CYBER SECURITY IN ORGANIZATION

Amalina Zelikha Binti Rajeli and Husna Binti Hakimi
Faculty of Information Management,
Universiti Teknologi MARA (UiTM)
Puncak Perdana Campus,
UiTM Selangor, Malaysia

Abstract
The aim of this research is to identify the importance of cyber security in organization. This paper discusses about the various strategies in implementing cyber security in organization. In order to be a successful in the cyber security, the commitment between organization and all level should be create to address cyber security and cyber privacy risk. In this era, to implement the cyber security is not easy. In implementing cyber security, an organization will face several of the problem and challenges. The biggest challenges are regarding the cost or budget, lack of professional staff skills, lack of facilities, and many more.
Keywords: Cyber security, strategies, organization, challenges, staff.

1. Introduction

In the era of technological advancement and sophistication, there are numerous challenges of life that we have to encounter together. Nowadays, we always heard about the news of cybercrime in all countries in this world. Cyber security also known as a protection of the systems, networks and data in cyberspace from being attack by the cybercrime. The cyber-attack makes organization felt that they should have the cyber security. Cybercriminal always target the corporate body as their victim. The ICT increasing makes the cybercriminal easy to attack the organization. As we know, major of organization have implement their own cyber security. Today, the strong cyber security measure is self-evident. According to America hospital association (2015), in this era with more of our activities depend on information systems and technology.It is not surprising that, when we think about our organizations' vulnerabilities, and high possibilities to get a cyber-attack. In this era, to implement the cyber security is not easy. In implementing cyber security, an organization will face several of the problem and challengers. The individual factor is the most challenging aspect in cyber security. The weakest link in any IT security chain is the user (Arabo, 2015). In this paper, several issues are discussed regarding on how well cyber security has an effect on organization performance for the growth of the company. Based on our observation from the research articles, there is some limitations may occur during implement and having the awareness about the cyber security toward organization.

Difference of concepts on understanding of cybersecurity among the netizen in an expansion of global computer networks will make them easily attack by the threat. According to Whitty (2015) stated that an individual who are believe that they are more knowledgeable about security are more confident and likely to share the password without any awareness's compared to those person whose believe they are less knowledgeable. They will insecure to share all the private data with other.

Home environment known as the one of the factor which is can effect to various threat in the cyber space. Arabo (2015) has stated that home ecosystem futures have connected to home environment as a references to various threat. Hence the problem of cybersecurity extend beyond computer. Today many housewife using the computer in making their par time job as online seller. From that it easily make them attack by the cybercrime.

Cyber security and cybercrime have the strong relationship each other. Based on Julisch (2013), the author stated that Cybercrime and cybersecurity are issues that can

hardly be separated. It is shown that the cyber security is connected each other. As we known without cybercrime there will be not have a cyber security. When the cybercrime are attacked to solve and handle the problem the cyber security must be provide. As a nutshell it is strongly show that each cyber have each relation and can hardly separate. When we talk about cyber security, it will relate to budget and must have a lot of funds. Based on International Telecommunication Union (2012) states that, to make the strengths of security in the organization need more cost. The small private sector have problem in this to implement the cyber security. In order to be competitive, businesses need to be online. However, this also brings risks based on Institute for Defense Studies and Analyses (IDSA, 2013) the increasing online population has proved a happy hunting ground for cyber criminals, with losses due to cyber-crime being in billions of dollars worldwide (Australian Government, 2016). According to Castro (2016) the poor of cybersecurity practice at the OPM make them successfully attach by cyber-attack, but this attack could have been prevented. This hack is a public management failure that has resulted from the U.S. government becoming apathetic towards cybersecurity and tolerating poor performance.

The aim of this paper is to propose a framework based cyber security in organization. The remainder of this paper is organized as follows. Section 2 is literature review. Proposed framework is in Section 3. Final section contains some concluding remarks.

2. Literature Review

2.1 Cyber Security in Organization

Previous study discuss about the cyber security in the organization. In the organization, cyber security is very importance things. The article focus on cyber security in the organization which is according to America hospital association (2015) inform that cyber security is very importance in private or public sector. In this article, they focus on the cybersecurity in the hospital. Here we can conclude that every organizations need the cyber security. Enisa (2012) has stated the cyber security in the organization of several countries. They has mention every countries has their own cyber security strategies. In this era, expansion of global computer networks will increase the number of computer users worldwide. In this case, an organization must have their responsibilities to improve their cyber security in the organization. They also must provide training for new workers about the data safety or information security.

2.2 Cyber Security Challenges

Although cyber security in every organization, there are various challenges that they will face in implementing cyber security to their organizations. First of all, IDSA (2013) has state the increasing of online population will be the opportunities for the cyber-criminal to do their job which is cyber-crime. In this era we need the internet and overall of our daily activities depend on the technology. This will difficult to us to avoid the cybercrime. In this article has explain the low cybersecurity in the device will possibilities to get a cyber-attacks. In the ITU (2012) stated the challenges to fight the cybercrime is the increasing of ICT. A cyber-attack targets the public web server that connects the corporate network with the internet. This difficult for us to fight the cybercrime. We need the strong cybersecurity to prevent the cybercrime. The strong cyber security needs cost. The low cost in the organization will difficult for them to make a strength cybersecurity.

2.3 Cyber Security Strategies

In order to overcome this challenges there are some cybersecurity strategies that can be implement by the organization. As we know, small private sector has low cost to make sure their security strength. In this situation, the government agencies should take responsibilities on the small private sector. Government should share their knowledge about

cyber security to make sure small private sector understand how to prevent cybercrime. According to Carr (2016) it should be noted that the public and private sectors is an organization that has partnerships with each other where it is called repeatedly as 'basic' or 'hub' in cyber security strategy. Between the two organizations as we know that each organization need each other to achieve the goals of the organization. If one of the organization being attacked by cybercrime it will affect other organizations which is both organization usually share the information and the data each other. It is show that both organizations related to each other to complement each other benefit. In order to cater these problems the governments also can make their own responsibility start develop national cyber-security strategies. This strategy that is developing by the government is to outline the ways in which they intend to address cyber insecurity. As know the government have their own responsibility and the organization which is have the responsibility to make sure the safety of our nation.

3. Proposed Framework

In this era, expansion of global computer networks will increase the number of computer users worldwide. This is because users will easy to connect to the internet connection using their computer, laptop and many more. They can access to the internet connection wherever they want. Besides, the information theft will easily to steal data or information from other organization. In this case, an organization must have their responsibilities to improve their cyber security in the organization. According to America hospital association (2015) cyber security is very importance in private or public sector. Online businesses are the ways to be a competitive in businesses but also bring risk to the organization. The organization connected to internet it's vulnerable to compromise. The value and quantity of information held online has increased as people and systems become more interconnected. This situation make the cybercriminal have efforts to steal and exploit the information, harming economy, privacy and safety (Australian Government, 2016).

Every organization need the cyber security. The government security should strengthen. Government plays the importance role for the private sector. Government agencies should share their knowledge especially to small business that may not have the cybersecurity (Castro, 2016). They must make sure that private sector cybersecurity well. The nation should work collaboratively on cyber security.There are various challenges that they will face in implementing cyber security to their organizations. First of all, IDSA (2013) state the increasing of online population will be the opportunities for the cyber-criminal to do their job which is cyber-crime. In this era we need the internet in our daily activities. This will difficult to us to avoid the cybercrime. Low cybersecurity in the device will possibilities to get a cyber-attacks. In the article a cyber-attack targets the public web server that connects the corporate network with the internet. This difficult for us to fight the cybercrime. We need the strong cybersecurity to prevent the cybercrime. The strong cyber security needs cost. The low cost in the organization will difficult for them to make a strength cybersecurity.

According to Castro (2016) the poor of cybersecurity practice at the OPM make them successfully attack by cyber-attack, but this attack could have been prevented. This hack is a public management failure that has resulted from the U.S. government becoming apathetic towards cybersecurity and tolerating poor performance.In order to overcome this challenges there are some cybersecurity strategies that can be implement by the organization. According to Carr (2016) it should be noted that the public and private sectors is an organization that has partnerships with each other where it is called repeatedly as 'basic' or 'hub' in cyber security strategy. Between the two organizations as we know that each organization need each other to achieve the goals of the organization. If one of the organization being attacked by cybercrime it will affect other organizations which is both organization usually share the information and the data each other. It is show that both organizations related to each other to complement each other benefit. To catch this problem

the governments also can make their own responsibility start develop national cyber-security strategies. This strategy that are develop by the government is to outline the ways in which they intend to address cyber insecurity. As know the government have their own responsibility and the organization which is have the responsibility to make sure the safety of our nation.

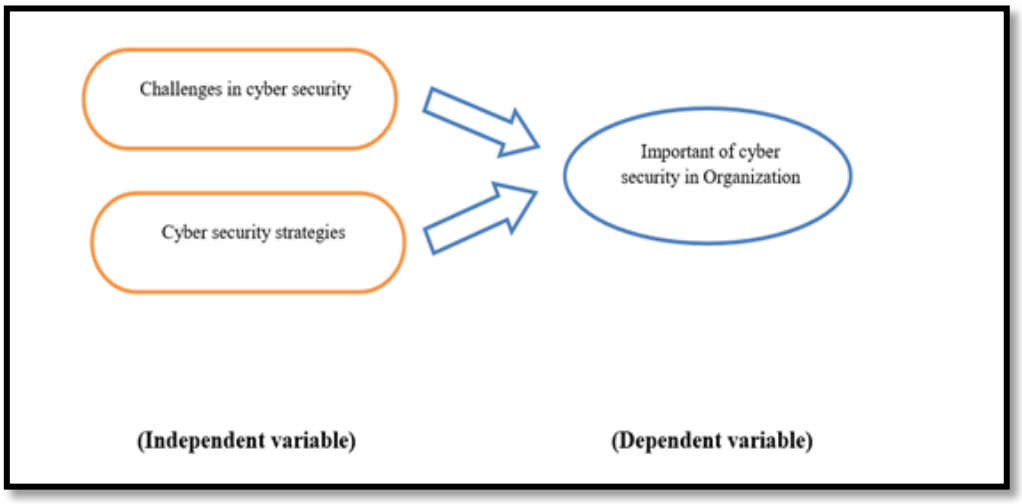

Figure 1. Proposed framework

Figure 1 is a theoretical framework that will be used to guide this research. Based on the previous study, the proposed theoretical framework illustrates a dependent variable important of cyber security in an organization, and two independent variable which is challenges in cyber security strategies of cyber security. The framework will be used to answer the main research question, that is, important cyber security in organization.

4. Conclusion

Cyber security is the protection of function in cyberspace and any of their assets that can be reached via cyberspace. In this era of technology, people in this world more prefer to use technology in their routine activities. However, this research focuses more on cyber security in organization. Cyber security is very important in today's society. Most organization also realize that the strength cyber security is very important and they implement the strength of cyber security application to their organization to avoid the cyber-attack. Besides that, this research also explains regarding strategies when implementing cyber security. There must have effectiveness strategies in implement the cyber security there are various advantages when implementing cyber security such as government role to private sector, balanced privacy and security, follow the rules of internet, and provide the application of cyber security. On the other hand, an organization face various challenges in implementing cyber security in organization. The biggest challenges that they faced is regarding the increasing of ICT, low cost and to detect the cybercrime. All these challenges can give big problem to the organization.

References

America hopital association. (2015). Cybersecurity and Hospitals.

Arabo, A. (2015). Cyber Security Challenges within the Connected Home Ecosystem Futures. *Procedia Computer Science*, *61*(0), 227–232.

https://doi.org/10.1016/j.procs.2015.09.201

Austrialian Government. (2016). *Australia's Cyber Security Strategy*. Retrieved from https://cybersecuritystrategy.dpmc.gov.au/assets/pdfs/dpmc-cyber-strategy.pdf?q=270716

Castro,Daniel. (2016).A New cyber security paradigm.

Carr, M. (2016). Public – private partnerships in national cyber-security strategies, *1*, 190 209.

Enisa. (2012). National Cyber Security Strategies, (December), 15. https://doi.org/10.2824/3903

IDSA. (2013). *India`s Cyber Security Challenge*.

International Communication Union (ITU) : (2012). Cybercrime Understanding Cybercrime

Julisch, K. (2013). Understanding and overcoming cyber security anti-patterns. *Computer Networks*, *57*(10), 2206–2211. https://doi.org/10.1016/j.comnet.2012.11.023

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 3–7. https://doi.org/10.1089/cyber.2014.0179