INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 7, Issue 9, (2017) E-ISSN: 2222-6990

Information Security Challenges: A Malaysian Context

Adnan Rizal Haris@Harib, Suhaimi Sarijan and Norhayati Hussin

Faculty of Information Management
Universiti Teknologi MARA, Puncak Perdana Campus
40150 Shah Alam, UiTM Selangor, Malaysia

DOI Link: http://dx.doi.org/10.6007/IJARBSS/v7-i9/3335

Published Date: 21 September 2017

Abstract

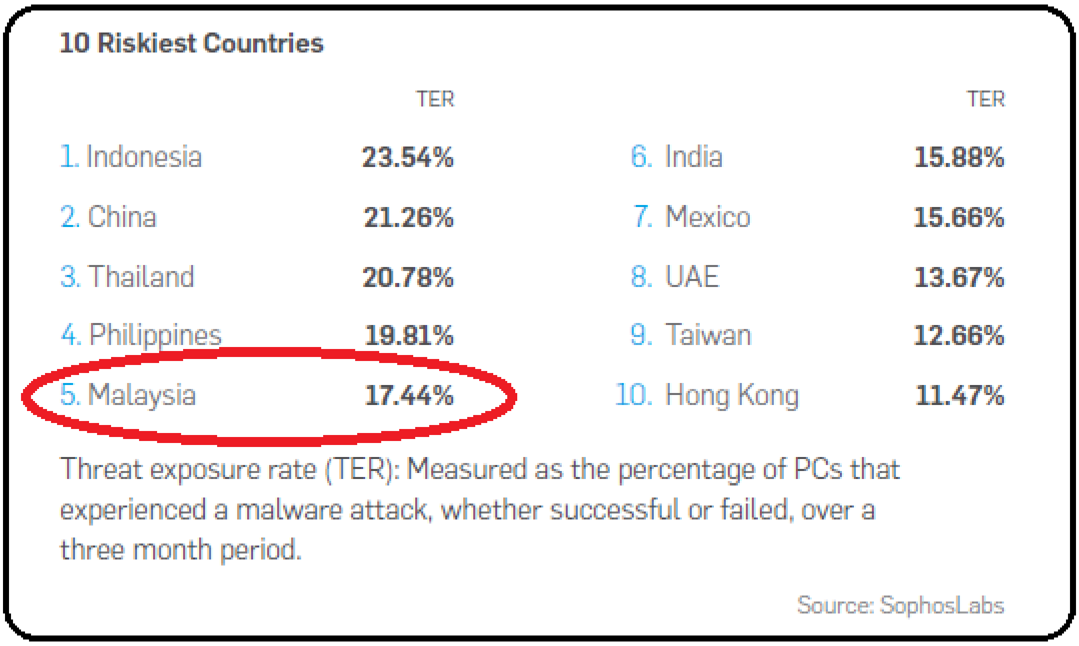
Information security sometimes known as Cybersecurity is the practice or action taken to prevent unauthorized access, use, disclosure, disruption, modification or destruction towards information. The cybersecurity is a concern for all. Data centres play important roles in managing data and information of an organization. Digital technology has become most important key to increase the level of innovation, competitiveness and growth. The economy sector is depending on effective measures to protect information in organization. Information plays an important part in giving services to people. At the same time, problems of intruders or attackers that we might not run away from it. In Malaysia, the CyberSecurity Malaysia is the agency dealing with defending the nation from cyber-attacks. Several functions initiated by the body to educate internet users and to prevent from attacks.

Keywords: Information Security, Cyber Security, Online Information, Malaysia

1.0 Introduction

Living in the digital age today could be so easy and meaningful if there is no any disruption from other parties. We might connect each other using internet and exchange information via technology devices. Users are not aware during transferring data in the internet, they are been watching by cyber attackers. In organization, information technology (IT) is a lifeline despite of their size and nature of business From this situation, information security crime is not a concern for nation level, but it related to individual, business and non-business organizations (Sameera, 2016). From this statement, the priority in giving security to information has becoming heavily important. The organization should implement policy in securing information and data. The policy should be written so that it can circulate among members of the organization on the important of keeping information safe.

In Malaysia, people are aware of the risks of cyber-attacks, but they are not doing anything to protect themselves from being attack. Referring to *Norton Cyber Security Insights Report*, complacency is the foremost reason on why Malaysians are easily becoming target to cybercrime. The cyber attackers see new technology introduced in the Internet as their opportunity to attack users especially on mobile devices. Malaysians has becoming among those who use Internet as the communication medium. Resulting from this point, Malaysia also listed as the most common target for cyber attackers. Image below shown Malaysia is at number five (5) for most vulnerable to cybercrime:



10 Riskiest Countries

	TER		TER
1. Indonesia	**23.54%**	6. India	**15.88%**
2. China	**21.26%**	7. Mexico	**15.66%**
3. Thailand	**20.78%**	8. UAE	**13.67%**
4. Philippines	**19.81%**	9. Taiwan	**12.66%**
5. Malaysia	**17.44%**	10. Hong Kong	**11.47%**

Threat exposure rate (TER): Measured as the percentage of PCs that experienced a malware attack, whether successful or failed, over a three month period.

Source: SophosLabs

Figure 1. Malaysia rank sixth in most vulnerable to cybercrime

From above listing, we could define that Asian countries are most targeted location for cyber-attacks compared to western countries. Types of threats that usually exist are cyber bully, phishing, email scam, ransom ware, digital pirate, hackers, online banking etc. Phishing could be defined as "*…the fraudelent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information such as passwords and credit card numbers*" (Oxford Online Dictionary). Phishing seems to be an effective way for the cybercrime to occur. This resulted to most Malaysians are unable to identify phishing emails and they experienced bad outcomes. The new update in the news recently is about ransomware attack called 'WannaCrypt'. Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid. CyberSecurity Malaysia reported that this attack could lead to temporary or permanent loss of information and reputation of organization. Statisitics of the reported incidents has been produced by them is illustrated in the chart below:

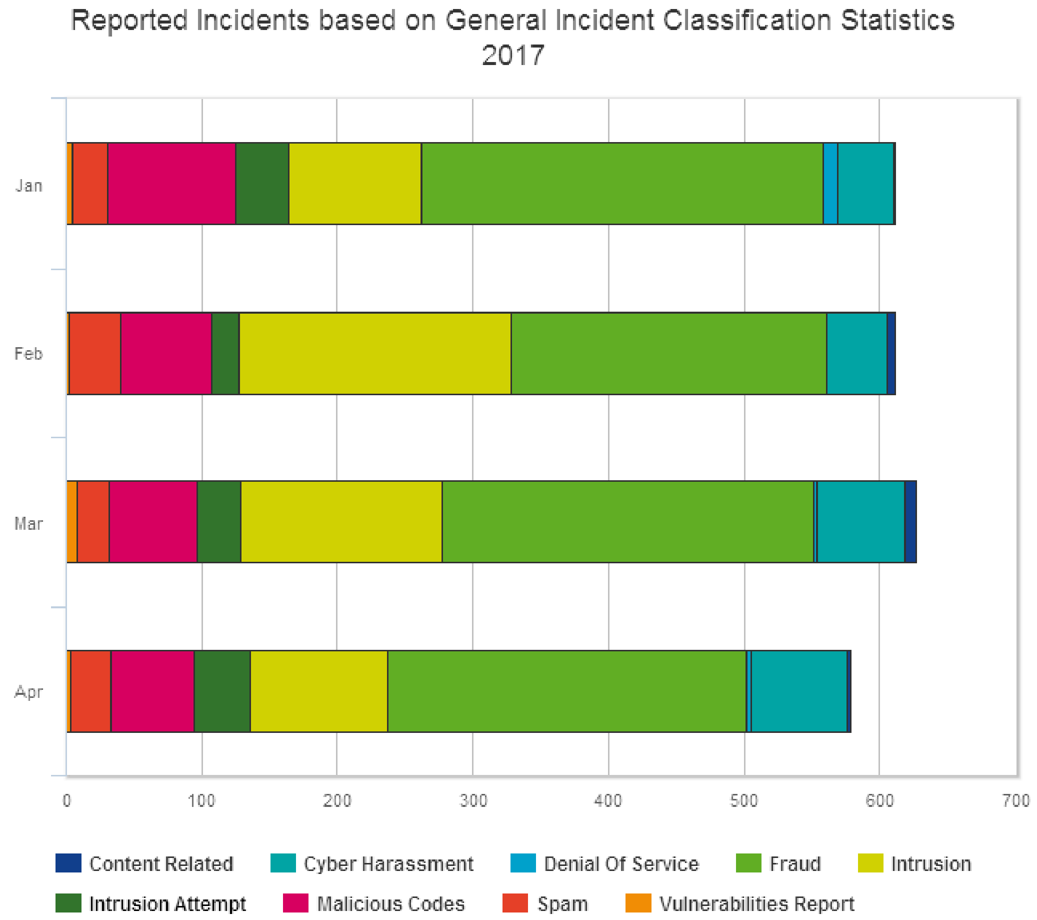


Figure 2. Report on cyber attacks in 2017

In the information security issue, there is a security standard that has been recognizing widely. It is the ISO 27001. The standard specifies the requirements for the Information Security Management Systems in keeping an organization from cyber-attacks. There are benefits in implementing the standard:

- Ensure controls are in place to minimize risk of security threats
- Improve organization image and build better reputation.
- Improve business profits
- Provide competitive advantage and market differentiation.
- Demonstrate capability without revealing security processes.
- Comply with legislation
- Clear channels and communication

This standard could be obtained from certified provider in which analysis will be done through the framework and according the requirement of the organization.

2.0 Literature Review

Information security management is concerned with ensuring organization business continuity and preventing the impact of security incidents that threaten information of the organization. Fenz et al. (2014) agreed with the information security is important but the challenges is to prove the factors contributing to problem itself. Due to that statement, securing corporate information from outsiders is becoming strictly important (Mitchell, Marcella & Baxter, 1999). Organization cannot deny the situation occurs nowadays due to internetworked world. These challenges and situation occurred because the easiness to access the digital data and information deployed by organization. This resulted an organization face serious challenges as more people providing easy data access (Jun, Punit & Kai, 2014). On other side, Kim (2014) voices his concern that information security awareness training could provide training and at the same time, awareness on how serious is the information security protection.

Electronic commerce is one of the new emerging business styles in the digital age. By using the Internet as the platform of the business communication, the risk of being attack by hackers or cyber troop is high. According to Labuschagne (2000), trading over the internet could incur business and technology risks. It is result from the technology and devices that been used to do the transactions online. Study by Sazili, Juwahir & Khairulnizam (2011) found that electronic commerce is a faceless business activity that does not require a physical location. The risk of being attack is always there since this transaction is connected with online banking system.

Furthermore, when discussed on the information security, there are several terms could be interconnected to the security of information or cyber. Some terms appeared are phishing, email scam, fraud etc. Refer to Mustaffa (2015), CyberSecurity Malaysia has managed more than 57,000 incidents from 1997 to 2014. These incidents include intrusion, fraud, cyber harassment, spam and malicious code. This was supported by Suhazimah & Ali (2011) in their research, because of the fact that information security is a complex, dynamic and multifaceted discipline in which no single component may be ignored, the effective management of this discipline is essential for any organization wishing to survive and thrive in the information age. In other words, it is mandatory action to taken by organization in ensuring their data and information

3.0 Discussions And Opinions

In Malaysia, to fight against the cyber attacks, the CyberSecurity Malaysia has implemented the National Cyber Security Policy in which the policy is to strengthen the defence of the country. The vision of the policy is make the infrastructure is in secre, resilient and self-reliant. Referring to paper done by Mustaffa (2015), another effort exist by the body is organizing the Internet Safe Day in 2015. The main purpose of his event is:

"To promote Internet safety, nurturing and increasing public awareness on cyber security especially amongst children and young people across the world so that they become more responsible when using technology and digital gadgets such as smart phones and tablets"

The Malaysian Government has introduced the Personal Data Protection Act in May 2010 and came into force in 2013, where the act is a written policy with the objective to protect personal data of individuals with respect to commercial transactions. In research done by Hannah & Vilasmalar (2014), they described personal data is regarded as any information related to an individual's identity, characteristics, behaviour of the individual that is identified and could be accessed from the information and database. It also includes any expression of opinion about an individual. This act could be somewhat protection to internet users if there are unwanted attacks came.

Following that, one new issue or term that has been discussed lately is the digital detox. In the article published in The Star (5 May 2017), the writer expressed his opinions that could be the best way to avoid spammers and cyber attacks. What does digital detox means here is a period of time where a person is refrains to use electronic connected devices such as smartphones or computers. Some benefits could be benefits from digital detox:

- Increase mental health
- Improving human relationships
- Good posture
- Increased productivity

A closer look at the literature review that mostly concern on the security of information in an organization. Phishing and email scams cases are discovered to be the most attacks experienced by internet users. This was supported by Mustaffa (2015) in which CyberSecurity is producing data and report on the attacks. Ransomware has been another attack when the software attacks two Malaysian companies recently (The Star, 16 May 2017). The malware attacked a director of a company and a automotive shop somewhere in Klang Valley. The Sun (16 May 2017) reported that automated teller machines (ATMs) could be the target of hackers in the near future.

4.0 Conclusion

To conclude on this issue, individuals and organization should realize the important of keeping information safe. Information Security has become a priority concern among information technology practitioners and that concern when shared by management, will benefit an organization as a whole. Top-down management support is critical for the survival of the initiative and its goal of creating a culture of security awareness within the organization. All members of the organization should play and response to whatever condition in securing from cyber-attacks. To this end, to ensure the information to be more secure, any personal data should not be exposed online.

5.0 References

Mohsen, A. S. (2017, May 16). WannaCry Ransomware: You Are at a Risk. The Sun Newspaper, p. 1 & 3.

Computer World Malaysia (2017). CyberSecurity Malaysia Issues New National Ransomware Warning. Retrieved on 8 May 2017, from *https://www.computerworld.com.my/resource/security/cybersecurity-malaysia-issues-new-national-ransomware-warning/*

Cybersecurity Malaysia. Statistics: Retrieved on 9 May 2017, from *https://www.mycert.org.my/statistics/2017.php*

Digital Detox [Def. 1]. (n.d.). In *English Oxford Living Dictionary,* Retrieved May 17, 2017, from https://en.oxforddictionaries.com/definition/digital_detox

Kim, E.B. (2014). Recommendations for Information Security Awareness Training for College Students. *Information Management & Computer Security*, 22 (1), 115-126. Retrieved 10 May 2017, from http://dx.doi.org/10.1108/IMCS-01-2013-0005

Stefan F., Johannes, H., Thomas, N & Fabian, P (2014). Current Challenges in Information

Security Risk Management. *Information Management & Computer Security*, 22 (5), p. 410-430. Retrieved 10 May 2017, from http://dx.doi.org/10.1108/IMCS-07-2013-0053

InNurture (2017). What Makes Information Security Important?. Retrieved on 8 May 2017, from *http://www.inurture.co.in/what-makes-information-security-important/*

Labuschagne, L & Eloff, J.,H.,P (2000). Electronic Commerce: The Information-security Challenge. Information Management & Computer Secuirty, 8 (3), p. 154-157. Retrieved 10 May 2017, from http://dx.doi.org/10.1108/09685220010372582

Malaysia Computer Emergency Response Team. Retrieved on 16 May 2017, from *http://www.mycert.org.my*

Malaysia Sixth Most Vulnerable To Cyber Crime. Retrieved 10 May 2017, from http://says.com/my/news/malaysia-sixth-most-vulnerable-to-cyber-crime

Ruth C.M., Rita. M., & Graeme, B. (1999). Corporate Information Security Management. *New Library World*, 100 (5), p. 213-227. Retrieved on 10 May 2017, from http://dx.doi.org/10.1108/03074809910285888

Shahibi, M. S., Ali. J., & Zaini, M. K. (2011). Elements of Trust in E-Commerce Interaction. *Journal of Information and Knowledge Management*, 1(1), p. 101-110.

Ahmad, M. (2015). Malaysia's Approach Against Cyber Threat and Cyber Attacks. CyberSecurity Malaysia. Retrieved 17 May 2017, from http://ris.org.in/images/RIS_images/presentation-pdf/Mustaffa%20Ahmad.pdf

Norton, R. (2016). 2016 Norton Cybersecurity Insight Report. Retrieved on 9 May 2017, from https://www.symantec.com/content/dam/symantec/docs/reports/2016-norton-cyber-*security-insights-report.pdf+&cd=3&hl=en&ct=clnk*

Hannah, N., & Vilasmalar, M. (2014). The Personal Data Protection Act 2010: Challenges to Comply. *eSecurity*, 36(1), p. 39-40. Retrieved 17 May 2017, from http:// *www.cybersecurity.my/data/content_files/12/1291.pdf*

Perceptions of Transnational Security Threats in Malaysia and Singapore: Windows of Cooperative Opportunities for the United States. Retrieved on 8 May 2017, from http://apcss.org/wp-content/uploads/2012/02/140-153-Perceptions.pdf

Phishing [Def. 1]. (n.d.). In *English Oxford Living Dictionary,* Retrieved May 17, 2017, from http://en.oxforddictionaries.com/definition/phishing

Ahmad, R. (2017, May 14). Malaysia also hit by WannaCry ransomware. The Star Newspaper, 4.

Dzazali, S., & Zolait, A.H. (2011). Assessment of Information Security Maturity: an

Exploration Study of Malaysian Public Service Organizations. *Journal of Systems and Information technology*, 14 (1), 23-57. Retrieved 16 May 2017, from http://dx.doi.org/10.1108/13287261211221128

University of Staffordshire (2017). Why is Information Secuirty is Important? Retrieved on 8 May 2017, from *http://www.staffs.ac.uk/support_depts/infoservices/rules_and_regulations/Infosecurimp.jsp*