JOSTIP

Vol. 7 No. 2 (Dec 2021)

AWARENESS OF ICT SECURITY POLICY TO ENSURE DATA PROTECTION IN FORESTRY DEPARTMENT PENINSULAR MALAYSIA

Renee Lee[1], Aini Suzana Ariffin[2*]
[1] Division of Silviculture and Forest Biodiversity Conservation, Forestry Department Peninsular Malaysia
[2] Perdana Centre of STI Policy Studies, Razak Faculty of Technology and Informatics

• Corresponding Author: ainisuzana@utm.my

Abstract

The Forestry Department Peninsular Malaysia's (FDPM) ICT Security Policy was developed and implemented in 2012 and reviewed in 2015. This policy aims to take the lead in managing data, hardware, software, network, and ICT security under legal regulations. Amongst the department's responsibilities are to implement data confidentiality, integrity, and availability policies to ensure the continuity of activities and services while mitigating the impact of security incidents. Accidentally, on September 16, 2016, a fire broke out in the FDPM building, causing property damage and document destruction with an estimated loss of RM30 million. Currently, in Malaysia, cybercrime and government data intrusion has become increasingly difficult to combat. Raising public awareness, particularly among officers who serve as service providers and department employees, is therefore critical to address those issues. Therefore, the objectives of this research are to determine the level of awareness of FDPM employees regarding FDPM ICT Security Policy as well as to investigate the factors that influence information security awareness. Inputs from this study were derived from both primary and secondary sources to meet the objectives. Primary data was gathered through surveys where 130 questionnaires were distributed to FDPM headquarters employees at the management, professional, and support team levels. Meanwhile, secondary data was gathered from FDPM annual and management reports, statistical data, journals, reference documents, and the Internet. The findings were analyzed statistically using SPSS. The level of awareness has been determined and an appropriate criterion to improve the level of information security awareness among FDPM employees was recommended which may help for a better understanding of department culture and increase a higher level of security awareness among FDPM employees.

Keywords: Awareness level; ICT security policy; Information security awareness; Forestry Department of Peninsular Malaysia (FDPM); Data Protection.

■ 1.0 INTRODUCTION

The ICT Security Policy of the Forestry Department Peninsular Malaysia (FDPM) was formulated in 2012 and updated in 2015. This policy aims to take a lead in data management, hardware, software, network, and ICT security by legal regulations. Implement policies for data availability, integrity, and confidentially to ensure the continuity of activities and services while minimizing the impact of security incidents. However, a fire broke out on September 16, 2016, in the FDPM building caused property damage and document destruction. The incident has resulted in departmental losses in terms of destruction of assets, property, and destruction of documents with an expected loss of RM30 million. Indirectly, it affects the work performance and comfort of officers in handling daily tasks. Moreover, cybercrime and government data intrusion have become increasingly difficult to deal with in Malaysia. Therefore, raising awareness among the public, especially officers, who serve as service providers and department employees, is necessary to address the issue.

Therefore, the objectives of this research are to determine the level of awareness of FDPM employees regarding FDPM ICT Security Policy. Besides, this research is to investigate the factors that influence information security awareness. As a result, recommend appropriate criteria to improve the level of information security awareness among FDPM employees. It is difficult to meet ICT security requirements due to the complexity of ICT systems, which are easily exposed to threats, vulnerabilities, and risks. As a result, understanding the ICT Security Policy is crucial not only for preventing cybercrime but also for improving data protection in FDPM. According to the complaint record, there are still a large number of cases reported with a total of 293 complaints in 2019, 140 complaints in 2021 with the average number of complaints received per month being around 15-20 cases. Furthermore, the programs are more focused on technical and technological applications, with less emphasis on ICT Security Policy awareness. The program is not comprehensive for all levels of the Department.

■ 2.0 LITERATURE REVIEW

Information Security Awareness (ISA) is a type of security knowledge that is acquired over time through continuous training to influence a trainee's behavior (Al-Daeef et al, 2017). Kruger and Kearney (2005) developed a model for evaluating information security awareness based on knowledge, attitude, and behavior (KAB). KAB's basic theory is that it tries to understand the relationship between these three components, demonstrating that as knowledge accumulates, it manifests itself in related behaviors. Previous research used the same framework, particularly from the field of social psychology, to respond favorably or unfavorably to a specific object based on three (3) components: knowledge (What does a person know?), attitude (How do they feel about the topic?) and behavior (What do they do?) (Refer to Figure 1).

According to Kruger and Kearney (2008), knowledge is based on the user's understanding of how to act in a given situation. Users who have the proper knowledge have a higher level of awareness because they can prevent threats and attacks. The user's belief that passwords should be kept secret and should not be written down or given to others will protect data from unauthorized access, resulting in maximum data confidentiality. Employee behavior is based on what they do and is related to their actual behavior (Kruger and Kearney, 2008). For instance, it is important to keep passwords secret and ensure that passwords are strong (Kruger, Drevin, and Steyn) (2010). To avoid data loss caused by a virus infection, which can also jeopardize data integrity, scanning email attachments for viruses is a good idea. Data availability is not disrupted when backups are performed regularly in alternate locations.

According to Jasber Kaur's (2013) findings, there is a significant relationship between user attitude and behavior and information security awareness. However, there is no relationship between knowledge and information security awareness. There was no correlation between information security awareness and knowledge. Employees are aware of their responsibilities in maintaining the confidentiality of business information and resources, implying that attitude and behavior play a significant role in confidentiality. Furthermore, user feedback indicates that they lack the necessary knowledge to deal with phishing emails and other similar issues. This may explain why knowledge constructs are meaningless. The organization should educate and improve employees' knowledge of information security.

Previous research on information security has emphasized the importance of security awareness in influencing employee behavior. According to Bulgurcu et al. (2010), employee willingness to comply is significantly affected by awareness. Puhankinen et al. (2010) conducted an action study to validate the training program for information security policy compliance. The results of the study indicate that awareness-raising and training programs will have an impact on users' compliance with information security policies. Chan and Mubarak (2012) concluded that a "lack of awareness and understanding of policies may cause employees to violate such policies. The information security policy purpose is to provide management support and guidance for information security (British Standard Institute, 1995). The ICT security policy explains how organizations address security issues to protect personal and confidential data.

Referring to the Data Protection Management Framework Whitepaper (2020) established by the SECO institute emphasized that effective data protection requires employees to be aware of data protection risks and handle personal data accordingly. To implement or improve awareness measures, the organization needs to analyze employees, behavior towards personal data, chart the present behavior, data protection concerns, define the desirable behaviors, and determine how employees will be inspired towards behavioral change and how to access the progress. Based on works being carried or by many scholars such as Mark A and Rezgui YA (2009), Puhankinen et al. (2006 and 2010), and Abdul RA, Muharman L., & Arif R.L. (2015) emphasize the significant factors that influence the level of Information Security Awareness. (ISA) as illustrated in figure 1 below.

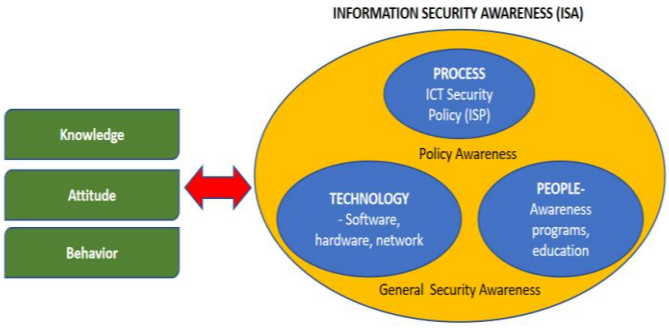

Figure 1: Factors that influence the level of Information Security Awareness (ISA)

In addition, the Government of Malaysia also plays a major role in Information Security initiatives particularly on infrastructure development and risk systems management. Referring to Mustaffa (2015), CyberSecurity Malaysia has managed more than 57,000 incidents from 1997 to 2014 which included intrusion, fraud, cyber harassment, spam, and malicious code. Suhazimah & Ali (2011) stated that information security is a complex, dynamic and multifaceted discipline in which no single component may be ignored and the effective management of this discipline is essential for any organization to survive and sustain itself in this information age.

Another related initiative was on Personal Data Protection Act where it was introduced in May 2010 and came into force in 2013. The objective of the Act is to protect the personal data of individuals from commercial transactions. In addition, Hannah & Vilasmalar (2014) described personal data is regarded as any information related to an individual's identity, characteristics, the behavior of the individual that is identified and could be accessed from the information and database which also includes any expression of opinion about an individual.

■ 3.0 METHODOLOGY

3.1 Research Design:

According to Sekaran & Bougie (2013), a research design was used as the study's blueprint to collect information, measure data, and analyze data to explain research problems. Goundar (2012) stated that the causal relationship between variables is measured and analyzed using a quantitative approach. Given this, a quantitative method has been adopted to determine employees' level of awareness on the FDPM ICT security policy which was introduced and to investigate the factors that influence information security awareness. Knowledge, attitudes, and behavior variables can be statistically measured and interpreted through this method.

In addition, the type of research used in this study is a descriptive survey method. According to Parmjit et al. (2006), this type of research seeks to elicit the thoughts, perceptions, and opinions of a large population about a specific issue. The main issue under this study is the level of awareness of the ICT Security Policy to enhance data protection among FDPM employees. Meanwhile, a descriptive study, according to Sekaran (2003), is used to describe the characteristics of the variables being studied. She emphasizes the importance of descriptive research in creating a profile or describing relevant aspects of a phenomenon of interest from an organizational, industry-oriented, individual, or other perspectives.

3.2 Respondents

The target respondent included 480 FDPM positions from various job positions and levels, such as higher group levels, management, and professional group levels, and support group levels (Annual Report FDPM, 2019). Due to time constraints, the sample size has been limited to 193 Headquarters FDPM employees from managerial and professional groups (grade 41-54) and the supporting group level (grade 19-40). These groups were chosen because they are directly involved in the application of ICT. In this study, simple random sampling, one of the probability sampling techniques, was used. The sample for this study was calculated with a 95% confidence level using Taro Yamane's (Yamane, 1973) formula. As a result, a sample size of 132 respondents was required for this study.

3.3 Data Collection Procedure

The first step in this study was to carry out literature reviews to gauge the significance of employee compliance with an FDPM's information security policy (ISP). This study looked look into the rational factors that motivate employees to comply with ISP requirements to protect the FDPM's information and technology resources. Next, identification of various instruments that are used to measure the ISA level, how the ISA instrument framework is conducted, and how the Human Aspect Information Security Questionnaire (HAIS-Q) framework developed by Parson (2017) can be applied to determine the ISA level in the department. All this information was gathered through reading materials such as reference books, journals, and other materials used as references. This data was used to reinforce all of the knowledge, results, and interpretation of the obtained results.

Survey questionnaires were distributed to gather responses and feedback from respondents. The questionnaires were based on an online form called Google Form, and they were distributed to respondents via a shared link via social media applications such as WhatsApp, as well as via email to employees. Respondents participated voluntarily, and data was collected over three weeks. Data obtained is being recorded, interpreted, and analyzed.

3.4 Data Analysis

During the early stages of data analysis, the data were entered into computer program software in the Microsoft Excel spreadsheet format. Any information gathered was analyzed quantitatively (via frequency analysis) with the Statistical Package for Social Science (SPSS). To begin, the base data for frequency, percentage, mean, and standard deviation were computed using descriptive analysis. Then, cross-tabulation was used to compare variable differences and Pearson Chi-squared P-value significance at the <0.05 level.

Second, data analyses were conducted to investigate and interpret the relationship between variables. To determine whether there was a statistical difference between the means of groups, a statistical comparison called One-way Analysis of Variance (ANOVA) was used. Meanwhile, a Simple Linear Regression analysis was used to look for a significant relationship between each of the factors that influence information security awareness. For data interpretation, a significance level of $p< 0.05$ is established.

For the management aims, demographic questions (e.g. gender, age, level of education, job position, and computer and internet usage) were analyzed using descriptive analysis. Meanwhile, factors that influence the level of information security awareness were analyzed using the Likert Scale and ANOVA. To eliminate neutral answers

and avoid bias, each question was appraised using five (5) modified Likert Scale: "Strongly disagree", "Disagree", "Neutral", "Agree", and "Strongly Agree." as shown in Table 3.1 below. The questionnaire.es were converted into points in data tabulation to obtain the quantitative result using the Likert Scale

Table 3.1: Likert Scale Point

POINTS	STRONGLY DISAGREE	DISAGREE	NEUTRAL	AGREE	STRONGLY AGREE
Positive Question	1	2	3	4	5
Negative Question	5	4	3	2	1

Finally, the tabulation's final score was classified using Kruger's Scale of Information Security Awareness Measurement and used in the analysis, with the results shown in Table 3.2:

Table 3.2: Kruger's Scale of Information Security Awareness Measurement Score

SCORE	RESULT
80-100	Good
60-79.99	Average and need improvement
0-59.99	Poor and need direct action

■ 4.0 RESULT AND DISCUSSION

4.1 Demographic Analysis

In terms of gender distribution, males made up the majority of respondents, accounting for 53.8% of all respondents. The majority of respondents were between 36-45 years old, accounting for 53.79% of all respondents. Approximately 73.48% of those who participated in the study were from the forestry field, and 53.03% were from grades 41-44. The majority of respondents (56.82%) held a Bachelor's degree.

The survey results show that 62.12% of respondents have used computers and the Internet for nearly 10-20 years, and 56.06% of respondents have used computers for 4-8 hours a day in their daily work. In addition, 68.94% of the respondents have been exposed to an ICT security course at least once, while 31.06% of the respondents have never participated in an ICT security course during the service period. Nearly 44% of courses are organized by FDPM. But in the past three (3) years (2018-2020), the survey results show that 56.06% of people did not participate in any ICT security courses. Demographic data are presented in the Table 4.1below.

Table 4.1: Respondent's Demographic Information

No.	Demographic Information	Variables	Frequency (N=132)	Percentage (%)
1.	Gender	Male	71	53.8
		Female	61	46.2
2.	Age	20-25 years old	1	0.76
		26-35 years old	39	29.55
		36-45 years old	71	53.79
		46-55 years old	19	14.49
		56-65 years old	2	1.52

3.	Scheme of service	Forestry (G)	97	73.48
		Economy (E)	2	1.52
		Information System (F)	5	3.79
		Engineering (J)	1	0.76
		Legislation (L)	2	1.52
		Administration and Diplomatic (M)	1	0.76
		Administration and Support (N)	16	12.12
		Social (S)	2	1.52
		Financial (W)	1	0.76
		Others	5	3.79
4.	Grade of position	19-26	23	17.42
		29-40	14	10.61
		41-44	70	53.03
		48-54	25	18.94
		Premier Grade C and above	0	0.00
5	Education level	Secondary School	15	11.36
		Diploma/ STPM/ HSC	17	12.88
		Bachelor's degree	75	56.82
		Master's degree	25	18.94
		PHD	0	0.00
		Others	0	
6.	Years of computer & Internet usage	1-5 years		0.76
		6-10 years	**1**	9.85
		10-20 years	13	62.12
		20-30 years	82	24.24
		30-40 years	32	3.03
			4	
7.	Hours of computer usage per day for work	None	2	1.52
		1-4 hours	33	25.00
		4-8 hours	74	56.06
		More than 8 hours	23	17.42
8.	How many ICT security courses have you attended during your service period?	0	41	31.06
		1	27	20.45
		2	17	12.88
		3	18	13.64
		More than 3	1	0.76
		4	2	1.52
		5	7	5.30
		More than 5	2	1.52
		6	1	0.76
		10	6	4.55
		More than 10	2	1.52
		11	1	0.76
		12	1	0.76
		15	1	0.76
		More than 15	1	0.76
		20	1	0.76
		More than 20	1	0.76
		Not sure	2	1.52
9.	How many ICT security courses have you attended in the last three (3) years (2018-2020)?	0	74	56.06
		1	24	18.18
		2	10	7.58
		3	14	10.61
		More than 3 times	1	0.76
		4	1	0.76
		Less than 5 times	2	1.52
		5	3	2.27
		6	1	0.76
		13	1	0.76
		More	1	0.76
10.	If you have ever attended an ICT security course, please indicate the organizer of the course	None	46	34.3
		Forestry Department Peninsular Malaysia	59	44
		Government	52	38.8
		Private/NGO	8	6
		Others	2	1.5

4.2 One-way Analysis of Variance

The analysis indicates a moderate positively significant correlation between factors of knowledge, attitude, and behavior (R=0.626, p<0.05). The regression analysis of the relationships between knowledge and attitude shows a low significant relationship (R=0.481, p<0.05). Meanwhile, the relationship between knowledge and behavior shows a moderate, positively significant relationship (R=0.645, p<0.05). Besides, the relationships between attitude and behavior show a moderate, positively significant relationship (R=0.616, p<0.05). On the other hand, there is no significant correlation between gender, age, service scheme, grade of position, education level, and time spent on computers and the internet. However, the results revealed a strong and significant correlation (p<0.05) between the total number of ICT security courses taken during the service period and the number of ICT security courses taken in the previous three (3) years (2018-2020). The result has shown as in Figure 2 below;

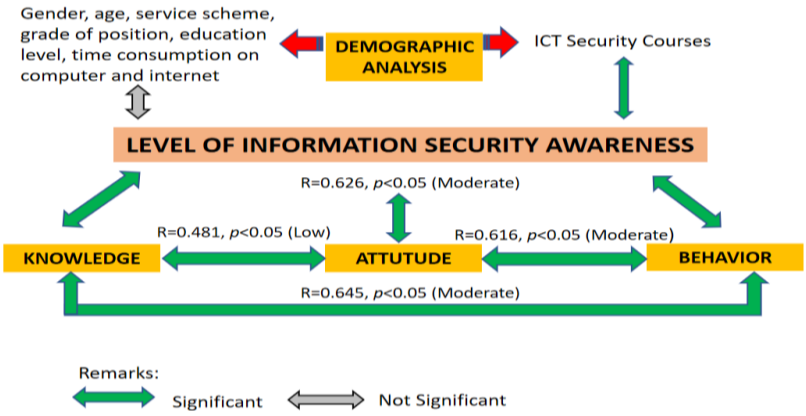

Figure 2: Correlation between Factor of Knowledge, Attitude & Behavior that influence level towards information security awareness

Kruger's Scale of Information Security Awareness (ISA) Measurement

As represented in Table 4.2 the ISA measurement is classified as Good with a total score of 83.86%. The general score for the Knowledge Dimension is 79.62% (average and needs improvement), the Attitude Dimension is 85.12% (Good), and the Behavior Dimension is 86.84% (Good). The results obtained show that there are four (4) focus areas that are classified as good and three (3) focus areas are classified as average and need improvement. The focus areas classified as good are Password Management, Mobile Devices, Incident Reporting, and Information Handling, while the focus areas that are classified as average are Social Media Use, Internet Use, and Email Use.

NO.	FOCUS AREA	AWARENESS VARIABLE SCORE (%)				RESULT
		PART B KNOWLEDGE	PART C ATTITUDE	PART D BEHAVIOR	AVERAGE	
1.	Password Management	88.80	87.24	91.96	89.33	Good
2.	Email Use	76.59	83.98	78.89	79.82	Average and need improvement
3.	Internet Use	74.89	67.92	76.24	73.02	Average and need improvement
4.	Social Media Use	65.95	84.78	89.00	79.91	Average and need improvement
5.	Mobile Device	86.06	90.86	90.38	89.10	Good
6.	Information Handling	91.29	90.12	91.45	90.95	Good
7.	Incident Reporting	73.73	90.92	89.95	84.87	Good
	Total Score for Awareness Level	79.62	85.12	86.84	83.86	Good

■ 5.0 DISCUSSION

The hypothesis that knowledge, attitude, and behavior influence the level of information security awareness among FDPM employees has been tested and proven. According to the findings, employees who are more knowledgeable about ICT security policies have a higher level of awareness about information security. Furthermore, employees with a more positive attitude and behavior toward ICT security policy awareness have a higher level of awareness towards information security awareness. These findings were elaborated further in research objectives as below;

5.1 Research Objective 1: To identify the level of awareness of FDPM employees of the FDPM ICT security policy.

A total of 132 responses received from various groups of gender, age, and service scheme, grade of position, education level, experience, and the number of ICT awareness courses attended were recorded and analyzed. 53.8% of respondents were male and mostly in the age group of 36-45 years old (53.79%). About 73.48% of the respondents who participated in the study were from the Forestry Sector with grades 41-44 (53.03%) and held a Bachelor's degree (56.82%). Almost all respondents were familiar with the use of computers and the internet and used them in their daily work routine (56.06%). However, there is still a lack of training because in the past three (3) years (2018-2020), the finding showed that 56.06% of people did not participate in any ICT security courses, which resulted in a moderate level of awareness of the ICT security policy. The result reveals that the number of ICT security courses attended has a strong and significant correlation with the awareness level of the ICT security policy.

Besides, there are four (4) focus areas that are classified as good and three (3) focus areas are classified as average and need improvement. The focus areas classified as good are Password Management, Mobile Devices, Incident Reporting, and Information Handling, while the focus areas that are classified as average are Social Media Use, Internet Use, and Email Use. The Email Use section focuses on user behavior when they click a link or open an attachment without considering the content. The reason for such actions could be a result of the trust formed between co-workers. This area showed only 79.82% of the score. Meanwhile, for the Internet Use section, the result shows the lowest score with 73.02%. This issue is related to downloading files, accessing websites, and entering information online, which can only be done on a trusted site. In addition, for Social Media Use, the scores of 79.91% deal with the content posted by the user, both in their private life and at work that reflects the FDPM's image. However, the results demonstrate that awareness is still at a good level, but there is still room for improvement from all of the focus areas. Thus, there are suggestions for improving these through awareness programs by providing educational techniques such as onsite or web-based training, peer presentations and mentoring for knowledge dimension, information and promotion techniques –making a poster, "do and don't" lists, screen savers on the employees' PCs, and warning banners on the intranet (Kusumawati, 2018).

It's difficult to create information security policies that are both enforceable and force compliance. Employees' noncompliance is frequently attributed to the policy's impact on their productivity and uncontrolled behavior. 20.38% of the employees are unaware of the existence and implementation of the FDPM ICT security policy, while knowledge of the policy stands at 79.62%, on an average level, and needs improvement. The survey also indicates that employees are probably unaware of the ICT security threats FDPM potentially faces. They are not fully exposed to the importance of ICT Security. Therefore, they must understand the risk they are exposing FDPM when using a network in an authorized manner.

In terms of behavior, the staffs believe that the task of maintaining data security is entirely under the control of the Information Management Division and thus do not take seriously the fact that maintaining ICT security is an individual responsibility. Employees believe that implementing an ICT security policy will increase the workload and limit social freedom. As a result, awareness must address why the policy is important to the users. Most policies require users to take additional steps that may slow or obstruct their work. At the very least, adherence to security policies will necessarily require a change in user routine. Users will be unmotivated to change their routines and will resist attempts to obstruct their work unless they understand how these policies will benefit them.

Furthermore, there is a knowledge gap between the support level and the professional and managerial levels because the awareness program does not reach all levels of the department. Awareness programs are not implemented continuously and are dependent on budget allocations throughout the year. There is still a lack of training. 31.06% of respondents said they had never taken any ICT security courses during their time in the service. As a result, the FDPM should provide adequate security awareness training. Furthermore, the findings stated that only one course on information security awareness had been held during the three years of 2018-2020.

In addition to raising employee awareness of ICT security issues, FDPM should maintain a top-down cyber

security policy. ICT security should be emphasized and communicated throughout the FDPM by leaders. Policymakers should identify and indicate which departments are most vulnerable to cybercrime. With rapidly evolving security threats, maintaining policies is a crippling challenge. As a result, the management team must be foresighted enough to include an imminent threat to data security in the policy. In addition, the policy's scope should be updated and expanded in the future.

5.2 Research Objective 2: To investigate the factors that influence information security awareness.

Information security awareness is the combination of a person's knowledge of security concepts and awareness or consciousness of the existence of an ICT security policy. The study discovered a significant correlation between knowledge, attitude, and behavior, and that each of these factors contributed to the level of awareness about the FDPM ICT security policy. The finding reveals that knowledge and attitudes have a low correlation. Meanwhile, there is a moderate, positively significant relationship between knowledge and behavior, as well as attitude and behavior. On the other hand, the result of the study revealed that employees' awareness level of the FDPM is moderate, with employees lacking knowledge but having a moderate level of attitude and behavior.

Forcht (1988) stated that education is required to raise users' ethical awareness. Changes in attitude are initiated as knowledge accumulates about a relevant behavior. Knowledge leads to a shift in attitude and, ultimately, a shift in behavior. Knowledge was integrated to comprehend the change process, but knowledge increase is not the ultimate factor in behavior change (Newbould and Furnell, 2009). The intention of the person determines the behavior change. Farrior (2005) stated that intention is influenced by two (2) factors. Whereas, the level of intention to act will be higher if the person has a more positive attitude (what the person likes or dislikes) and more of a subjective norm (person's belief about what others think about them) toward the behavior.

■ 6.0 RECOMMENDATION

The level of ICT security policy awareness among FDPM employees has been identified, and the factors that contribute to the level of awareness have been determined. This study made several recommendations for appropriate criteria to improve FDPM employees' information security awareness. Based on the feedback, it proves that ICT security courses have a massive impact on the level of awareness of the FDPM ICT security policy. Generally, there are three (3) main aspects that FDPM needs to be emphasized, especially technology, process, and people which are also similar to the work carried out by Ong Lean Ping (2014). The technological aspect of information can be addressed by implementing or introducing the most recent security software, hardware, network protection scheme, encryption methodology, firewall, or regular penetration test to the system. Second, consider the procedural aspect in the form of checklists, standards, regulatory requirements, or security certification.

The employees need to understand what the policy is; why it is being implemented; and what the implications of the security programs are for the FDPM. Furthermore, on the human side, the level of awareness can be established through security awareness programs, education, monitoring, and ongoing security awareness maintenance within the FDPM. Improving the compliance of employees with ICT awareness training programs is important. In addition, security training may help to protect an FDPM's reputation. In terms of employees' morale, security awareness training programs can educate discreetly, enhancing attitudes and behavior along the way.

To be effective in the long run, the implementation of an information security awareness program necessitates careful planning and preparation. There are four (4) criteria that FDPM needs to take into consideration (PCI DSS, 2014): -

I. Determine the need for Information Security Awareness Programs.
   - To formulate a security awareness team for developing, delivering, and maintaining the security awareness programs.
   - Involvement of top management to encourage security awareness in employees, reinforcing security messages to employees, addressing security-related issues, and setting security expectations.

II. Identify the sources used for the Information Security Awareness Programs.
   - To identify communication channels that are divided into two (2) methods, consisting of electronic communication methods (e.g. email, eLearning, internal social media, etc.) and non-electronic notification (e.g., in-person events, posters, newsletters, internal mailers, and instructor-led training events).

III. Responsibility for developing the Information Security Awareness Programs.

- Information Security Officer (ISO) was responsible for overseeing the implementation of the ICT programs, coordinating incident investigations, and managing corporate-wide awareness.

IV. Development of Information Security Awareness Programs.

- General Training- the FDPM's information security policies, the impact of unauthorized access, office and physical security, virus and password protection, the internet, email, data backup, and recovery.
- Specialized Training-for users who perform specific roles in the FDPM
- To develop metrics to assess awareness training
- To prepare Security Awareness Program Checklist

■ 7.0 CONCLUSION

Based on the findings and analysis, it is possible to conclude that this study archived the objectives, which identified the preliminary level of awareness of FDPM employees about the FDPM ICT security policy. According to the results of the analyses, the level of awareness was moderate. The level of awareness regarding email use, internet use, social media use, and incident reporting was average and needs to be improved. The study discovered that knowledge, attitude, and behavior have a significant relationship and that each of these factors contributed to the level of awareness of the FDPM ICT security policy. As there were only 132 respondents, which may not be the best number of FDPM representatives where it should be representative of all levels of the Department. Therefore, future research can be carried out to obtain a reliable and precise result. It is suggested that further research should look into the ethics of transparency and honesty in data sharing.

REFERENCES

Abdul Rahman A., Muharman L., & Arif R.L. (2015) 'Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures', Procedia Computer Science 72 (2015) 361-373

Ahmad A., Omar E., & Amit D. (2012),'Information Security Policy Compliance: The Role of Information Security Awareness', AMCIS 2012 Proceedings

Ahmad, M. (2015). Malaysia's Approach Against Cyber Threat and Cyber Attacks. CyberSecurity Malaysia. http://ris.org.in/images/RIS_images/presentation.

British Standards (1995) Information Security and ISO 27001 http://www.itgovernance.co.uk

Alan Pike (2019) 'An Evaluation of the Information Security Awareness of University Students' Technological University Dublin

Annual Report Forestry Department Peninsular Malaysia (2019)

Bilal Khan et al. (2011). Effectiveness of Information Security Awareness Method Based on Psychological Theories. African Journal of Business Management Vol.5(26), pp.10862-10868

Bulgurcu et al. (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

Christopher Kuner (2009) 'An International legal framework for data protection: Issues and Prospects'.Computer Law & Security Review 25 (2009) 307-317

El-Haddadeh R.,Tsohou A, and Karyda M. (2012). Implementation Challenges for Information Security Awareness Initiatives in e-Government. European Conference on Information Systems.

Forcht, K A, Pierson, Joan K. Bauman and Ben M. (1988) Developing Awareness Of Computer Ethics. ICIS 1988 Proceedings. https://aisel.aisnet.org/icis.

Farrior M (2005). Breakthrough strategies for engaging the public: Emerging trends in Biodiversity Project. Source: https://www.comminit.com/en/node.

Hannah, N., & Vilasmalar, M. (2014). The Personal Data Protection Act 2010: Challenges to Comply. eSecurity, 36(1), p. 39-40. http:// www.cybersecurity.my/data/content

Jasber K and Norliana M (2013) Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME Conference: Research and Innovation in Information Systems (ICRIIS).

Kruger and Drevin, Steyn (2006) 'A Framework for Evaluating ICT Security Awareness

Kusumawati A (2018). Information Security Awareness: Study on a Government Agency

Conference: 2018 International Conference on Sustainable Information Engineering and Technology (SIET)

Hong Chan, Sameera Mubarak (2012) 'Significance of Information Security Awareness in the Higher Education Sector. International Journal of Computer Application (0975-8887), Vol 60-No.10, December 2012

Mark A, Rezgui YA (2009). Comparative study of information security awareness in higher education based on the concept of design theorizing. International Conference on Management and Service Science

McCormac, Calic, Butavicius et al.(2017) 'A Reliable Measure of Information Security Awareness and the Identification of Bias in Responses'.Australasian Journal of Information Systems 2017.

Malehi Motiei (2012) 'Study on Information Security Awareness among staffs'.Universiti Teknologi Malaysia

Margit SCHOOL (2018) 'Awareness in Information Security', Systematic, Cybernetics and Informatics, Volume 16, No.4 (2018)

Mohd Fairuz Iskandar Othman et al.(2019). 'The level of Information Security Awareness among Academic Staff in IHL' Journal of Telecommunication, Electronic and Computer Engineering

National Security Council, 'Malaysia Cyber Security Strategy 2020-2024.

Ong Lean Ping and Chong Chien Fatt, (2014) 'Information Security Awareness: An Application of Psychological Factors- A Study in Malaysia', International Conference on Computer, Communication and Information Technology. (CCIT 2014)

Parsons K., Malcom P. & Cate J. (2014) 'Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q), Computer & Security.

Pihakainen PA. (2006). Design theory for information security awareness. Doctoral Disertation. Faculty of Science, Department of Information Processing Science, University of Oulu

Puspita K.S, Candiwan, Nurvita T.(2014) 'Information Security Awareness Measurement with Confirmatory Factor Analysis', International Symposium on Technology Management and Emerging Technologies (ISTMET 2014)

Rao F.A, Dominic D.D & Kashif Ali (2020) 'Organizational Governance, Social Bonds and Information Security Policy Compliance: A Perspective towards Oil and Gas Employees

Suhaizimah D and Ali Z (2012) Assessment of information security maturity: An exploration study of Malaysian public service organizations. Journal of Systems and Information Technology 14(1):23-57

SECO Institute. Whitepaper Data Protection Management Framework 2020.

Sekaran, U. and Bougie, R. (2013) Research Methods for Business: A Skill-Building Approach. 6th Edition, Wiley, New York.

Tammyana R, Aristides F., Basic D. et.al. (2020) 'Measuring Information Security Awareness of Client's Information Security: Case Study at PT XYZ, International Journal of Advance in Electronics and Computer Science, ISSN(p): 2394-2835, Vol.7 Issue-7