Addressing the Threats of Online Theft of Trade Secret and Cyber Espionage in Malaysia: The Legal Landscape

Juriah Abd Jalil
Ahmad Ibrahim Kulliyyah of Laws, International Islamic University Malaysia, Kuala Lumpur, Malaysia.
juriah@iium.edu.my

***Abstract*— Online theft of trade secrets and commercial cyber espionage are growing threats to businesses and national economy in this digital economy. This global phenomenon of targeting trade secrets of corporation has caused the loss of billions of dollars in the UK, US, Japan and some others. These crimes are committed by rivals and in most cases with the help of an insider who is normally an employee of the organization. In the US the prosecution of a Chinese national who disclosed a company trade secret in China while working in US indicated the cross border nature of the crimes. Responding to the threat, the US regards theft of trade secret and economic espionage in whatever form as crime against the state under the Economic Espionage Act 1996. In Japan such crimes are regarded as threats to the business industry that are penalized under the Unfair Competition Law of Japan. Although such decision broke the tradition of allowing mobility of workers and protecting the loyalty of workers in Japan, such law was introduced to protect the industry from unethical business practice and also to protect research and development to boost the Japanese economy. In contrast Malaysia like the UK has no specific law criminalizing economic espionage and theft of trade secrets even though the threats are growing. Without such laws the business community particularly the small business enterprises are exposed to this digital risks. However in relation to online theft of trade secrets and cyber espionage, the Communication and Multimedia Act 1998(CMA) and Computer Crimes Act 1997 (CCA) may be relied on to criminalized online theft of trade secrets and cyber espionage. By adopting SWOT and comparative analysis, this paper examines the administrative policy by the Malaysian Government and the current regulatory framework governing cyber espionage and online theft of trade secret in Malaysia. This paper concludes that both administrative policy and regulatory framework should complement each other to give better protection against online theft of trade secrets and commercial cyber espionage in Malaysia.**

Keywords—cyber espionage; online trade secret theft, cyber crimes, small business enterprises, digital economy.

I. INTRODUCTION

Trade secrets or valuable corporate information are a 'gold nugget' of every company and business entity. Because of its significant value, trade secrets become the target for theft and unauthorised use.[1] Although theft of trade secrets and economic espionage is not a new crime but the method use to steal is new i.e. using cyber technology to root out and steal trade secrets and intellectual property.[2] Reliance and dependency on IT system and networks by companies without placing proper safeguard to protect their trade secrets exposed them to cyber attacks by competitors, foreign government and hacktivists groups. [3] As a result, cyber espionage and online theft of trade secrets posed serious threats to businesses all over the world.[4] The statistic below indicates the impact on the UK economy whereby IP theft and industrial espionage range the top 2 causing the loss of £ 9.2 billion because of IP theft and £7.6 billion due to espionage. [5] This tally with the survey conducted by Trend Macro Incorporated in 2016 that revealed 20% of global organization has ranked cyber espionage among the most serious threat to their business.

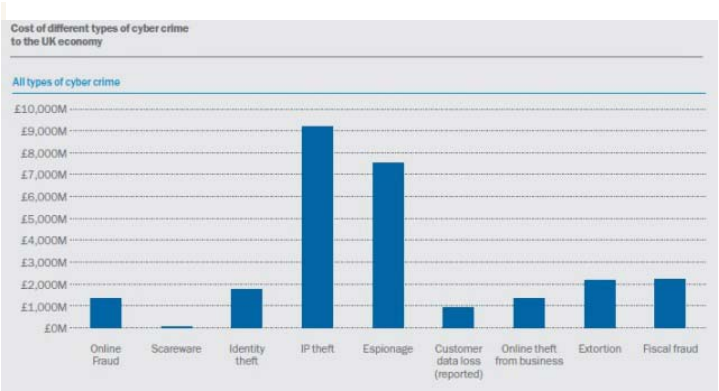

Fig 1 IP theft and Industrial Espionage in UK
(Source: The Cost of Cybercrime, Detica/Cabinet Office)

In the US, research shows that one in five business organizations has suffered cyber espionage regardless of whether a big corporation or a small business entity. Recent statistic on cyberattacks indicated that cyber espionage constituted 11.8% in Dec 2017. [see Fig. 2] The biggest threat was from China. Nevertheless Symantec reported that the economic espionage such as stealing trade or commercial secrets has dropped "following a mutual agreement between the US and China not to target intellectual property." [6] Thus while law alone may not be sufficient to reduce the crime, administrative and diplomatic policy may provide some

solution in reducing the threat. Figure 2 also separate cyber espionage from cyber crime giving the indication that on its own, cyber espionage is a crime and a potential threat to businesses. Similar threats occur in Japan forcing the government to criminalise theft of trade secrets and commercial espionage.

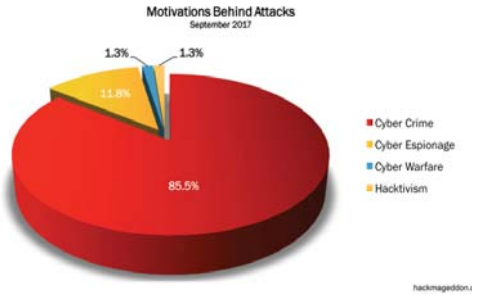

Fig 2 Statistic on Cyber Attacks Dec 2017
Source: Hackmageddon Information Security Timeline Statistic

II. COMPANIES AS PRIME TARGET

Digital age has made it more challenging for companies to protect their trade secrets. In fact they are increasingly falling victim to cyber-attacks from the insiders or employee, former employee, suppliers, consultants or other third parties, rogue cyber criminals or hackers and state sponsored criminals.[7] Among these threat actors, the most feared is former employees as seen in Fig.2 which constitute 32%. This is largely due to the employee's familiarity with the working environment, the organization procedures and technology used by the companies.

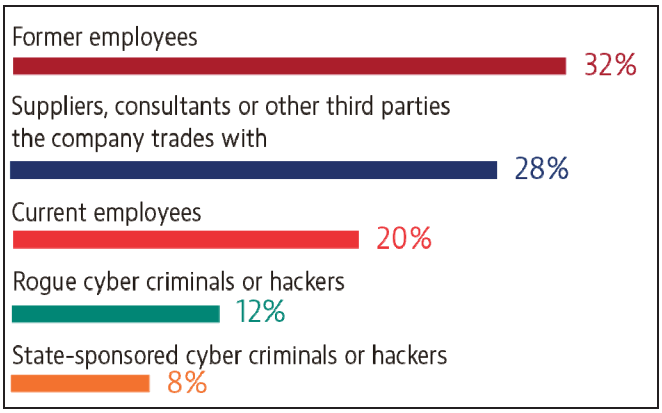

Fig. 3 Threat Actors

Source: Bakermakenzie, Trade Secrets Theft, a Trillion Dollar Problem?

One of the main reasons why companies are so vulnerable to attack is due to the extensive use of computers and other digital devices in all areas of business. [8] Such heavy reliance has created an ideals condition for cyber espionage and theft of trade secrets to strike. An employee for example can just download any documents or valuable company information by using a flash drive or competitors or hackers can just rely on malware to stealing corporate data without the company knowledge. Using of such device makes it much easier to transfer data or valuable information to the cyber criminal.

However protecting trade secrets especially online is a challenging matter since hackers, cyber criminals and other threat actors are using different type of techniques as seen in Fig.4 to steal information from the company.

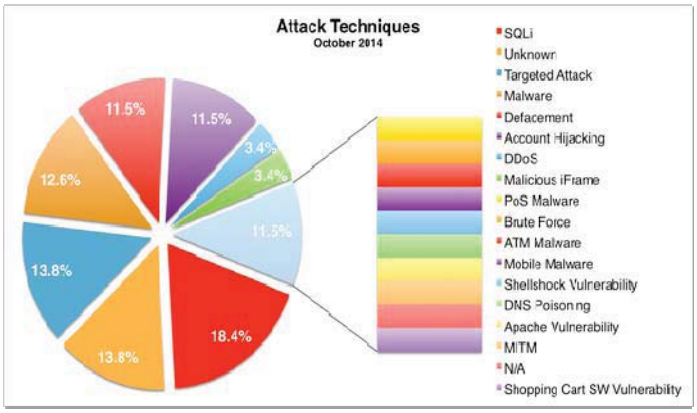

Fig.5- list of attack techniques used by the threat actors.

The availability of such techniques indicates that online theft of Trade secrets and cyber espionage or spying are "becoming more sophisticated and widespread" to the extent that a company only knew that it has become a victim after the losses has occurred.[9] Further cybercriminals also use destructive programs such as encryptors, shredders and 'army of zombies' to devour every available resource on company web servers and data transfer network [10]. Aside from the cyber attack, theft of mobile devices, desktops and laptops also contribute to the theft of trade secrets. Criminals are targeting these devices as important source of information to infiltrate company's computer and as well as IT system. Trade secret is therefore not only vulnerable but fragile. The impact of losing it could clearly destroy the future of the victims companies in the hand of competitors.[11] Since companies contributed to the economic development of a country, many countries are taking different approach to protect trade secrets from theft and corporate espionage. Due to wide spread and global nature of the problem, it is important to see how protection of trade secrets is framed at the international level.

III. INTERNATIONAL LEGAL FRAMEWORK

The protection of trade secrets was initially based on Article 10*bis* of the Convention for the Protection of Industrial Property (Paris Convention).[12] The Convention requires member States to provide effective protection against unfair competition. This provision was later referred to by Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights or TRIPS of the World Trade Organisation (WTO) under Section 7 on Protection of Undisclosed Information. In contrast to the Paris Convention, TRIPS provide some general standard to qualify for protection under this provision namely that the information must be secret,

have commercial value for being a secret and reasonable efforts must have been taken to protect and maintain it secrecy. But implementation of TRIPS requirements into the national systems varies within the WTO members. As a result countries protect trade secrets under civil, common law, and unfair competition law. At this juncture many countries however still rely on civil rather than criminal law to protect trade secrets because of the intangible nature of trade secrets.[13] The cause of action for suing can be on breach of contract especially in employment cases, breach of trust and breach of confidence under common law and misappropriation or unlawful and unauthorised use of trade secrets under the unfair competition law. The available remedies are injunction, damages and account of profits. With the advance of technology, online theft and commercial cyber espionage increases, resulting in the enactment of cyber law to combat the risks online.

In a more recent development, the European Parliament and the Council has on 8 June 2016 adopted a Directive that aims to standardise the national laws in the European Union countries against unlawful acquisition, disclosure and use of trade secrets.[14] The directive was issue as measure to protect the EU economy against the major threat of trade secret theft by harmonising the law and to ensure that there is a sufficient and consistent level of civil redress in the internal market. Failure of the member states to do so will allow the European Commission to initiate legal action against the member states. As such unimplemented or badly implemented directive can have direct legal force.

As the importance of trade secrets become recognised, protecting trade secrets have become the subject of domestic and international policy. However within ASEAN, the ASEAN ECONOMIC Blueprint only focus on strengthening IPR Protection in general and was silent on online theft of trade secrets and commercial espionage. Nevertheless some of the ASEAN countries namely Brunei, Singapore, Vietnam and Malaysia are members of the Trans-Pacific Partnership Agreement (TPPA) that have agreed to provide stronger protection to criminalise theft of trade secrets thus provide stronger protection than the TRIPS agreement. [15] Article 18.78 of the TPPA requires the parties to provide protections from unauthorised access of trade secrets, misappropriation of trade secrets and fraudulent disclosure of trade secrets including by state-owned entities and to provide criminal procedures and penalties.

The TPPA was the first document to criminalize theft of trade secret and economic espionage. It introduces criminalisation of trade secret theft in both online and offline environment. The provision was integrated into the TPP following the US method of criminalization of theft of trade secrets and corporate espionage under the Economic Espionage Act which was strongly advocated by President Obama. However President Trump back out from the TPP, leaving the 11 other parties to continue under a different name known as Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) which was signed on March 8, 2018 in Chile. As Malaysia is a party to the agreement Malaysia must criminalise the theft of trade secrets and economic espionage in all forms. In this regards it is worth to look at the national legal framework of the US and Japan as guideline.

IV. NATIONAL LEGAL FRAMEWORK

Incidents of online theft and commercial cyber espionage have prompted countries such as the US and Japan to criminalise theft of trade secrets and economic espionage under a different laws namely the US Economic Espionage Act was enacted under security law since the US regarded both crimes as crimes against the State. In Japan the threats are address under the Japan Unfair Competition Prevention Act (UCPA) to protect the business industry. [16] The UCPA provides both civil and criminal sanctions to combat theft of trade secrets and commercial espionage. In contrast Malaysia as the member of the CPTPP does not have any specific law that criminalise the crimes. Nevertheless Malaysia has in existence three cyber laws that indirectly can be relied upon to address these crimes. The laws are Communication and Multimedia Act 1998, the Computer Crimes Act 1997 and Personal Data Protections 2010.

A. US National legal framework on combating online theft of trade secrets and cyber espionage.

According to the National Security Agency Chief and the Commander of U.S. Cyber Command, Gen Keith Alexander the loss of the industrial information and intellectual property through cyber espionage constitutes the ‘greatest transfer of wealth in history’ that can make “our future disappearing in from of us”. [17] In the recent case between *U.S v Sinovel Wind Group Co*, Sinovel, a Chinese wind turbine company was convicted for stealing trade secrets from AMSC causing the company to lose more than $800 million. In this case Sinovel recruited an employee of AMSC subsidiary to join the Chinese Company and secretly copied information from AMSC’s computer system including the source code for some part of its wind turbine control system. This case illustrates the tremendous harm that can be done to a company due to the trade secrets theft and it illustrated how the EEA has been successfully applied to punish both the individual and the corporate body involved in committing the crimes.

Prior to the enactment of the Economic Espionage Act 1996 (EEA), the US has addressed the domestic theft of trade secret under the Depression-era Interstate Transportation of Stolen Property Act, The Mail Fraud statute and Wire Fraud statutes to combat crimes that involved trade secret theft. But these statutes has it limited scope of application and were not sufficient to combat economic espionage. [18] This limited scope has prompted the US government to enact the EEA. The act specifically criminalises corporate or economic espionage and online theft of trade secrets. The Act also imposes harsh punishment for violation of the law. The punishment range for individual is 15 years imprisonment or a

maximum fine of $500,000 or both and for organisation the maximum fine is $10 million.

Nevertheless despite having the law to enforce online theft and cyber espionage, the threat are still persistent. As a result, the US wage war against economic espionage and regard it as a crime against the state.[19] However criticisms were made questioning the enforceability of the Act since prosecution was very little. According to the EEA prosecution data based on the Public Access to Court electronic Records from 1999-2008, there were 147 defendants in 95 cases involving the EEA. In 1999, there were only 2 cases involving companies from Taiwan that were prosecuted for trade secret theft from 700 investigations that has been conducted by the FBI. Notwithstanding the existence of the Act, the U.S economy suffered $13 billon loss to economic espionage between 2011 and 2012 especially because of economic espionage by China as seen earlier. The amount decreases when both countries resort to a bilateral agreement to respect each other intellectual property. To expedite investigation and prosecution the FBI has formed an "Economic Espionage Unit to combat the specific threat' however critics said economic espionage still posed dangerous threat to the US company. Thus apart from criminal sanctions the law in the US provides the victims of trade secrets theft and cyber espionage with civil remedies under the Uniform trade Secrets Act and the Defence Trade Secret Act. In all three legislations, the definition of trade secrets are synchronised and trade secrets in regarded as valuable commodity whether in whatever form.

B. Japan National legal framework protecting trade secrets.

In comparison to the US, Japan was a bit late to criminalise theft of trade secrets and economic espionage due to cultural influence of protecting employee mobility and loyalty to work place. Nevertheless after big cases were litigated over the couple of years involving misuse of trade secrets by employee who defected and worked with foreign entity, Japan started her move to criminalise trade secrets theft in whatever means by providing recourse under the Unfair Competition Prevention Act (UCPA). The Act regulates trade secret infringement as one of the acts of unfair competition and criminalizes trade secret misappropriation as an offence under Article 21 of the UCPA. Comparing the approach of the US and Japan, Japanese approach is to protect the business industry by preventing unfair competition. This is in line with the Paris Convention and TRIPS even though criminal sanction was not specifically provided under the convention and TRIPS.

The Act has undergone several revisions. In 2003 the Act introduced criminal recourse and from 2005 -2009 several revision were made to strengthening the punishment. In 2011 revision was made to deal with the maintenance of criminal procedures for appropriate protection of trade secrets in courts. Despite the above, a major amendment was made to the Act in 2015 amending both the civil and criminal articles with the purpose to increase deterrents against infringement of trade secrets. [20] This was made after the occurrence of two important trade secrets infringement cases namely the Nippon Steel & Sumitomo Metal Corporation in 2012 and Toshiba Corporation in 2014.

In brief, the amendment broadened the criminal protection coverage and increase deterrents. In relation to coverage, four elements were introduced namely punishment is extended to subsequent dishonest acquisition without any limit, punishment for attempted infringement whereby punishment is now applicable to attempted infringement of trade secrets, regulation of distribution of trade secret infringing products and lastly punishment of trade secret crimes outside Japan which make wrongful acquisition is a crime outside Japan.

Under the heading of deterrents, prosecution of the offender can now be made in the absence of complaint unlike before where prosecution will only take place upon complaint by the injured party. Lastly the Act introduces procedures for discretionary confiscation of profits and import ban on goods infringing trade secrets. In relation to increase deterrents, the penalty for natural person is 20 million Yen and for judicial person 500 million yen. It imposes heavier fine against specific crimes which negatively affect the Japanese economy.

Since the US has back out from the TPPA. Japan is expected to lead the new CPTPP. This will influence the development of the Malaysian law to address the issue of theft of trade secrets and corporate espionage.

C. Malaysia

The ransom ware attack in Malaysia in 2017 and series of cyber crimes that occurred indicated that Malaysia is not free from the above threats. This has been confirmed by the Cyber Security Malaysia, the Royal Malaysian Police and computer security company.[21] This incident also questioned the adequacy of the Malaysian law to address this problem. [22] Accordingly there is a need to address the threats immediately especially now when Malaysia is a member of CPTPP. The threats are not limited to hacker but also organised crimes and national states that are targeting the trade secrets and valuable information of commercial entities in this country. Such crimes have potential to affect the business and commercial industry in Malaysia as well as the economy of the country. Looking at the US and Japanese approaches, Malaysia has several choices whether to regard the crime as a crime against the state as in the US thus criminalise it under national security law or to protect the industry under unfair competition law following the Japanese. The other choice is to regulate online theft and cyber espionage by enhancing the cyber laws.

While the legal framework to on these new crimes is still in dilemma, the Malaysian government has placed several strategies to address the threats. Firstly is to place digital development a high priority in the national agenda. On this point the Minister of Science Technology and Industry (MOSTI) states "With more people connected to the internet…….. It is our collective responsibility to ensure that Malaysians are safe from unscrupulous individuals or criminal organisation that thrive unsuspecting cyber victims for personal gain." The duty to ensure this policy is achieved is entrusted to the Royal Malaysian Police which has identified three (3) threat actors namely within / via insiders, using malware and external attacks by former employee and

competitors. Alert on the impact of these crimes, the Malaysian Government has set up the Police Cyber Investigation Response Centre (PCIRC) and the Cyber Security Malaysia or CSM set up the Cyber Threat Intelligence Program (CTIP) in collaboration with Microsoft Malaysia. [23] The main reason for such set up is to collect and distribute the existing actionable cyber threat information to help Governments, networks owners and Internet Services Providers identify and help machines that have been affected by malware.

To work on this matter, the Cyber Security of Malaysia (CSM) has been entrusted to provide specialised cyber security services aiming at preventing or minimizing disruption to the national critical information infrastructure to protect the public, the economy and government services. The CTIP that is set up by CSM acts as a powerful big-data resource that allows CSM to have the statistic and to have a better situational awareness of existing cyber threats and potential malware related security issues in Malaysia. With such collaboration, CSM can monitor and control the real-time cyber threat and keep up with the fast-paced and ever-changing cybercrime landscape and work with business to eliminate cyber espionage and theft of trade secrets and other cyber attacks.

One identified technique of stealing confidential business information or trade secrets is through malware. This malware that distributed by the criminals can turn a computer into a robot or zombie which then allows the victims computer to perform automated malicious tasks over the internet without their knowledge. Through such botnets, criminal can steal personal data, trade secrets and commit financial fraud. Since the attack occurred without the knowledge of the owner, the best method to fight or combat cybercrimes comes from awareness and prevention. Apart from botnets, business and consumers should be aware that unsecure supply chain such as usage of counterfeit software invites malware, thus provides easy target for hackers and cyber criminals. A survey conducted by National University of Singapore (NUS) and IDC Cybersecurity Research showed that out of 203 new PCs purchased in 11 countries with counterfeit software installed on them, 61% of those PCs were pre-infected with malware. [24]. The detrimental effects and inherent risks of counterfeit software is that the malware that is loaded onto counterfeit software can infects and steal information from a victim's computer. Once the malware is planted into the computer, the cyber criminals are then able to use that information to illegally enter and abuse the victim's online services, including online bank accounts, email system and social networking sited. This can have damaging effects on user's financial security and personal safety as well as pose a risk of corporate espionage and surveillance. On this aspect CSM said "Using a computer with counterfeit software is just like opening doors to cyber criminals. People and business who use counterfeit software have no guarantee that their personal, confidential, sensitive data, activities and communications online using these devices will be safe from cyber criminal that intend to do harm."

However to ensure consumer and companies to buy a genuine and trusted software ecosystem is a challenge especial when costs become a main concern. Nevertheless business must take proactive steps to ensure that they are safe online particularly when purchasing a new PC such as installing a genuine copy of the operating system, buy the product from a trusted seller or reseller and ensure all software purchase come in their original packaging and to report any pirated software.

While the policies are catching up with the latest development in addressing online theft of trade secrets and cyber espionage, the law in Malaysia is lacking behind to criminalise these two crimes. These could be due to the following reasons namely (1) there is no clear definition of trade secrets and cyber or economic espionage, (2) both crimes are new crimes that is not covered by any of the national security laws or Penal Code in Malaysia, (3) Malaysia does not have unfair competition law and (4) the existing cyber laws does not specifically govern online theft of trade secrets and cyber espionage.

In contrast to the US Economic Espionage Act and Japan Unfair Competition Prevention Act, there is no definition of online theft and cyber espionage in Malaysia. The Penal Code only defines theft in relation to tangible property thus exclude trade secret and valuable information which is considered as intangible property. The Malaysian security laws also lack definition of commercial or economic or industrial espionage. Accordingly online theft of trade secrets and cyber espionage does not fall within the crimes against the state. Although protecting business community is part of the national agenda, Malaysia only have competition law and have yet to enact unfair competition law as in Japan. Nevertheless the relevant law to govern cyber crimes is the Communication and Multimedia Act 1998(CMA) and the Computer Crime Act 1997 (CCA). Both legislations have been enacted with the view to protect Malaysia from any cybercrime and computer misuse. Although not specifically directed to online theft of trade secrets and commercial espionage, the CMA does protect trade secrets from these crimes. Section 233 makes it an offence to obtain information by improper use of network facilities or network services to transmit any communication that is considered as threat or abuse. However this provision has been criticised to be too wide and are more relevant to govern matters relating to freedom of expression rather than protecting trade secrets even though trade secrets falls within the meaning of 'content' under the Act. Perhaps section 234 may be relied on by the owner of trade secrets.

Clause 1 (a) and (c) of section 234 prohibits interception of any communication and content of the communication. This may include act of cyber espionage whereas clause 1(b) prohibits disclosure of any trade secrets that have been obtained through intercept of communication, thus may covers online theft of trade secrets.

Apart from CMA, CCA especially under section 3, 4, 5 and 9 can also be used to criminalise online theft of trade secrets and cyber espionage. Section 3 governs unauthorised access to computer materials and section 5 deals with unauthorised modification of contents of any computer. Thus planting a malware in a computer is an offence under both provisions whereas any employee or insider who wrongfully communicating any password, number or code whom he is

duly authorised to communicate can be charged under section 6 for wrongful communication.

If the online theft of data includes for example customers list, subscribers list and personal data of person which are regarded as trade secrets, then the crime is punishable under Section 9 and section 130 of the Personal Data Protection Act 2010 (PDPA). Section 130 deals with unlawful collecting, processing and etc of personal data while section 9 provides for security of the personal data.

Since online theft of trade secrets and cyber espionage are relatively new in Malaysia, the cyber laws did not directly govern and regulate these threats. The cyber laws as mentioned above could either be too wide or too specific and mechanism such as imposing obligation on victims to report any incident of data leak and disclosure of trade secret was not covered. Another pertinent issue is the punishment for online theft and commercial espionage. Is the punishment under the CMA and CCA sufficient? Will it cover subsequent recipients of the stolen trade secrets as seen under the Japanese law. There are a lot of legal uncertainties relating to this matter thus until the law is strengthen, the government or relevant authority must provide the necessary administrative measure to reduce the threat of online theft and cyber espionage in Malaysia.

V. Conclusion

The unprecedented value of a company trade secrets has make the company a target of online theft and cyber espionage. It is thus challenging for a company alone to protect its trade secrets from competitors, hactivits and state sponsored espionage without the government involvement. In the US and Japan, the respective government has adopted a different legal approach in combating these crimes that is suitable to the need of the country. In comparison Malaysia has a lot to learn to ensure the legal landscape is suitable to protect business from online theft and cyber espionage. Since the awareness and initiative have been taken by the relevant government agencies to address these threats, the most sensible legal mechanism is to enhance the existing cyber laws.

ACKNOWLEDGEMENT

This research is sponsored by the Ministry of Higher Education, Malaysia under the Fundamental Research Grant Scheme.

REFERENCES

[1] WIPO “Trade Secrets Are Gold Nuggets: Protect Them”. WIPO Magazine, April 2002.

[2] Pierluigi Paganini, “10 Biggest Cyber Espionage Cases” Dec 11, 2017. http://securityaffairs.co/wordpress/66617/hacking/cyber-espionage-cases.html

[3] Baker Makenzie, The Board Ultimatum: Protect and Preserve. 2017. Euromoney insitutional investor thought leadership at www.euromoneythoughtleadership.com/TheBoardUltimatum

[4] Elizabeth A. Rowe, RATs, TRAPs, and Trade Secrets, 57 B.C. L. Rev. 381 (2016), available at http://scholarship.law.ufl.edu/facultypub/

[5] Detica Report. The Cost of Cybercrime. Cabinet office at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

[6] Symantec Internet Security Threat Report April 2017.

[7] Bakermakenzie, Trade Secrets theft, a trillion dollar problem? 2018 at http://insight.bakermckenzie.com/trade-secret-theft-a-trillion-dollar-problem

[8] Kapersky Lab Corporate threats: Overview of the year December 2013 at https://www.kaspersky.com/about/press-releases/2013_corporate-threats-overview-of-the-year

[9] Pierluigi Paganini, “10 Biggest Cyber Espionage Cases” Dec 11, 2017

[10] Kaspersky security bullettin 2013 https://media.kaspersky.com/pdf/ksb_2013_en.pdf

[11] Create.org: Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential threats February 2014.

[12] OECD. approaches to the Protection of trade secrets https://www.oecd.org/sti/ieconomy/Chapter3-KBC2-IP.pd

[13] Brian T. Yeh. Protection of Trade Secrets: Overview of Current Law and Legislation. Legislative Attorney April 22, 2016

[14] R. Baron and M. Pigeon “Adapting the EU Directive on Trade Secrets ‘Protection’ into National Law. A transposition guide for legislators and civil society organizations.” Corporate Europe Observatory, February 2017. Cook, T. (2014). The proposal for a Directive on the Protection of Trade Secrets in EU Legislation.

[15] U.S Chamber of Commerce. The Case for Enhanced Protection of Trade Secrets in the Trans-Pacific Partnership Agreement. Covington& Burling LL.P

[16] R. Melanie “A Comparative approach to Economic espionage: Is any nation Effectively deaing With This Global threat. University of Miami Law Review. Vol 70, pp 757-829.

[17] J. Rogin, NSA Chief: cybercrime Constitutes the “Greatest Transfer of Wealth in History” The Cable, July 2012., R. A. Khan “Economic espionage in 2017 and beyond: 10 Shoking Ways They are Stealing Your Intellectual Property and Corporate Mojo”. Business Law Today. May 2017.

[18] K. Calia, D. Fagan, J. Veroneau, G. Vetere, K. Eichensehr. Economic espionage and Trade Secret theft: An Overview of the Legal Landscape and Policy Responses. Covington & Burling LLP, September 2013.

[19] Van Arnam, Robert C. "Business war: Economic espionage in the United States and the European Union and the need for greater trade secret protection." *NCJ Int'l L. & Com. Reg.* 27, 2001, p 95.

[20] Jonesday, Japan Strengthens Deterrence measure. Available at http://www.jonesday.com/files/Publication/2b509a75-1a2e-4a7d-8b32-6c82a6edeb8d/Presentation/PublicationAttachment/b7bb32d1-b712-4021-b090-7c98eceee9b4/Japan_Strengthens_Deterrence_Measures.pdf

[21] Computerworld Malaysia - Malaysia at risk: CyberSecurity Malaysia chief covers espionage and state level attack. Computer World malaysia. April 2017.

[22] Melissa Darlyne Chow, Expert: Malaysia Il-prepared for cyber attacks. http://www.freemalaysiatoday.com/category/nation/2017/12/30/expert-malaysia-ill-prepared-for-cyber-attacks/

[23] Azizul Rahman Ismail. Politically motivated hactivism is the second biggest threat in Malaysia. Available at http://www.hardwarezone.com.my.

[24] http://news.microsoft.com/en-my/2014/11/12/cybersecurity-malaysia-an-microsoft-keep-malaysians-safe-online-through-joint-malware-threat-intelligence-initiative/