CYBER SECURITY THREATS

Dini Sharleena Subhi Shah
Faculty of Information Management,
Universiti Teknologi MARA (UiTM)
Puncak Perdana Campus,
UiTM Selangor, Malaysia

Abstract
The aim of this research is to identify the effect of cyber threats towards the national security, organizational and industrial institutions. Currently, cyber threat topic has expanded all around the world. Technologies have succeeds in helping many institution to expand their business. However, with the technologies also increased the number of cyber threat. This paper classified the impact of cyber threats to the three types of institutions which are national, organizational and industrial institution.
Keywords: Cyber threat, national security, organizational, industrial, technologies

1. Introduction

Cyber threat topic currently arising and get attention most of the countries. With this new era of globalization, cyber threat is one of the growing topics that should be prioritized by the individual, organization institution and also the nation. According to Solms & Solms (2018) stated that cyber-security defines as all the inclusive term that replacing information security. They also added that information security is actually the same as information security. Threat is something that we need to avoid since it can occurs negative impact. According to Pipyros et.al. (2016) and US National Research Council (2009), cyber threat defines as an action to disrupt computer network of other parties. There are studies have found that evolution of the technologies can cause negative impact such as private harassment, social violence and psychological effect (Solms & Solms 2018; Martin & Rice 2011). According to (Solms & Solms 2018; Ignatuschtschenko 2016), cyber threat can bring damage as well as destruction such as physical and psychological suffer of an individual. She also added that the consequences also bring harm to organizational infrastructure and national development. There are three main possibilities of cyber-security threats based on the research that has been done which are on national security, organizational and industrial.

First cyber-security threat is on national security. Technology is growing rapidly nowadays and the globalization has changed on how the government leads the countries in order to reduce the gap between the growing technology (Alqahtani 2015; Tadjbakhsh & Chenoy 2007). According to Alqahtani (2015), cyber threat issue has become a serious topic in nationwide because most of the attack aimed for a country. Although the advancement of technology gives many positive benefits, however it also can bring a nation down with the attack on cyber network. A country infrastructure has

potential to face cyber threat which is cyber terrorist. This can lead any country to face a critical situation related to their national bodies. According to Alqahtani (2015), cyber threat become more critical since it related to cyber terrorists. He added that terrorists who exist in cyber network were really advanced nowadays since the technology is growing fast day by day. Cyber terrorists mostly aimed for developed and large countries that have an effective development such as Saudi Arabia Alqahtani (2015). It is because in any countries will have its own private and confidential document in every institution such as financial institution, military institution, academic institution, industrial institution and so on. Cyber threat can involve many parts of the country such as in political, economic and social. It shows that cyber threat to national security is a crucial thing that need to be taken seriously by all parties especially leaders of the country.

Second cyber-security threat is on organization. The growing of technology has changed the business environment in many organizations. Technologies give many benefits to build the infrastructure of the organization but however it also comes with negative impact. According to Adu & Adjei (2018), as a result for increasing technology, the system and services of an organization are easy to attack (Adu & Adjei 2018; Magele 2005) said that internet provide many opportunities for an organization but they also faced with information risk. Cyber threat can attack the whole organization and in order to fix it back huge amount of money will needed. According to Adu & Adjei (2018) and Juniper Research (2016), according to their observation that many organizations forced to bear high losses in 2019 due to the cyber threat attack. Most of the organizations generated their data on cyber network. Data on cyber network growth will grow every year and this can risk the data to be attack someday.

Last but not least, cyber-security threat can attack on the industry. According to Ani, He & Tiwari (2019), many organizations from many industries keep updating their technologies. According to Mani, Choo & Mubarak (2014), physical barrier is not a problem anymore for the industrial institution to conduct their businesses. As long as there is internet connection, the business can still be continued. However, cyber-attacks on industrial environment have been continued to arise Ani, He & Tiwari (2019). This situation can brings harm to the industrial institution since there are many things to be protected such as business details, stakeholders, customer details, financial statement and so on. The attackers might be manipulate and exploit whenever they have opportunities. Cyber threat can be the crucial thing that needs to be aware in industrial institution. The purpose of this study is to identify the cyber threats that affect national security, organizational and industrial institution.

2. Literature Review

This research is expected to analyze the effect of cyber threats that affect national cyber security, organizational and industrial institution. Technologies have been widely used in infrastructure of national, organizational and industrial institution. Those three effects are believed to be the main factor to be attacked by the hackers.

2.1 National Cyber Security Threat

Technology is growing rapidly nowadays. However, technology also has its own consequences and some of it will result to severe damage. The adverse effects of technology can bring harm to the national security. According to Abomhara & Kolen (2015), cyber threat can attack the structural of the government entities. According to Kuru & Bayraktar (2017), many large countries were on the lists that have potential to be attack on cyber network such as United States, Turkey and United Kingdom. Cyber-attacks have been increasing day by day and transformed the cyberspace into the fifth dimension of war mentioned by Pipyros et.al. (2016). They added that existing legal framework that should protect the cyber space seems inadequate to deal with the cyber-attacks such as in United States. A few researched have been done that most of the terrorists used the advancement of internet for their communication and it is stated by (Gallova et.al. 2018; Taylor et.al. 2014). Another research shows that internet has been used for radicalization and it is been identified almost 15 cases used internet to spread their extremist opinion and radical information (Gallova et.al. 2018; Von Behr et.al. 2013). Cyber-attacks have triggered the governments and scientific community for several times. It is proven when NASA has been attacked on its network with the WANK worm in 1989 stated by Pipyros et.al. (2016). Every countries has its own secret they need protect such as their government, military, sensitive data and many more. Some of the advancement of technology can bring a nation down. It is called cyber-attack. Cyber threat caused many negative impacts to the country and its public such as private harassment, private violence and expose to the embarrassment (Solms & Solms 2018; Martin & Rice 2011).

In this era of globalization, cyber-security threat has changed the world. It is because every leakage of information can threatened a nation. There are no rules in transmit the information even though through all over the world. As long as there is internet connection, any information can be transferred. There are many cases happened that need worldwide to concern related to cyber-security such as the threat of terrorism. According to Alqahtani (2015), threat of terrorism has increased over the past of 30 years because of the technology. Technology caused the terrorism issue become worse. Alqahtani (2015) said that the phenomenon of terrorism changing due to the technology but main motives of terrorism still remain the same that can threatened the nation. With the cyber-terrorism, methods and strategies are different than traditional war such as hijacked planes, bombs, weapon and so on. It is more advanced because it can attack national cyber-security. According to Alqahtani (2015), whoever launched their attack on networks and systems in any country in order to achieve their political goals are considered as terrorism. There are many cyber threat effects can be affected to the country itself as well as its public such as bad reputation of a country, economic downturn, physical and psychological crisis, industries breakdown and national harassment (Solms & Solms 2018; Ignatuschtschenko 2016). According to Kuru & Bayraktar (2017), there are certain countries need to incur extremely high losses of money due to the cyber threat. The added that according to previous research, United States spent a huge amount of money which is 9 million dollars to bear cyber-crime that occurred in their country and even other countries also. Other than cyber-terrorism, cyber fraud also one of the cyber threat that occurred in most of the countries and it is

also called as cyber-scam Whitty (2019). This case will involve the country to be aware because most of the victims are the public. Almost 52 billion spent by United Kingdom government in order to bear the fraud cost occurred in their country (Whitty 2019; The National Fraud Authority 2013).

Based on the previous studies, finding shows that national security is in dangerous situation where they need to overcome this problem immediately. It is because previous research has shown that many cybercrime happened in many countries and cyber-war might be happen if this situation not immediately resolve.

2.2 Organizational Cyber Security Threat

Adu & Adjei (2018) expressed that evolution of technology changed the environment of business in most organizations nowadays. They added that although technology gives positive impact to the organizations such as using internet transaction, somehow it also exposed to the cyber-attack. Information transferred to the third parties is also at risk (Adu and Adjei 2018; Magele 2005). This has been proven with a research in 2016 where almost one percent of sent emails were at risk and cyber-attack on companies and hospitals in almost 150 countries in 2017 were recorded (Adu & Adjei 2018; Global Cyber Security Index 2017). Latest cases regarding to cyber-attack were recorded in 2019 which many organization's computer systems and files were locked and threatened by irresponsible parties (Adu & Adjei 2018; Juniper Research 2016). Many organization losses due to cyber-attack and economic were also affected. According to previous researched by Fenz et.al. (2014), they said that people and organization nowadays are really depends on computer software to fulfill the works and it place cyber threat is one of dangerous case trend to be happen. Many organizations already concerned about the cyber threat that can attack their organization anytime at a worse place (Ani, Hongmei & Tiwari, 2019).

Nowadays, crimes happened in many ways including cybercrime. Cybercrime defines as illegal or criminal activities that related with the use of technology (Malik & Urooj Islam 2019; Hunton 2009; Kraemer-Mbula et.al. 2013). According to Malik & Islam (2019), cybercrime have become a serious concern to many organizations out there. It is because most of the cases related to cybercrime or cyber-attack will involve a huge amount of money. Criminal will attack information that relate with organization's confidential information such as password or pin code and they will blackmail and ask for money in return (Malik & Urooj Islam 2019; Gercke 2011). For example, research shows that payments must be made in order to unlock the computer systems and files (Adu & Adjei 2018; Juniper Research 2016). Many organizations faced cyber-crime that occurred at their organization such as financial organization, commercial organization, government organization, private organization and many more (Kuru & Bayraktar, 2017).

Based on the previous research, it discovered that organization also threatened with the thread of cyber-attack. It can cause most of the organizations in insecure position. Their business might be ruin if some of the important data lost and a huge amount of money needed in order to get the information back.

2.3 Industrial Cyber Security Threat

According to Abomhara & Kolen (2015), technology and its network are growing rapidly as well as the number of threats are also growing up. It shows that many institutions such as industrial institution have potential to be attack on its system. Attack related with cyber security has been an increasing concern in most of the industrial sites such as chemical and process industry (CPI) (Moreno et.al. 2018; Argenti et.al. 2015. They added that most of the industries have loss of system control because of cyber-attack. Cyber-attack in industries mostly driven by business reason because they want to steal the important data from other industry or business (Moreno et.al. 2018; North America Oil &Gas Pipeline 2013). Most of hackers or attackers, they aimed on attack, sabotage and lock the information of a certain industries or businesses to interrupt their daily activities (Eling & Schnell 2016; CRO Forum 2014). According to Eling & Schnell (2016), technology has been used widely including the industry and everyone connected to the main network which is Internet. So, Internet and technology is one of the main sources the cyber threat may occur. There is no doubt that technology really helps industry and business spread widely but it also may have its consequences (Eling & Schnell 2016; Biener et.al. 2015).

According to Mani, Choo & Mubarak (2014), there is no physical barrier to conduct any businesses or daily activities in the industry with the existence of technology as a solution. Most of the attackers are aimed for the assets of an industry. According to Abomhara & Kolen (2015), asset defines as something that valuable, confidential and precious for an entity. The attackers might be the competitor in the industries itself. It is because any confidential data from the industries may be valuable for the competitors since they can know what are the strengths and weaknesses of other industries (Mani, Choo & Mubarak 2014; Griffith 2011). There are many cyber threat cases related to the industries occurred. Trade regime faced a complicated situation where they need to adapt with cyber-security threat Grindal (2019). Other than that, there is a case where the customer's details leaked and it involved by Vodafone workers (Mani, Choo & Mubarak 2014; AAP 2011). There is also a case happened in the real estate industry at South Australian. According to Mani, Choo & Mubarak (2014), there are over 85 percent case reported because of the malware threat and attack their hardware such as laptop, mobile phone and CCTV. The effects of the incidents are they cannot access to their email, other network systems and interrupt the daily operation. According to Abomhara & Kolen (2015), structural threat is one of the serious threats towards the industrial institution, government and business entity.

Based on the research, it has been proven that industries also faced the same threat as others in term of their cyber-security. There are many researches proved that possibility for industries to be attack is higher. It is because most of the industries nowadays used computer network as their daily business.

Table 1. Analysis of Review

Author(s)	National Cyber Security Threat	Organizational Cyber Security Threat	Industrial Cyber Security Threat
Solms & Solms (2018)	✓		
Adu & Adjei (2018)		✓	
Alqahtani (2015)	✓		
Fenz et.al. (2014)		✓	
Kuru and Bayraktar (2017)	✓	✓	
Ani, He & Tiwari (2019)		✓	
Pipyros et.al. (2016)	✓		
Whitty (2019)	✓		
Malik & Islam (2019)		✓	
Gallova et.al. (2018)	✓		
Grindal (2019)			✓
Abomhara & Kolen (2015)	✓		✓
Moreno (2018)			✓
Eling &Schnell (2016)			✓
Mani, Choo & Mubarak (2014)			✓

3. Conclusions

As a conclusion, cyber-security threat is one of the crucial issues nowadays. Many of the parties are involved and affected by the cyber-security threat whether at national level, organizations or industries. There are many finding show that the implication of the cyber-attack can cause a huge problem in terms of money, security level and community. All parties needed must cooperate together to avoid serious cases happen in the future such as cyber-crime or cyber-war. For national security, it is a priority for any countries to be aware with cyber threat because once we overlook for this cases a nation can fall anytime. Cybercrime that happened in any countries must be overcome to avoid any dangerous situation occur. For organization, cyber-attack can threaten their daily routine business because it will expose them to unsafe position. Other than that, cyber-attack also can cause an organization to use a lot of money. For industries, its possibilities to be attack is higher because they used computer network in their routine work. It has proven in many previous researches.

References

Abomhara, M., & Kolen, G. M. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *4*, 1-25.

Adu, K. K., & Adjei, E. (2018). The phenomenon of data loss and cyber security issues in Ghana. *Foresight, 20*(2), 1-13.

Alqahtani, A. (2015). Towards a framework for the potential cyber-terrorist threat to critical national infrastructure: Aquantitative study. *Information & Computer Security, 23*(5), 1-39.

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology, 21*(1), 1-35.

Eva Ignatuschtschenko (2016). Developing a cyber-harm model.

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance, 17*(5), 1-20.

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. *Information Management & Computer Security, 22*(5), 1-23.

Gallova, V., Palasinki, M., Shortland, N., Humann, M., & Grieve, L. B. (2018). Anxiety about digital security and terrorism and support for counter-terror measures. *Safer Communities, 17*(3), 1-12

Gercke, M. (2011). Understanding cybercrime: A guide for developing countries. *International Telecommunication Union, 89*, 93.

Grindal, K. (2019). Trade regimes as a tool for cyber policy. *Digital Policy, Regulation and Governance, 21*(1), 1-14.

Hunton, P. (2009). The growing phenomenon of crime and the internet: A cybercrime execution and analysis model. *Computer Law and Security Review, 24*(6), 528-535.

Juniper Research (2016). Cybercrime will cost businesses over $2 trillion by 2019.

Kraemer-Mbul, E., Tang, P. and Rush, H. (2013). The cybercrime ecosystem: Online innovation in the shadows? Technological Forecasting and Social Change, 80(3), 541-555.

Kuru, D., & Bayraktar, S. (2017). The effect of cyber-risk insurance to social welfare. *Journal of Financial Crime, 24*(2), 1-19.

Magele, T. (2005). E-security in South Africa: White paper prepared for the forge ahead e-security event.

Malik, M. S., & Islam, U. (2019). Cybercrime: An emerging threat to the banking sector of Pakistan. *Journal of Financial Crime, 26*(1), 1-12.

Mani, D., Choo, K.-K. R., & Mubarak, S. (2014). Information security in the South Australian real estate industry: A study of 40 real estate organisations. *Information Management & Computer Security, 22*(1), 1-20.

Martin, N. and Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. *Computer & Security, 30*, 803-814.

Moreno, V. C., Reniers, G., Salzano, E., & Cozzani, V. (2018). Analysis of physical and cyber security- Related events in the chemical and process industry. *Process Safety and Environment Protection, 116*, 1-11.

Pipyros, K., Mitrou, L., Gritzalis, D., & Apostolopoulos, T. (2016). Cyberoperations and international humanitarian law: A review of obstacles in applying international law rules in cyber warfare. *Information & Computer Security, 24*(1), 1-17.

Solms, B. v., & Solms, R. v. (2018). Cybersecurity and information security- What goes where? *Information & Computer Security, 26*(1), 1-9.

Tadjbakhsh, S. and Chenoy, A. (2007). Human security, concept, and implications.

Taylor, R.W., Fritsch, E.J. and Liederbach, J. (2014). Digital crime and digital terrorism.
T., M. (2005). E-security in South Africa: White paper prepared for the forge ahead e-security event.
Von Behr, I., Reding, A., Edwards, C. and Gribbon, L. (2013). Radicalisation in the digital era: The use of the internet in 15 cases of terrorism and extremism.
Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime, 26*(1), 1-17.