Chapter 31
The Challenges and Solutions of Cybersecurity Among Malaysian Companies

Puteri Fadzline Tamyez
University Malaysia Pahang, Malaysia

ABSTRACT

The objective of this chapter is to analyze the challenges faced by Malaysian companies in cybersecurity and to determine solution for Malaysian companies to overcome challenges in cybersecurity. The data were collected from the expert people in cybersecurity fields using interview sessions. The finding confirmed that the awareness and budget are very important in other to implement the element of cybersecurity in the company. Cybersecurity is good and desired as a protection for an organization in developing strategic planning to gain more profitability and increase the productivity of goods and services. This research will be beneficial for the organization because it will provide the solution for the company to overcome the cybersecurity issues. From this research, an organization can have potential to enhance competitiveness and understand the problem occur, then do the improvement by implementing cybersecurity.

INTRODUCTION

Industry 4.0 invites tremendous advantages for companies towards business sustainability. It has nine pillars altogether, namely, internet of things, big data, supply chain, cloud computing, horizontal and vertical integration, autonomous robot, addictive manufacturing, cyber security, simulation and augmented reality. However, the major challenge in facing this digitalization era is on cyber security (Jay Lee, 2016). Privacy and security of the data will always be top security measures that any organization should take. We live in a world where information are secured in digital or a cyber-form. Data from multiple sources has different formats gives difficulty for analysts to integrate the data (Ibrar, 2017). Lack of monitoring and protection against unauthorized changes or alteration will create unwanted changes

DOI: 10.4018/978-1-6684-3698-1.ch031

in data information. Most companies faces inadequate of development phase (Ibrar, 2017), thus makes it important in order to limit the risk of application related assaults or attacks.

The inadequacy of development phase as brought small and medium size enterprise (SMEs) face different risks as compared to large companies, as these organizations have limited and minimum human and monetary resources to apply information technology (IT) and cyber security systems (Heikkila, 2016). Most SMEs own traditional security mechanisms, which could not accommodate the technology of the Internets of Things (IoT) due to limited resources (Ibrar, 2017). Apart from that, they need to overcome the inadequacy of security budget and low security alertness among the workers. Lack of employee training and recovery planning has contributed to its low security alertness among employees (Heikkila, 2016). This finding further elaborates that only a few companies report on the provision of safety-related training for all employees. However, the lack of deployment process shall cause problems in managing the cyber security (Ibrar, 2017).

The inadequacy of security software's upgradability and patch ability is also one of the issues in cyber security. A number of companies usually do not put much effort in upgrading security software due to lack of resources. The low and inadequacy of physical security will allow and provide an unrecognized user to enter the data or devices using Universal Serial Bus (USB) port. This may cause companies to face many problems. Another issue is trust. Network interactions with systems that have lower standard security will invite more trust issues. Data transference is mostly carried out by wireless network, which increases the probability of miss-data problem to occur (Ibrar, 2017). This may affect in aspects of incomplete or false information. Thus, cyber security is crucial in all industries to make sure all of their data were being safely secured. This research attempts to answer the accompanying inquiry in aspects of the challenges faced by Malaysian company in cybersecurity and the solution for Malaysian companies to overcome challenges in cybersecurity.

BACKGROUND OF STUDY

Most industries are affected by technological change and innovation or rather called industrialization revolution (Jay Lee, 2016). This revolution is due to mechanization in the first industrial revolution, the use of electricity is 2nd industrial revolution and electronics and automation is industrial revolution 3. The revolution not only affected the production itself, but also the labour market and education system as well (Lasi, 2014). Due to development of digitalization and robotics, the industry faces the next industrial revolution, known as Industry 4.0. These new emerging technologies have a huge impact on people's education and scope of work (Katharina M., 2015).

Only qualified and highly educated workers will be able to control this technology. Digital supply chain is smart, worth-driven network that is the current path to automation and analysis in order to generate unique forms of interest and business value (Keliang Zhou, 2015). Cyber security as one of the nine pillars is exposed to external and insider cyber threats with complicated and sophisticated cyber security landscape (Wells, 2016). It is known as an activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and or defended against damage, unauthorized use or modification, or exploitation" (DHS, 2014). Other than that, cyber security involves reducing the risk of malicious attack to software, computers and networks (Dan Craigen, 2014). This includes tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, enable encrypted communications, and on and on. Thus, the goal of this study