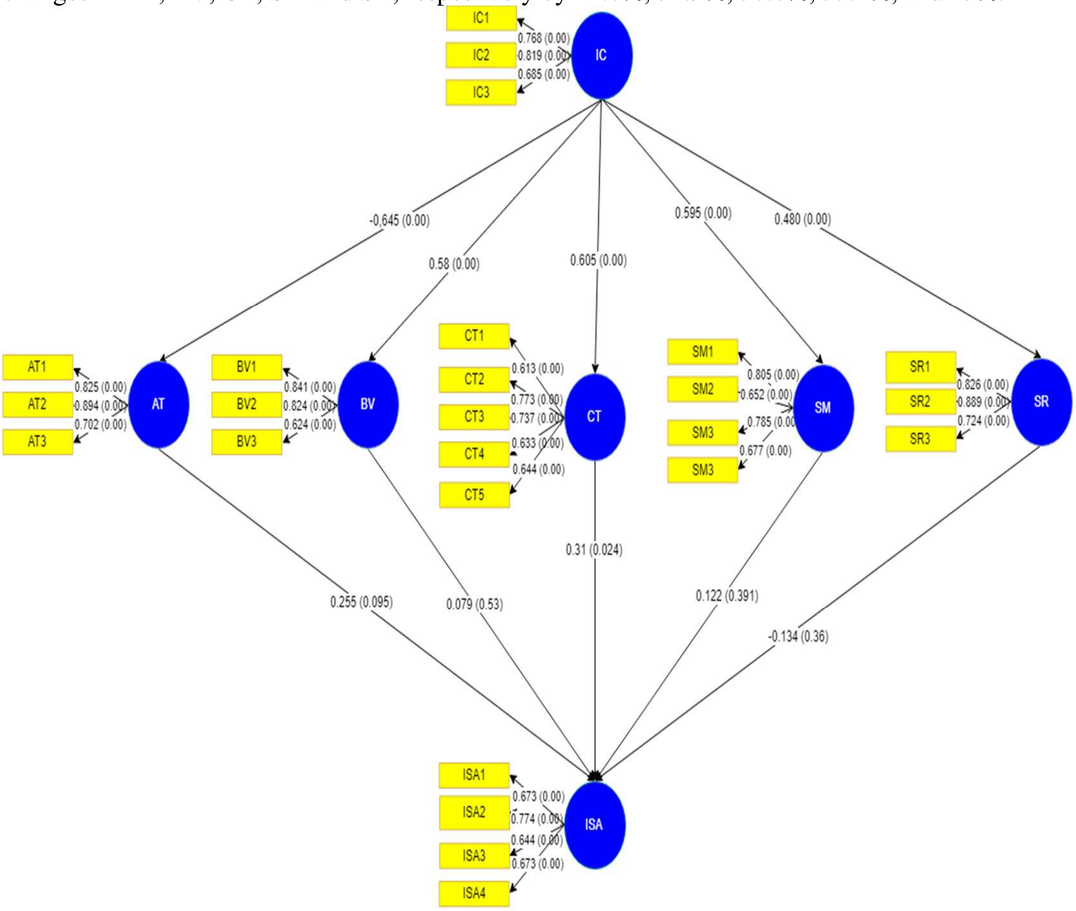


Fig. 1. SADAR Framework Model PLS Result

H1. The relationship of AT and ISA has path coefficient 0.255 (p=0.095) which means that AT has a weak significant effect positively to ISA so hypothesis 1 is accepted.
H2. The relationship of BV and ISA has path coefficient 0.079 (p=0.530) which means that BV has not significant effect positively to ISA so hypothesis 2 is rejected.
H3. The relationship of CT and ISA has path coefficient 0.310 (p=0.024) which means that CT has a medium significant effect positively to ISA so hypothesis 3 is accepted.
H4. The relationship of SM and ISA has path coefficient 0.122 (p=0.391) which means that SM has not significant effect positively to ISA so hypothesis 4 is rejected.
H5. The relationship of SR and ISA has path coefficient -0.134 (p=0.360) which means that SR has not significant effect positively to ISA so hypothesis 5 is rejected.
H6. The relationship of IC and AT has path coefficient -0.645 (p=0.000) which means that IC has a strong significant effect negatively to AT so hypothesis 6 is accepted.
H7. The relationship of IC and BV has path coefficient 0.580 (p=0.000) which means that IC has a strong significant effect positively to BV so hypothesis 7 is accepted.
H8. The relationship of IC and CT has path coefficient 0.605 (p=0.000) which means that IC has a strong significant effect positively to CT so hypothesis 8 is accepted.
H9. The relationship of IC and SM has path coefficient 0.595 (p=0.000) which means that IC has a strong significant effect positively to CT so hypothesis 9 is accepted.
H10. The relationship of IC and SR has path coefficient 0.480 (p=0.000) which means that IC has a strong significant effect positively to CT so hypothesis 10 is accepted.

5 Conclusion

Many organizations recognize that their employees, who are often considered the weakest link in information security can also be helpful in reducing the risks associated with information security. Therefore, raising awareness of information security to employees is important, because they can anticipate numerous problems or threats that might occurred. This study explores the possible factors that influence a person's information security awareness, specifically exploring the individual antecedents of SADAR framework that have been developed previously [1] which can be used to measure IS awareness of employees from their own perspective in executing policies and objectives expected by the organization. In previous studies, antecedent individuals did not have a significant effect on ISA in the academic environment. Interestingly, this study shows that self-attitude and self-cognitive factors have a significant influence on ISA positively in the banking environment while intention to comply as moderating factor have a strong significant influence on individual antecedent. Therefore, this research is expected to help organizations in the early phase of IS strategy change by considering the factors that exist in this study in order to provide policies that are in accordance with the conditions and objectives of the organization. It can be said that this is the most important element of trust because every skill, quality and other task can be performed and brought back to awareness as it will give the students or employees an insight into their beliefs leading to positive action. This study still has limitations from several aspects, so it needs to be improved in further research, including the number of samples that suggested for this study more than 100 so that the samples can represent the population and more reliable. In addition, more explore other factors that have an influence on information security awareness to better represent the factors that influence such awareness based on the perspective of the user himself. Finally, the factors that influence information security awareness in this study can be considered in further research studies.

References

[1] Ahlan, A.R., Lubis, M., and Lubis, A.R.: Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. *Procedia Computer Science* 72, p. 361 – 373 (2015).

[2] Cavusoglu, H., Cavusoglu, H., and Raghunathan, S.: Economics of IT Security Management: Four Improvements to Current Security Policies. *Communication of the Association for Information Systems*, 14, p. 65-75 (2004).

[3] Brancheau, J.C. and Wetherbe, J.C.: Key Issues in Information Systems Management. *MIS Quarterly*, 11 (1) p. 23-45 (1987).

[4] Warkentin, M. and Willison, R.: Behavioral and Policy Issues in Information Systems Security: The Insider Threat. *European Journal of Information Systems*, 18 (2), p. 101-105 (2009).

[5] Whitman, M.E., Townsend, A.M. and Aalberts, R.A.: Information Systems Security and the Need for Policy. Information Security Management – Global Challenges in the Next Millennium. Ed. Gurpreet Dhillon. Hershey PA: IGI Global, p. 10-20, (2001).

[6] Durgin, M.: Understanding the Importance of and Implementing Internal Security Measures. *SANS Institute Reading Room* (2007).

[7] Lee, J. and Lee, Y.: Holistic Model of Computer Abuse Within Organizations. *Information Management and Computer Security*, 10 (2) p. 57-63 (2002).

[8] Lee, S.M., Lee, S-G. and Yoo, S.: An Integrative Model of Computer Abuse based on Social Control and General Deterrence. *Information and Management*, 41 (6), p. 707-718 (2004).

[9] Ajzen, I.: The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, 50 (2), p. 179-211 (1991).

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

[11] Paternoster, R. and Pogarsky, G.: Rational Choice, Agency and Thoughtfully Reflective Decision Making: The Short and Long-Term Consequences of Making Good Choices. *Journal of Quantitative Criminology*, 25 (2), p. 103-127 (2009).

[12] Kaur, J. and Mustafa, N.: Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME. *International Conference on Research and Innovation in Information Systems* (ICRIIS), Kuala Lumpur (2013).

[13] Wahyudiwan, D.D.H., Sucahyo, Y.G. and Gandhi, A.: Information security awareness level measurement for employee: Case study at ministry of research, technology and higher education. *International Conference on Science in Information Technology* (ICSITech), Bandung (2017).

[14] Waly, N., Tassabehji, R. And Kamala, M.: Improving Organisational Information Security Management: The Impact of Training and Awareness. *IEEE 14th International Conference on High Performance Computing and Communication* (2012).

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

[16] Kajava, J., Anttila, J., Varonen, R., Savola, R. and Roning, J.: Senior Executives Commitment to Information Security - from Motivation to Responsibility. *International Conference on Computational Intelligence and Security*, Guangzhou (2006).

[17] Stajkovic, A.D. and Luthans, F.: A Meta-Analysis of the Effects of Organizational Behavior Modification on Task Performance. *Academy of Management Journal*, 40 (5), p. 1122-1149 (1997).

[18] Vardi, Y. and Weitz, E.: Misbehavior in Organizations: Theory, Research and Management. Hillsdale, NJ: Lawrence Erlbaum Associates, (2004).

[19] Huselid, M.A.: The Impact of Human Resource Management Practices on Turnover, Productivity, and Corporate Financial Performance. *Academy of Management Journal*, 38 (3), p. 635-872 (1995).

[20] Tyler, T.R. and Blader, S.L.: Can Businesses Effectively Regulate Employee Conduct? The Antecedents of Rule Following in Work Settings. *Academy of Management Journal*, 48 (6), p. 1143-1158 (2005).

[21] Hair, J., Hult, T., Ringle, C.M. and Sarstedt, M.: A Primer on Partial Least Squares Structural Equation Modelling (PLS-SEM). SAGE Publications, January (2014).

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

[23] Fornell, C. and Larcker, D.F.: Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, 18 (1), p. 39-50 (1981).

[24] Lubis, M., Kartiwi, M. and Zulhuda, S.: Election Fraud and Privacy Related Issues: Addressing Electoral Integrity. *Proceedings of the IEEE ICIC* (2016).

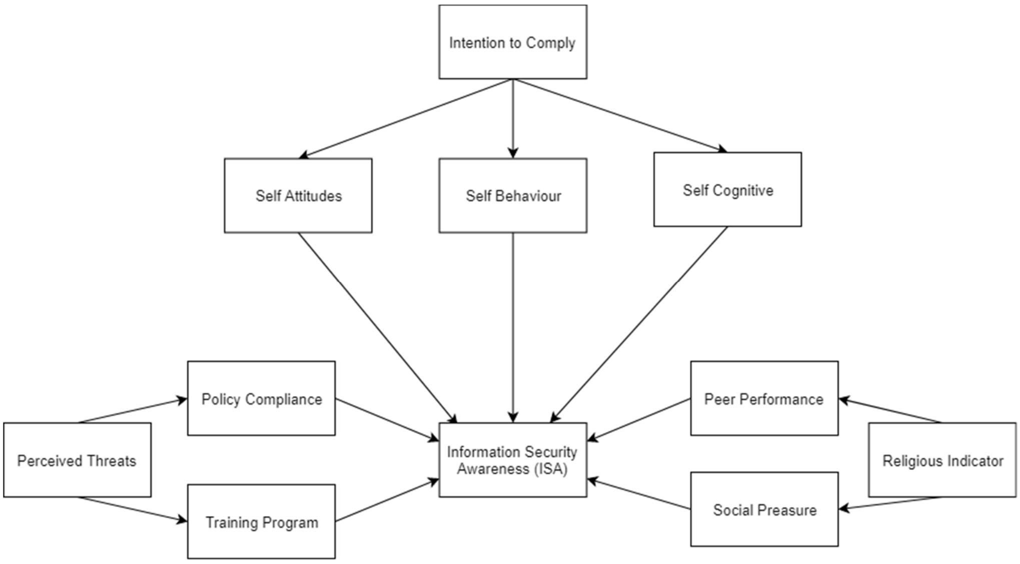
[25] Lubis, M. and Maulana, F.A.: Information and Electronic Transaction Law Effectiveness (UU-ITE) in Indonesia. Proceedings of ICT4M (2011).

[26] Lubis, M and Azizah, A.H.: Towards Achieving the Efficiency in Zakat Management System: Interaction Design for Optimization in Indonesia. Int. Conf. On User Science and Engineering, User Science and Engineering pp. 289-301 (2018),

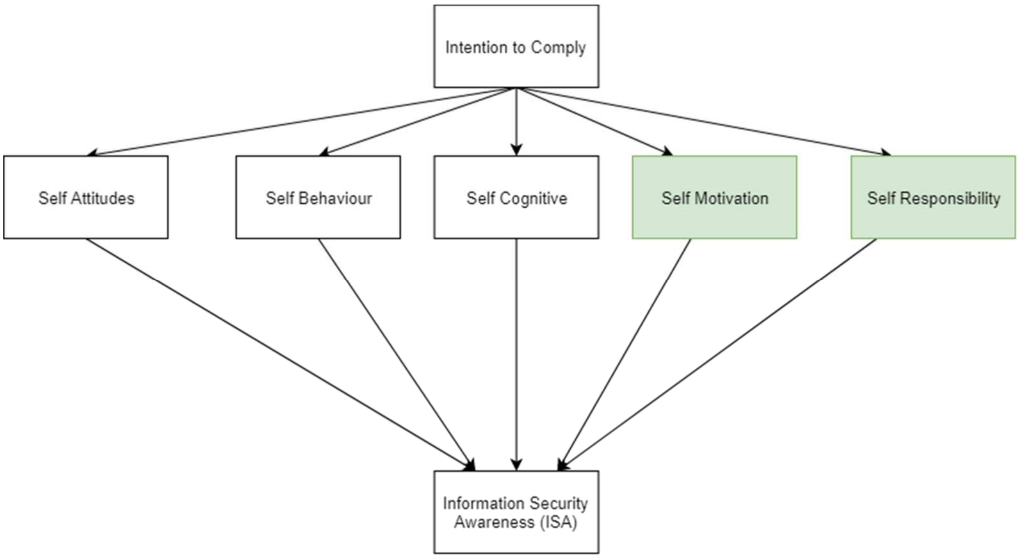
Appendix A. Survey List Simple Translated Questions in English

Self Attitude (AT)	
1	Increased KPI (Key Performance Indicator) is influenced by the performance of coworkers
2	It's more convenient to use a legal software
3	Fully entrust information security to company management
Self Bahavior (BV)	
1	Often access company information with public networks
2	Prefer learning from experience rather than a system manual book.
3	It is not a problem to divulge important information as long as it does not cause problems
Self Cognitive (CT)	
1	Always ask friends if there is a problem with the ERP system
2	Always update information about system security procedures
3	Always share the experiences that I have with colleagues
4	Awareness that company management information systems have disadvantages
5	Awareness that capabilities become more improved after utilizing a company information system
Self Motivation (SM)	
1	Awareness that if company information is spread, it will suffer losses
2	Understanding that information security systems are very important things to control
3	An information security system will be achieved through mutual agreement
4	Appreciation needs if they works well
Self Responsibility (SR)	
1	appreciate the advice given by superiors
2	understand that mistakes made will interfere with the performance of others
3	Responsibility to help their colleagues who have difficulty using company information systems
Intention to Comply (IC)	
1	Restricting access needs to be done to several system functions
2	Committed to using company information systems professionally based on the responsibilities given
3	Understand the universal principles of data security
Information Security Awareness (ISA)	
1	Comply with the responsibilities given in managing information systems
2	Responsible for acknowledging mistakes
3	Information about the bad implications of the media about the dangers of negligence on data security can trigger the behaviour to always comply with regulations

Appendix B. SADAR Framework in Previous Study



Appendix C. SADAR Framework in this Study


Intention to Comply
Self Attitudes
Self Behaviour
Self Cognitive
Self Motivation
Self Responsibility
Information Security Awareness (ISA)