The Level of Information Security Awareness among Academic Staff in IHL

Mohd Fairuz Iskandar Othman[1], Fayez Alqahtani[2], Md Ahsanul Bari[1], Ahmad Naim Che Pee[1],
Yahaya Abdul Rahim[1], Hamzah Asyrani Sulaiman1[1]

[1]Human Centered Computing - Information Systems Lab (HCC-ISL),
Centre for Advanced Computing Technology (C-ACT)
Faculty of Information and Communication Technology (FTMK), Universiti Teknikal Malaysia Melaka
Hang Tuah Jaya, Durian Tunggal 76100, Melaka, Malaysia
[2] Computer Science Department, King Saud University, Riyadh, Saudi Arabia
mohdfairuz@utem.edu.my

***Abstract*— IS security awareness plays a significant role in the process of the overall information security of any organisation. Based on an empirical study of 368 academic staff in three institutions of higher learning (IHL), we found that the level of information security awareness can be considered good, but it can certainly be improved further. Employees need further training in this area mainly at institutions which only recently received the ISO/IEC 27001:2013 certification. Our sample seems to suggest that demographics such as the age of the respondents contributed to their information security risk tolerance and adherence behaviour.**

***Index Terms*—Information Security Awareness (ISA); ISMS; Risk; Institutions of Higher Learning (IHL).**

I. Introduction

Most organisations' functioning greatly relies on corporate information systems (IS). Thus, managing risk associated with security threats is getting increasingly important since violations of information security often have serious financial and reputational consequences for companies and their customers [1]. Ensuring information security has become one of the major priorities and challenges for organisations. Consequently, academia and businesses are interested in how information system security (ISS) threats can be reduced effectively [2]. Prior research on ISS was mainly focused on technological issues such as encryption technology, spyware and virus detection, or firewalls [3].

For many organisations, people, and not technology, have become one of their greatest security risks. People, just like computers, store, process and transfer information. Many organisations do little to secure and protect their human resources, exposing the organisation to varying levels of risk. The purpose of this survey is to help quantifiably measure the human risk they are exposed to. The results of this survey can then be used to establish a human risk baseline, can be used to compare progress over time, or can be used by organisations to compare their level of human risk to other organisations in their industry.

IS security awareness plays a significant role in the process of the overall information security of any organisation [4]. The important role of the human factor in IS security has been recognised by both the research community and IS security practitioners [5]. As such, users' IS security awareness is reflected in their attitudinal and behavioural patterns [6]. However, these attitudinal and behavioural features had a socio-cultural and human dimension that needs to be analysed and understood to ensure full users' commitment and adherence to IS security regulations.

The research explores the level of information security awareness of academic staff, in institutions of higher learning within the context of an emerging economy, Malaysia. Related work is first given, followed by an overview of the methodology that underpins the research. A comprehensive analysis of the results is provided, followed by an in-depth discussion. Finally, the paper concludes with a set of recommendations to initiate and promote IS security awareness in the studied environment.

II. Literature Review

A. *Information Security Awareness*

According to [7] ISA is defined as an employee´s general knowledge about information security and his cognisance of the information security policy in the organisation. ISA is composed of general information security awareness and policy awareness. Since ISA plays such a pivotal role in lowering information security risks its increase in organisations is essential.

Information security is related to the protection of data, which are stored either in the form of symbols, writing or by other communication, information technology and other electronic systems. Information security requirements can be divided into three categories:

a) Physical security is a protection against any threats occurring in the physical space; its major parts are the protection against natural disasters, mechanical protection, electronic signalling system, manned security, access control systems, surveillance systems, the power supply, the protection against radiated and conducted interference, air-conditioning and fire protection.
b) Logical protection is a form of protection implemented in the electronic information systems with information technology tools and procedures (programs, protocols).
c) Administrative protection is composed of organisational, regulation and control measures, supplemented by regular education on protection procedures (in relation to the adequacy of management systems). In order to achieve the appropriate level of

information security and maintenance, it is needed to look beyond the physical and logical protection, and we have to manage the threats caused by the human factor as well. These threats can be traced back mainly to the lack of necessary knowledge and the low level of the awareness of the cause and effect relationships related to the information processing activities.

There is a conceptual understanding in the literature that both compliance and motivation of users/employees/civil servants can be achieved by raising policy awareness, systematic enforcement and regular maintenance of technological and human procedures [8]. Derived from this logic, our unit of analysis are the user and his/her information security awareness (ISA) since ISA is a key element of all security policies [7].

B. Research Gap

The number of scientific studies that consider IS security awareness in developed countries, especially in higher education environments, is very limited [9]. The situation is even more dire in the case of developing countries where the socio-cultural environment combined with a lack of resources and knowledge may present even more barriers to promote IS security awareness. The proposed research contributes to the body of knowledge by addressing these identified gaps.

III. Research Methodology And Data Collection

Our research design is based on the SANS model and questionnaire which was created by information security experts in the US in 2012 [10].

This survey consists of 25 questions, divided into three parts:

- *Demographic questions*: in addition to the most important demographic data (e.g. gender, year of birth, education level, income status), the respondents' IT skills were also questioned.
- *Questions on the workplace*: type of IHL, years working at the IHL.
- *Questions on information security awareness were centred around the following issues*: work organisation and regulation, everyday use of skills related to information security, the use of IT tools and data management, general computer usage habits.

The questionnaire is aimed at measuring everyday user habits, assessing them by giving scores ranging from 1 to 5.

Some of the question responses indicate strong awareness and good security practices while others indicate weak awareness, negligent behaviour, or high-risk activities. Based on these differences, each question response in this survey (except for the first question) has been assigned a risk value (1-5). "One" is the lowest risk value and "five" is the highest risk value. When the results of the survey have been collected, they can be used to determine the overall risk score or risk level of the organisation.

a) Add the total risk values from each survey to determine the cumulative total for the organisation.
b) Divide the survey cumulative response total by the number of survey takers to calculate the survey (or organisation's) risk score.
c) Using the risk score, check the "Risk Levels" table below for the organisation's general risk rating.

Based on the aggregated scores, the respondents are classified into five risk categories (refer to Table 1):

- Low: It is typical of the employees belonging to the first category that they are aware of the security principles as well as the dangers, they are well-educated, their everyday behaviour meets workplace safety rules and guidelines.
- Elevated: Employees found in the second category participated in some information security training, they are also aware of the dangers but do not fully follow the relevant safety principles and rules.
- Moderate: Representing the group of average risk, those employees come under the third category, who are aware of the dangers and know that they should keep some basic safety principles but they are in need of further education on the subject. They do not recognise IT incidents and do not know what to do in such cases.
- Significant: The employees included in the fourth category are neither aware of the dangers and safety principles nor the security regulations in their organisation.
- High: Finally, employees belonging to the fifth category are not aware of the dangers and do not comply with the security regulations, either.

An online questionnaire was designed to collect data carefully. The survey questionnaire was delivered via email links. The data was collected from the academic staff of each university using random sampling, resulting in a total of 368 usable samples being successfully obtained.

Table 1
Risk Levels and their Description

Risk Levels	Description
Low (25 – 39)	Users are aware of good security principles and threats, have been properly trained, and comply with all organisational security standards and policies.
Elevated (40-60)	Users have already been trained in organisational security standards and policies, they are aware of threats, but may not follow good security principles and controls.
Moderate (61 – 81)	Users are aware of threats and know they should follow good security principles and controls, but need training in organisational security standards and policies. They also may not know how to identify or report a security event.
Significant (82 – 96)	Users are not aware of good security principles or threats nor are they aware of or compliant with organisational security standards and policies.
High (97 – 120)	Users are not aware of threats and disregard known security standards and policies or do not comply. They engage in activities or practices that are easily attacked and exploited.

IV. Results And Discussion

From the responses received, 84% of the respondents were male, and 16% were female. Table 2 shows a summary of the respondent information. Most of the respondents have been working at their respective IHL for 3-5 years.

Table 2
Summary of Respondent Information

IHL	No. of respondents	Respondent median age	ISMS (ISO/IEC 27001:2013) certified? (year)
A	145	34	Yes (2014)
B	108	47	Yes (2015)
C	115	45	Yes (2016)

University A is a technical or focus university. Focus universities are institutions that pay attention to specific fields such as technical, education, management and defence. University A risk level was **Elevated**.

University B is a research university. A research university seeks to participate in new adventures of ideas actively, experiment with innovative methods, and take intellectual initiatives to discover further and expand the frontiers of knowledge. The focus is on research activities and teaching based on research and development (R&D). University B obtained a risk level of **Moderate**.

University C is a comprehensive university. Institutes recognised as comprehensive universities offer courses in various fields of studies for all levels of education including pre-undergraduate, undergraduate, and postgraduate degrees. University C risk level was **Moderate**.

It is interesting to note that all universities involved in the survey were certified to Information Security Management Systems (ISMS-ISO/IEC27001). This is according to the Malaysian Cabinet Directive (February 2010) that states that all Critical National Information Infrastructure (CNII) entities must be ISMS certified within three years. These CNII entities must ensure that the certification scope covers the information security management in the operating areas that deliver their critical services and products to the nation (national economy and public).

Certified organisations have shown to establish a systematic approach to protect especially sensitive information from wide range of threats to ensure business continuity, minimise business damage due to attacks, leakages and natural disasters, maximise return on investment and business opportunity. It encompasses people, processes and information technology systems. In the context of this standard, the term information includes all forms of data, documents, messages, communications, conversations, recordings, and photographs.

A. Interpretation of data

Based on the results, it appears that the majority of respondents have a reasonable knowledge of threats such as computer viruses and trojans. With regards to phishing, it was quite surprising that 20% indicated that they do not know what the term means. There were a high number of respondents who were willing to give their passwords away under certain circumstances.

Owing to paper length constraints, not all results can be discussed here. The results do show that the survey questionnaire and the accompanying risk level descriptions can make a definite contribution in helping to identify the level of risk as well as to identify specific areas for security education.

In the case of this study, it was quite apparent that the relevant authorities should focus their attention on explaining terms like phishing that are not common knowledge to the layman. Furthermore, the awareness program should inculcate users of the dangers of using the same passwords for all their different applications. Only a small portion of the awareness program should then be dedicated to aspects such as computer viruses.

V. Conclusion

In this paper, we intended to identify the level of information security awareness in three IHL in Malaysia. Generally, the overall picture shows that IHLs are taking positive actions to increase the level of awareness of their users.

A. Limitations and Avenues for Future Research

There are several limitations to this study that create opportunities for further research. First, since this survey was administered online, the respondents were self-selected among academic staff. Second, It was also limited to academic staff of only three Institutions of Higher Learning (IHL) in Malaysia. Therefore, these results are the only representative of the state of awareness and security practices in certain populations of users at these IHLs.

B. Recommendations

The following are recommendations for the respective risk levels identified:

Elevated

- Practice reward and punishment. It is important to monitor performance and advertise reward and punishment of IS conduct or misconduct. This is necessary not only for reinforcement but also to illustrate the level of commitment of the organisation to it is IS security. Previous research has shown that intrinsic and extrinsic motivations influence information security behaviours [11].

Moderate

- Train users on IS security best practices to increase their awareness. Training should be regular. Basic level training should be mandatory for all users. It is also recommended that training should be included in the induction program for new hires and new students. The establishment of training ensures that users are informed and can be accounted liable for IS misconduct. It is also important that the message and materials of IS training are the same regardless of who the trainer is.
- Campaign IS security awareness best practices and advertise IS security training sessions and materials. It is also important that these messages reach as many users and allow enough time for users to participate.

Acknowledgement

This research was supported in part by UTeM and TRGS grant (TRGS/1/12014/FTMK/02/2/D00002).

References

[1] H. Cavusoglu, B. Mishra, and S. Raghunathan, "A model for evaluating IT security investments," *Communications of the ACM,* vol. 47, pp. 87-92, 2004.

[2] J. D'Arcy, A. Hovav, and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach," *Information Systems Research,* vol. 20, pp. 79-98, 2009.

[3] J. L. Spears and H. Barki, "User participation in information systems security risk management," *MIS quarterly,* pp. 503-522, 2010.

[4] M. E. Thomson and R. von Solms, "Information security awareness: educating your users effectively," *Information management & computer security,* vol. 6, pp. 167-173, 1998.

[5] M. T. Siponen, "A conceptual foundation for organizational information security awareness," *Information Management & Computer Security,* vol. 8, pp. 31-41, 2000.

[6] P. Puhakainen and R. Ahonen, "Design theory for information security awareness," 2006.

[7] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *MIS quarterly,* vol. 34, pp. 523-548, 2010.

[8] K. J. Knapp and C. J. Ferrante, "Policy awareness, enforcement and maintenance: Critical to information security effectiveness in organizations," *Journal of Management Policy and Practice,* vol. 13, p. 66, 2012.

[9] A. Marks, "Exploring universities' information systems security awareness in a changing higher education environment: A Comparative Case Study Research," PhD, University of Salford, 2007.

[10] T. Bond, C. Stephens, and D. Piscitello, "Security Awareness Survey," 2012.

[11] T. Herath and H. R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decision Support Systems,* vol. 47, pp. 154-165, 2009/05/01/ 2009.