INFORMATION SECURITY AWARENESS IN CORPORATE GOVERNANCE

Sham Sul Kamal Wan Fakeh, Mohd Sazili Shahibi, Adnan Jamaludin, Wan Ab Kadir Wan Dollah, Muhammad Kharulnizam Zaini, Yamin Kamis, Ahmad Soufien Othman.

Abstract — The matrix analysis of the literature review in this study succeeded in producing factors that contribute to information security awareness. Information security awareness plays an important role in the continuity of an organization. Information security refers to the elements of confidentiality, integrity, and availability, of data or information, in an organization. The research began with definitions of information, information security, and information security awareness, as identified by previous publications. The four independent variables established in this study are policy of information security, education of information security, knowledge of IT, and employee's behaviour towards information security in the workplace. A survey was selected as a research method for the study, and was conducted in order to gain respondent's feedback on the level of information security awareness. The survey findings showed that the level of information security awareness was considered high, but the relation or contribution factors proposed by this study were only slight correlated.

***Keyword*: Information Security, awareness, organization, variables, integrity**

I. INTRODUCTION

These days, many organizations are interconnected through their Information Technology (IT) systems, for an easier and faster sharing of data for work, study, and communications, and many other routine human tasks. This may result in an information security risk for an organization (Solms R. v., 1998). The disruption of information security will kill the main purpose of this sophisticated technology, hinder the smooth operation of an organization, make users feel suspicious and traumatised, and could cause losses to the organizations involved.

Manuscript received May 14, 2014.

Sham Sul Kamal Wan Fakeh, Faculty of Information, University Teknologi (UiTM) Mara Shah Alam, Selangor Malaysia, 019-6038522, 03-79622143 (e-mail: shamsul@salam.uitm.edu.my) **Mohd Sazili Shahibi,** (e-mail: mohdsazili@salam.uitm.edu.my), **Adnan Jamaludin,** UiTM(e-mail: adnanj@salam.uitm.edu.my), **Wan Ab Kadir Wan Dollah** (e-mail: wkadir@salam.uitm.edu.my), **Muhammad Khairulnizam Zaini** (e-mail: nizam0374@salam.uitm.edu.my), **Yamin Kamis** (email: Yamin36@salam.uitm.edu.my) **Ahmad Soufiean Othman** (email: ahmadsoufiean@salam.uitm.edu.my) .

Most of the information on security issues relies on physical devices. The device is used to guarantee the three main elements of information security. They are confidentiality, integrity, and availability. Discussion about these three elements, how equipment can protect data in the system or database, how the firewall protects to prevent outside attacks, how secure are the software or applications used to dispel hackers, and why technology cannot ensure against humans making mistakes. This forms another part of the information security issue, namely information security awareness.

II. LITERATURE REVIEW

According to Boyce & Jennings (2002), security awareness occurs when a user understands the security policies, procedures, and practices, in order for them to make sound judgments when a potential security issue occurs, in the absence of further guidance. Information security awareness focuses more on the motivation of the employee in an organization to follow the policy and regulations towards the security of information in the company. An approach which is often taken to raise awareness is having a program, training, or a seminar in the workplace. The objective of awareness is to minimize human related faults (Siponen M. T., A conceptual foundation for organizational information security awareness., 2000). Several authors state that the motive of information security awareness is to define that term. It is to refer to a state where people in a company are aware of their security mission (Siponen M. T., A conceptual foundation for organizational information security awareness., 2000). For instance, it means that a company wants to secure its confidential information from its competitors. Therefore, employees should not reveal particular information to their opponents; otherwise, the level of awareness amongst staff in that company is not as good as their mission. More disturbing, is the existence of those that are complacent and ignore the issue of information security, until their behaviour leads to information leakage. Either intentionally or unintentionally, information leaks can harm a company. Without trouble, these people do not work hard for the company, hacking and stealing information, with little regard for the people in the

organization itself, and this information falls into the hands of unscrupulous people easily. In 1998, Solms stated that the aim of information security is to ensure business continuity and to minimize business damage, by preventing and minimizing the impact of security incidents. Information protection usually relies on an information security plan and management, which involves humans (Kruger, Drevin, & Styen, 2010). This means that knowledge, education, and awareness, plays a role in the success of information security, to protect information in an organization. For example: When an employee does not logoff from a computer after use, unscrupulous people can steal data from the computer and use it for personal gain or to compete with that particular company. Therefore, this is the effect of a behaviour that does not consider information security matters, or in other words, does not realize the importance information security awareness.

III. RESEARCH FRAMEWORK

One constraint of an organization, which impacts the effectiveness of technologies, is the behaviour of the human beings that administer, use, access, and maintain, information resources (Solms & Solms, 2004; Vroom & Solms, 2004). According to Stanton, Stam, Mastrangelo, & Jolton (2005), appropriate and constructive behaviour by end users, system administrators, and others, can enhance the effectiveness of information security; while inappropriate and destructive behaviour can substantially inhibit its effectiveness. An article by Thomson & Solms (1998) talked about changing human interest for information security awareness program, by using psychological principles that have been ignored by information security practices. Gordon (2010) directly determined the relationship between security awareness and security behaviour in individuals. According to Kruger & Kearney (2006), human behaviour consists of an intention to act in a particular manner. Moreover, maintaining a security-positive behaviour, is a critical element in an effective information security environment. Figure 1: Shows a clear view of the four factors that influence information security awareness in corporate governance.

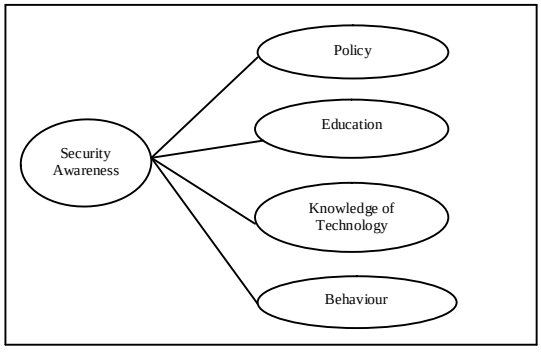

Fig 1: Four factors that influnce awareness

These factors are the main points of understanding, taken from the previous articles, research, and dissertations of several authors. The next paragraph will explain how these factors relate to information security awareness. Policy is a reference for employees. It is a tool for management to guide their subordinates, by educating them based on what the policy states. Education is a communication between user and educator. Education can influence the knowledge of the end user. Knowledge of technology is important, as information is organized and communicated using technology. For instance, an employee must not click any link sent to them, because he/she feels insecure about that link. However, if the link appears frequently, he/she can refer to the IT department for further information. Two right behaviours in this situation are (1) he/she did not click the undefined link, and (2) he/she refers to IT department before ignoring or proceeding to the next action.

IV. RESEARCH METHODOLOGY

Many methods can be incorporated into a social survey. Survey is an approach in which there is empirical research pertaining to a given point in time, which aims to incorporate the widest and most inclusive data possible. A survey is a systematic method of collecting data from a population of interest. It tends to be quantitative in nature, and aims to collect information from a population sample, in such a way that the results are representative of the population, within a certain degree of error. The purpose of a survey is to collect quantitative information, usually through the section examined the information security education of the respondent. The fourth section questioned the knowledge of technology of the respondents, whilst the fifth section attempted to cover the respondent's behaviour characteristics. The final section was about information security awareness. A survey is a systematic method of collecting data from a population of interest. It tends to be quantitative in nature, and aims to collect information from a population sample, in such a way that the results are representative of the population, within a certain degree of error. The purpose of a survey is to collect quantitative information, usually through the use of a structured and standardized questionnaire. Questionnaires are cost effective compared to face-to-face interviews. This is especially true for studies involving large sample sizes and large geographic areas. Written questionnaires become even more cost effective as the number of research questions increases. Questionnaires are familiar to most people and easy to analyse. Nearly everyone has had some experience completing questionnaires, and generally, they do not make people apprehensive. Questionnaires reduce bias. There is a uniform question presentation and a no middle-man bias.

V. DATA ANALYSIS

A numerical index, known as correlation coefficient, expressed the degree or magnitude of the relation. The numerical index +1.00 is the highest possible value that the correlation coefficient can assume and indicates a perfect

relationship between variables (Burn, 2000). Table 1 shows a guide to the degree of relationship indicated by the size of the coefficients.

Absolute Value of Correlation Coefficient	Remarks on Correlation (rho)	Nature of Relationship
0.90 - 1.00	Very high correlation	Very strong relationship
0.70 - 0.90	High correlation	Marked relationship
0.40 - 0.70	Moderate correlation	Substantial relationship
0.20 - 0.40	Low correlation	Weak relationship
Less than 0.20	Slight correlation	Relationship so small as to be negligible

TABLE 1: Data of Degree Correlation Coefficient

Table 2, "Is the policy regarding information security awareness one of the factors influencing information security awareness?" The first question asked about the existence of a security team in the organization. The results revealed that 75.0 percent of the respondents' said yes, 25.0 percent were not sure, and none of the respondents said no. Some organizations allow any website to be retrieved either during or after office hours. However, some organizations, such as libraries (though not all libraries), have a policy and restrictions to not enter certain groups of websites. For instance, no access is allowed to social networks or pornography in the work place using the organization's facilities, including networks. When asked about whether the respondents had policies on which websites were allowed, 66.7 percent of the respondents answered yes; another 16.7 percent answered no, and the rest were unsure. In terms of guidelines regarding information security in the respondent's work place, the majority (65.0 percent) answered yes, while 18.3 percent were unsure, and the rest (16.7 percent) said no.

Elements	No	Not Sure	Yes	Total
We have a security team in this organization	0.0	25.0	75.0	100
I know who to contact if my computer is hacked or infected	0.0	6.7	93.3	100
The firewall on my computer is always enabled	8.3	0.0	91.7	100
My computer is configured to automatically update	16.7	8.3	75.0	100
I have policies on which websites I am allowed to visit	16.7	16.7	66.7	100
There are guidelines regarding information security in my workplace	16.7	18.3	65.0	100

TABLE 2: Policy Factors Influencing Information Security Awareness Frequency

Using a scale of one (no), two (unsure), and three (yes), the overall data was summarized in Table 3. The ranking is performed by comparing means with other variables. The highest mean is ranked as one, and so on. The findings show that the most significant factor fell under the knowledge of who to contact if a computer was hacked or infected. After that, the firewall on the computer is always enabled ranked second, and guidelines regarding information security in the workplace ranked last.

Element	Mean	Std. Deviation	Rank
I know who to contact if my computer is hacked or infected	2.9333	0.25155	1
The firewall on my computer is always enabled	2.8333	0.557744	2
We have a security team in this organization	2.7500	0.43667	3
My computer is configured to automatically update	2.5833	0.76561	4
I have policies on which websites I am allowed to visit	2.5000	0.77021	5
There are guidelines regarding information security in my workplace	2.4833	0.77002	6

TABLE 3: Policy Influencing Information Security Awareness Analysis

"Is education regarding information security one of the factors influencing information security awareness?" Table 3 shows that 65.0 percent of the respondents answered that they knew what a phishing attack was, whilst 20.0 percent of the respondents answered no, and the rest (15.0 percent) were unsure. As shown in the Table, 8.3 percent and 6.7 percent of the respondents answered no and unsure about what to do if the computer was infected with a virus, and the rest (85.0 percent) knew what to do. About 53.3 percent of

the respondents answered no, for the element never finding a virus, 40.0 percent said they never found a virus, and less than 6.7 percent of the respondents answered that they were unsure whether they had found a virus or not. A total of 33.3 percent of the respondents were unsure about the value of their computer to the hackers, 46.7 percent said yes, and 20.0 percent said no for this element.

Elements	No	Not Sure	Yes	Total
I know what a phishing attack is	12 20.0%	9 15.0%	39 65.0%	60 100.0%
I know what to do if my computer is infected with a virus	5 8.3%	4 6.7%	51 85.0%	60 100.0%
I never found a virus or a Trojan on my computer at work	32 53.3%	4 6.7%	24 40.0%	60 100.0%
My computer has no value to hackers, they do not target me	12 20.0%	20 33.3%	28 33.3%	60 100.0%
I always download and install software on my computer at work	35 58.3%	5 8.3%	20 33.3%	60 100.0%
I do not sharing my work password	11 18.3%	4 6.7%	45 75.0%	60 100.0%
I receive training about information security in my workplace	36 60.0%	9 15.0%	15 25.0%	60 100.0%

TABLE 4: Education Factors Influencing Information Security Awareness Frequency

The overall response of respondents about education as a factor in information security awareness is summarized in Table 4 and Table 5. As can be seen from the table, the action for when a computer is infected with a virus; was found to be the most important factor in education. This was followed by not sharing passwords and knowing what a phishing attack was. The lowest score was about training received.

Element	Mean	Std. Deviation	Rank
I know what to do if my computer is infected with a virus	2.7667	0.5980	1
I do not share my work password	2.5667	0.78905	2
I know what a phishing attack is	2.4500	0.81146	3
My computer has no value to hackers, they do not target me	2.2667	0.77824	4
I never found a virus or trojan on my computer at work	1.8667	0.96492	5
I always download and install software on my computer at work	1.7500	0.93201	6
I receive training about information security in my workplace	1.6500	0.86013	7

TABLE 5: Education Influencing Information Security Awareness Analysis

Since IT knowledge was mentioned in the literature review as being one of the causes of information security awareness amongst employees, respondents were asked five questions related to the elements of IT knowledge (as shown in Table 6). The respondents were asked about antivirus usage. The results show that 91.7 percent of the respondents answered that they knew how to handle antivirus software and 8.3 percent of the respondents were unsure. Next, the respondents were asked about the risk of opening emails from unknown senders. The majority of the respondents (90.0 percent) knew the risk of opening these emails, 8.3 percent of the respondents were unsure of the risk, and only 1.7 percent had no idea at all. Based on these results, more than 60.0 percent of the respondents knew what an email scam was, and how to identify it. Meanwhile, 31.7 percent of the respondents were unsure. In the last question of the IT knowledge section, respondents were asked about knowing how to use antivirus software and how to scan for viruses. All of the respondents knew how to use it, thus making a response of 100 percent.

Elements	No	Not Sure	Yes	Total
I have installed, updated, and enabled, antivirus software on my computer	0 0.0%	5 8.3%	55 91.7%	60 100.0%
I know what the risk is when opening e-mails from unknown senders; especially if there is an attachment	1 1.7%	5 8.3%	54 90.0%	60 100.0%
I know what an email scam is and how to identify it	0 0.0%	19 31.7%	41 68.3%	60 100.0%

I know how to use antivirus software and how to scan for viruses	0 0.0%	0 0.0%	60 100.0%	60 100.0%

TABLE 6: Knowledge of IT Factors Influencing Information Security Awareness Frequency

The analysis of this section tries to find answers for the fourth research question. The research question looks at the elements of behaviour amongst employees as one of the influencing factors in information security awareness. In this section, respondents were asked several questions about the behaviour that will most likely influence information security awareness. The questions were asked with the purpose of identifying whether the behaviour factor is significant to information security awareness. The results of this analysis can be seen in Table 7. Table 10 demonstrates that about 81.7 percent did not take information from the office to their home to work on. About 18.3 percent of the respondents did do that. Further analysis was performed to look at the respondent's responses to the statement that their organization's PC was safe. The table indicates that 65.0 percent of the respondents felt that their organization's PC was safe, while less than 20.0 percent answered no. Another 15.0 percent of the respondents were unsure.

Elements	No	Not Sure	Yes	Total
I'll make sure that when I delete a file from the computer or USB stick, that the information is recoverable	5 8.3%	23 38.3%	53 53.3%	60 100.0 %
I do not share my work password	9 15.0%	0 0.0%	51 85.0%	60 100.0 %
I use the same password on my work and personal accounts	48 80.0%	5 8.3%	7 11.3%	60 100.0 %
I never give my work password to someone else	1 0.0%	4 6.7%	55 91.7%	60 100.0 %
I often take information from the office and use a computer at home to work on it.	49 81.7%	0 0.0%	11 18.3%	60 100.0 %
I feel that my organizations' PC is safe	12 20.0%	9 15.0%	39 65.0%	60 100.0 %

TABLE 7: Frequency analysis of the Employees Behaviour Element

Table 8, shows the distribution of the overall opinions by respondents on the behaviour element as a factor of information security awareness. It was found that respondents slightly accepted all factors that were asked of them. They treated all elements of the behaviour factors as being less important.

Element	Mean	Std. Deviation	Rank
I never give my work password to someone else	2.9000	0.35415	1
I do not share my work password	2.7000	0.72017	2
I feel that my organizations' PC is safe	2.4500	0.81146	3
I'll make sure that when I delete a file from the computer or USB stick, that the information is recoverable	2.4500	0.64899	4
I often take information from the office and use a computer at home to work on it	1.3667	0.78041	5
I use the same password on my work and personal accounts	1.3167	0.67627	6

TABLE 8: Analysis of the Elements of the Employees Behaviour Factor

VI. CONCLUSION

Since information security importantly ensures that business process continuity in an organization runs smoothly and without interference, information security awareness is considered as being vital to the organization. Policy is constructed and implemented within organizations.

Employees are educated during seminars, awareness programs, training, and campaigns. Knowledge of IT is also important in order to avoid misuse of IT devices, which leads to the lack of information security. Finally, employee behaviour is interrelated with awareness of information security in the workplace. Good behaviour towards information security practices can also influence information security awareness. However, analysis of the data gained from the survey needs to be improved, because the correlation coefficient analysis in the tables show above a slight correlation; meaning that the relationship is so small, as to be negligible.

REFERENCES

[1] Ahmad, A.M (2010). Information security governance in Saudi organizations: an empiral studhy. Information Management & Computer Security, 18 (4), 226-276.

[2] Blyth, A., & Kovacich, G. (2006). Information assurance: Security in the information. Cambridge: Spriger.

[3] Burn,R.B.(2000).Introduction to research method.Australia: Longman

[4] Caroll, M.D. (2006). Information security: Examining and managing the insider threat. ACM Proceeding of the 3rd Annual Conference on Information Security Curriculum Development 2006. Kennesaw.

[5] ENISA. (2006). A users' Guide: How to raise information security awareness. Retrieved March 17, 2012.

[6] Gross, J.B, (2008). Looking for trouble: ACM Proceedings of the 2008 Human Interaction for the Management of Information Technology. (p.10) Cambridge. MA.

[7] Kruger, H.A., & Kearney, W.D.(2006). A Prototype for assessing information security awareness. Computer & Security, 25, 289-289.

[8] Saint-Gemain, R. (2005). Information security management best practice based on ISO/IEC 17799. Information Management Journal, 39 (4), 60-65.

[9] Stroub, D.W. (1990). Effective IS Security: An Empirical Study. Information System Research, 1 (3), 255-276.

[10] Takemura, T. (2011), A Quantitative Study on Japenes Workers' Awareness to Information Security Using the data collected by Web based survey, American Journal of Economics and Business Administration, 20-26.

[11] Theiss, H. (1983). On Terminology. Information Science in Action: System Design, 1,84-94.

[12] Thomson, M.E., & Solms, R.v. (1998). Information security awareness: educating your users effectively. Information Management & Computer Security, 6 (4), 167-173.

[13] Tipton, H.F., & Krause, M. (Eds.) (2004). Information Security Management Handbook (5th Edition ed.) U.S.A: CRC Press LC.

[14] Vroom, C., 7 R.v. Solms, 2004. Towards information security behavioral compliance. Computers & Security, 23(3): 191-198.

[15] Whitman, M.E., & HJ. Mattord, 2005. Principles of Information Security (2nd Edition ed.). Australia: Thomson course Technolgy.

Sham Sul Kamal Wan Fakeh, received of Master of Science in Information Management from University Teknologi Mara. Area of Interest: Multimedia Application, Information Content & Management, Information System Management. (UiTM).

Prof Madya Dr, Mohd Sazili Shahibi, received PhD in area of Information System Management from University of Malaya (UM).

Prof Dr, Adnan Jamaludin, received PhD in area of Strategic Information Management (USM).

Prof Madya Dr, Wan Ab Kadir Wan Dollah, received PhD in area of Library (UM).

Muhammad Khairulnizam Zaini, received of Master of Science in area of Information System Management. (UiTM).

Yamin Kamis, received of Master of Science in area of Information System Management, (UiTM)

Ahmad Soufiean Othman, received of Master in Information System Management, Progress study PhD in area Strategic Planning.