International Journal of Business and Society, Vol. 21 S1, 2020, 49-65

BUSINESS UNDER THREAT: THE CRIMINAL LIABILITY OF TRADE SECRET THEFT IN MALAYSIA?

JuriahAbdJalil[♣]
International Islamic University Malaysia

Halyani Hassan
International Islamic University Malaysia

NasarudinAbd Rahman
International Islamic University Malaysia

Raja BadrolHisham Raja Mohd Ali
International Islamic University Malaysia

Duryana Mohamed, Ahmad Najib
International Islamic University Malaysia

ABSTRACT

Maintaining and ensuring secrecy of valuabletradesecret offers competitive advantage to its owner over the competing rival. Because of this, the trade secret is often subject to various threats ranging from misappropriation, theft and corporate espionage launched by rivals and also the employee. Such threats can impede growth of the victimized firms and discourage further innovative and inventive endeavor. One of the ways to deter such offence is by providing specific criminal sanction for the theft of trade secret as practiced in the US and Japan. The US regards theft of trade secrets as a federal crime under the Economic Espionage Act 1996 and in Japan, theft of trade secret is a crime under the Unfair Competition Law. In comparison, Malaysian law does not provide any specific legislation criminalizing theft of trade. But being a member of the TTPA, Malaysia is required to criminalize such theft. This article analyzes the competency of the existing criminal, cyber and national security laws in Malaysia to address the issue. In doing so, the practice of the US and Japan is taken as example to shed light as to the proper implementation of criminal prosecution against the theft of trade secret.

***Keywords**:* Trade secrets theft; Misappropriation of business information;Confidentialinformation;Corporate espionage.

Received: 11 February 2019
Accepted: 20 August 2019

[♣]Corresponding Author. Department of Legal Practice, Ahmad Ibrahim Kulliyyah of Laws, International Islamic University Malaysia, Kuala Lumpur, Malaysia. Tel: (603) 61964366, E-mail: juriah@iium.edu.my

1. INTRODUCTION

Trade secrets are 'fundamental building blocks' that drive investment, innovation and economic growth (Create, 2014). Due to this reason trade secrets are often subject to various threats ranging from misappropriation, theft, corporate and economic espionage launched by the rivals, employee and state sponsored. To the small and medium business, losing trade secrets will kill the very existence of the business. Similar fear occurred among big businesses particularly those that have spent billions of dollars to conduct research and development to produce new product. The fear of losing trade secrets is genuine because of its impact on competitive advantage, financial returns and reputation of the business. But protecting trade secret especially in this digital aegis most difficult and challenging. Competitors and criminal can resort to various measures to obtain the trade secrets using both physical and electronic means to intrude, hacks, using malware and other gadgets to obtain the trade secrets. The impact of this theft and corporate espionage is great because it reap the owner of the trade secrets the economic benefits and profits that could be derived from it. Based on this, developed countries such as US and Japan are criminalizing theft of trade secrets and corporate and economic espionage under two different laws. The US enacted the Economic Espionage Act 1996 that criminalize theft of trade secrets and economic espionage whereas Japan punished such acts under the Unfair Competition Prevention Act 1991. UK and Malaysia however do not have specific law that criminalizes theft of trade secrets and economic espionage even though in the UK concerns on this issue has been raised by Sir Edward Boyle in 1968 who said "It is not too much to say that we live in a country where …the theft of the board room table is punished far more severely than the theft of the board room secrets" (Hansard, 1968). Since the impact of theft of trade secrets, corporate or economic espionage is huge not only to the business but also to the economy of the country, three questions arose here namely first, should such illegal act be criminalized and the culprit be punished, second, under which law - national security law, cyber law or Penal Code?

2. THE ISSUES IN QUESTION

Some authors equate theft of trade secrets and economic espionage as a new form of commercial piracy, thus since piracy is a crime, theft of trade secrets and the like should be regarded as crime. Similarly in relation to official secret, the Official Secrets Act was enacted to punish those who has abstracted or divulged government secrets in order to protect the security and integrity of a country, thus stealing, disclosing and divulging of commercial secrets that is the life blood of a company should also be treated the same.

Nevertheless such comparison does not apply in the like manner for theft of trade secrets especially in Malaysia. This could be due to several factors namely first, the intangible nature of the trade secrets themselves that makes them fall outside the scope of the criminal law of theft which is tied up to the physical object or tangibility of property. Second, the wide concepts of trade secrets challenge the scope of criminal liability and will depend on whether the information comes within the definition of trade secrets. Thirdly, the burden of proof lay down by the Trade Related Aspect of Intellectual Property or TRIPs's requirement namely the information must be a secret, have commercial value for being a secret and reasonable efforts taken to protect and maintain it secrecy are difficult to proof. The 'reasonable efforts' requirement have cause difficulty especially to the

owner of a trade secret to prove their case for breach of confidential information in civil litigation. The same need to be proven in criminal cases. These issues will be discussed and highlighted in this paper. Before discussing further it is important to know what is trade secrets and why should it be protected.

3. WHY IS IT IMPORTANCE TO PROTECT TRADE SECRETS?

A study conducted by the European Commission found that there is a consensus among economists that regards trade secrets play an important role in protecting the returns to innovation and that trade secret protection is an integral and important part of the overall system of protection available to EU firms to protect their intangible assets, like patents and copyrights" (European Commission, 2013)In the US case of *Kewanee Oil Co v Bicron Corp*, 416 U.S 470, 493(1974) the court observed that "trade secret law promotes the sharing of knowledge and the efficient operation of industry; it permits the individual inventor to reap the rewards of his labour by contracting with a company large enough to develop and exploit it." Accordingly, trade secret protection promotes innovation and economic efficiency (Saunders & Evans, 2017).

Due to it nature of importance, trade secrets are targeted upon by corporate competitors, malicious insider and former employee, hackers and even state actors or foreign government. According to US Chamber of Commerce and OECD, the act of misappropriation or theft of trade secrets and espionage through physical and cyber means has caused billions of dollars in annual losses to business entity and national economy globally (US Chamber of Commerce, 2013; OECD, 2016). On this aspects, Pricewaterhouse Coopers and the Center for Responsible Enterprise and Trade (Create.org) estimated loss to the value of trade secret theft in the US in 2014 to be between USD200 billion to USD550 billion per year (CREATE, 2014). In this regard the effect of threat are twofold, firstly "tremendous loss of revenue and reward for those who made the inventions and secondly the theft undermines both the means and incentive for entrepreneurs of new inventions and industries that can further expand the world economy" (IP, Commission, 2013).In this regard misappropriation and theft of trade secrets as well as corporate espionage posed real risk to business entity and has potential to stunt not only innovation, growth, development and investment of business entities but also national economy.

In the EU, the directive on trade secret protection that is Directive (EU) 2016/943 on the protection of undisclosed knowhow and business information (trade secrets) against their unlawful acquisition, use and disclosure was issued because of the threat to theft of trade secrets. Recital 4 of the EU Directive further explain the challenge that requires harmonization and stronger civil protection of trade secrets - "Innovative businesses are increasingly exposed to dishonest practices aimed at misappropriating trade secrets, such as theft, unauthorized copying, economic espionage or the breach of confidentiality requirements, whether from within or from outside of the Union."

A survey conducted for the European Commission in 2013 demonstrates the significant scope of this problem. The survey found that over the past 10 years, approximately one in five respondents experienced at least one attempt or act of misappropriation within EU countries and nearly 40 percent of respondents believe that risk has increased during the same period (European

Commission, 2013). The directive was therefore aim to cater for this issue and member starts should implement the directive into their national laws starting from 9 June 2018. This will ensure that the trade secrets holder has the right to apply for measures, procedures and remedies provided in the directive in order to prevent or obtain redress for the unlawful acquisition, use or disclosure of the trade secrets (Cook, 2014).The directive however focuses on civil remedies and does not mandate for criminal liability. Nevertheless the EU did not interfere with the legal system of any member countries that has criminalized theft of trade secrets.

Similarly, in Japan and South Korea, the Japanese government for example found that more than 35 % of respondents manufacturing firms reported some form of technology loss. While South Korea estimated the economic loss due to economic espionage will tripled. In fact statistic shows that a total of 43 confirmed espionage case was uncovered in the year 2009. This raised further concern when a senior judge from the Seoul Central District Court was reported to say that "technology leak oversea should be prosecuted severely" (Paik & Lim, 2010)

In Malaysia, the threats exist although are not apparent since there was no reportor research conducted to analyze the value loss due to misappropriation or theft of trade secrets trade secrets. However there are several civil actions on misappropriation of trade secret and breach of confidential information brought by employer against the employee. The method of misappropriation includes downloading of documents into personal computers, on to flash drive, stealing of physical documents, using insider to supply documents and breach of non-disclosure agreement to third party. In the case of *Worldwide Rota SdnBhd v Ronald Ong CheowJoon*[2010] MLJU 288, the court rely on the law of breach of confidential information to find the defendant, a former employee who start a new similar business to be liable but the third person who committed the corporate espionage or acted as a spy for him was only called to be the witness. In the case of *Dibena Enterprise SdnBhd v Huawei Technologies (Malaysia) Sdnbhd&Anor*[2012] MLJU 154 the court considered the 1st defendant argument on the impact of commercial espionage on it business and other companies that have dealing with it, before limiting the plaintiff application for discovery of documents which contain sensitive commercial trade secret between the defendant, a company in Hong Kong and Telekom Malaysia Berhad. These two civil cases acknowledge the existence of corporate espionage and theft of trade secrets in Malaysia.

Further, the attack by the 'ransomware' virus in Malaysia in May 2017 has brought warning to the business entities of the cyber-attack and hacking that can be done by external factors. In fact in those incidents only 2 out of 16 business entities or organization that have been attacked made a report to the police to allow investigation to take place. Such attacks indicated that Malaysia is also a target. On this point the CEO of Cybersecurity Dato Dr. Haji Amiruddin Abdul Wahab urged the public to report any type of ransonware attacks to CyberSecurity Malaysia. He also reminds system administrators to patch their systems and keep them from clicking on suspicious emails and files. (The Sundaily, 2017). Therefore cybercrime such as hacktivism, cyber espionage are already existing in Malaysia. These attacks can take the form of any cyber offensive action ranging from web defacement, system intrusion, cyber espionage, and malicious software (malware) infection to high-scale cyber-attacks with diverse political and economic motives. The cyber-attacks which include cyber espionage are nowadays committed at the organizational and state levels. The attacks are becoming more sophisticated, covert and continuous especially with APT or Advance Persistent Threat which can be made based on well-coordinated plan to achieve both

business and political motives. He added that with Malaysia increased investment and diversifying economies, Malaysia can be a potential target for APT cyber attacks.

There are however a downside to criminalizing theft of trade secret. Criminalizing such act may affect the employment market since most theft of trade secrets are committed by employee.

4. COMBATING THEFT OF TRADE SECRETS AND ECONOMIC ESPIONAGE IN THE US, JAPAN AND OTHER SELECTED JURISDICTIONS

To protect trade secrets from these risks, the US, Japan, EU and some countries such as South Korea has taken steps to strengthen the legislation in both civil and criminal aspect. In all the above countries, trade secrets were first protected under civil action providing civil remedies to the owner of the trade secrets. In some countries the protection is afforded firstly by the State law, such as in the US, and by individual member countries the EU. However the difficulty to enforce the law especially in cross border lead to the federalization of the law in the US and the harmonization of the law in EU through EU directive as seen above. Trade secrets protection to criminal law was later enhanced in the US but not in EU. In contrast to the US and EU, Japan and South Korea provide both civil and criminal protection under the Unfair Competition Prevent law and Unfair Competition and Trade Secret Protection Act.

The US has enacted several laws at the federal level to enhance the protection of trade secret theft beginning with harmonizing the various state law regulating trade secrets by enacting the Uniform Trade Secret Act (UTSA). According to the Uniform Law Commission, the UTSA contained codification of common law principle that is practiced by States with proper clarification of rights and remedies. The reason for such codification was first to assist in balancing the commercial importance of state trade secret law to interstate business. Second, there is undue uncertainty concerning the parameters of trade secret protection and the appropriate remedies for misappropriation of a trade secret even in States where there has been significant litigation. Accordingly the Pro harmonization law observed that due to technological and economic pressures, "industry continues to rely on trade secret protection despite the doubtful and confused status of both common law and statutory remedies. Clear, uniform trade secret protection is urgently needed. (Editors, 1971).

To achieve the aims, the UTSA defines trade secrets under section 1 (4) as "information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy. This definition is in line with TRIPS agreement that highlights the economic value of trade secrets. In brief a trade secret refers to exclusive knowledge of economic value which has been generated by the owner who has an interest in protecting its value. Thus, according to the Uniform Law Commission, "the essence of trade secrets protection is that a person with a trade secret may have a remedy in equity and law if the secrets had been misappropriated". This definition was later adopted in the Economic Espionage Act 1990 and the recent Defence Trade

Secret Act 2017. UTSA also defines the terms misappropriation as acquiring a trade secret by improper means and what constitute improper means include theft, bribery and misrepresentation. The remedies under the Act include injunctive relief, damages for actual loss and unjust enrichment as well as exemplary damages for willful and malicious misappropriation. At this junction misappropriation of trade secrets is still a civil action and not criminally sanctioned.

However harmonizing the law does not deter the theft of trade secret and economic espionage. The US still faced the loss of billions of dollars due to theft of trade secrets. As a result the Economic Espionage Act was enacted in 1990 and raised the status of the theft of trade secrets from civil malfeasanceto a felony against both firms and potential thieve (Searle, 2012) This new incentive also injected the principle of criminal deterrent to trade secret theft and that the prime role of the punishment in criminal cases is the deterrent effect. The EEA criminalized theft of trade secrets under section 1832 and economic espionage under section 183. Both provision has clearly explain the criminal acts for theft of trade secrets and for economic espionage as seen in Table I below

Table 1: Criminal Acts for Theft of Trade Secrets and Economic Espionage Under the EEA

Theft of trade secrets - Section 182	Economic espionage – section 183
"(a)Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly— (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information; (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; (4) attempts to commit any offense described in paragraphs (1) through (3); or (5)conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,	Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly— (1) steals, or without authorization appropriates takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret; (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; (4) attempts to commit any offense described in any of paragraphs (1) through (3); or (5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy

The same criminal acts apply to both provision and the elements that differ the two criminal actions are: for theft of trade secrets is when trade secrets is used for intended for use in interstate or foreign commerce to the benefit of anyone other than the owner and whilst for economic espionage the offence is committed for the benefit of any foreign government or foreign agent. Nevertheless both

provisions provide severe punishment to both individual and organization involved in committing the offence. Under section 182 an individual can be fined or imprisoned not more than 10 years or both and for organization shall be fined not more than the greater of USD 5,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret. In case of economic espionage, a person can be fined not more than $5,000,000 or imprisoned not more than 15 years, or both and If the act is conducted by an organization, the organization shall be liable to a fine not more that "the greater of $10,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided."

Despite the existence of the EEA, only 147 defendants were charged under the EEA from 1996 to 2008 with most threats came from insiders or employee measuring to 76% and only 25 defendant's outsiders that consist of competitors and non-employees (Searle, 2012). The effectiveness of EEA was doubted and further criticized when the country continues to lose billions of dollars of trade secrets due to rapid technological advances and cyber espionage especially by Chinese government. The technological advancement provides greater connectivity and data storage but at the same time allows for breach of corporate network and acquisition of sensitive corporate data through cyber espionage. On this issue the U.S Department of Defense noted that "[e]very year, an amount of intellectual property larger than that contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government departments and agencies." (Department of Defense, 2011). This was further confirmed by General Keith Alexander, the head of the National Security Agency and U.S Cyber Command in 2012 who stated that IP theft due to cyber espionage is the "greatest transfer of wealth in history," which is "likely . . . comparable to the current level of U.S. exports to Asia—over $300 billion" (IP Commission, 2013). According to Saunders and Evan, the threat of theft of trade secrets still persistent and the main reason for the failure of the Act was due to the lack of interest among the federal prosecutors to bring charges under the Act unless the case involves theft of trade secrets owned by large corporation or economic espionage by agents of a foreign government (Saunders & Evans, 2017). Further in relation to the economic espionage by the Chinese government, the US has entered into the bilateral agreement with China where both countries agreed in principle among other things "to provide timely responses to requests for information and assistance concerning malicious cyber activities, refrain from conducting or knowingly supporting cyber-enabled theft of intellectual property, pursue efforts to further identify and promote appropriate norms of state behavior in cyberspace within the international community, and establish a high-level joint dialogue mechanism on fighting cybercrime and related issues" (Rollins, 2015). However discussion is still going on under the Trump administration.

Apart from the EEA, there are other federal laws that are available to prosecute theft of trade secrets and economic espionage such as The Computer fraud and Abuse Act, the Federal Wiretap Act and Stored Communication Act, and Electronic Communications Privacy Act. At state level, most States in the US has criminal laws that criminalize theft of trade secrets. This law provides alternative to the prosecutor to charge and prosecute theft of trade secret apart from the EEA. Thus in brief the US law provides both civil remedies for misappropriation of trade secret and criminalize theft of trade secrets and corporate espionage which are regarded as crime against the

state. In 2015 the Defense to Trade Secrets Act was enacted making a civil action for misappropriation of trade secret a federal law thus allowing both civil and criminal law to be commenced against the misappropriator and the criminal.

In Japan and South Korea the protection of trade secrets from theft and misappropriation is afforded by the law of unfair competition. The main reason for introducing the law is to protect the industry from unfair business practice and to encourage healthy competition between parties. In Japan, similar to the US, series of attacks involving the theft of the secret information belonging to big companies have triggered the government to enact the Unfair Competition Prevention Law 1990. These include big companies such as Nippon & Sumitomo Metal Corporation, Toshiba Corporation and Benesse Holdings, Inc. According to Japan Patent Office (JPO) "Criminal Protection of Trade Secret Technical data which has not yet been subject to a patent application, in addition to production know-how, sales manuals and customer information are all sources of competitiveness for businesses, and as such are kept as trade secrets. However, as competition intensifies on a global basis and information technology develops, there are growing concerns over damage to competitiveness due to trade secret leaks. Thus, the Unfair Competition Prevention Law provides criminal penalties against trade secret infringement" (Japan Patent Office, 2008).

The JPO further explains that there are two types of acts constituting trade secrets infringement namely first – the act of acquiring, using or disclosing trade secrets for the purposed of unfair competition in violation of the owners maintenance through fraud, assault, threats or other unlawful means. Accordingly act of misappropriating trade secrets originally obtained in a lawful manner by former employee fall within this category. The second type refers to the acts done by officers or employees of a company to use or disclose to the outsider trade secrets for the purpose of unfair competition. However due to continuous attacks on big company and disclosure of trade secrets by former employer has urged the government of Japan to amend the law in 2016. The amendment enlarged the scope of criminalizing theft of trade secrets and economic espionage. The government and the Japanese companies regard trade secrets infringement as a serious risk of corporate information leakage thus the current governing Act was revised to enhance the protection of trade secrets. Article 21(1) of UCPA provides the Penal Provision. In relation to criminal aspects the revision focuses on two aspects (Nakajima, 2017) as seen in Table 2.

Table 2: Revise Scope of Protection Under the Japan Unfair Competition Prevention Law

Expansion of punishment coverage	Upgrading of deterrents by strengthening penalties
○ Punishment of subsequent acquirer has been added making those whoever subsequently acquire the trade secrets will be punished. ○ Regulation of assignment, import/export, etc., of trade secret infringing products ○ Punishment for attempted infringement of trade secrets ○ Punishment of trade secret crime outside Japan	○ Increase in fine for the crime of trade secret infringement ○ Heavier fine for the crime of trade secret infringement outside Japan ○ Prosecutable without a complaint from the trade secret owner ○ Discretionary confiscation and additional levy of crime proceeds.

The government participation in revising the scope of protection indicates the commitment of the country to protect their business industry and to meet the demand of the business industry to enhance trade secret protection. Similarly in South Korea, trade secrets theft is criminalized under the Unfair Competition and Trade Secret Protection Act (UCPA) and Industrial Technology Act. Article 18 of UCPA extend to criminalize the act of use or acquire a company trade secrets in a foreign country or disclosure of the trade secrets to a third party knowing it will be used in the foreign for the purpose of obtaining improper benefits or damaging the company. The punishment is quite severe wherein the person if liable could be imprisoned with labour not exceeding ten years or to a fine exceeding twice of pecuniary profit to not exceeding ten times of it.

As seen from the above discussion, countries adopt different mechanism and different legal regime to protect trade secrets. The US and Japan as well as South Korea provide both civil and criminal protection. The US criminalizes the act of theft and economic espionage under a specific national law whereas Japan and South Korea criminalizes the acts under the unfair competition law which more an industry oriented and in line with Paris Convention and Trips. In all three jurisdictions, the law is clear on the definition of trade secrets and the scope of the crimes is adequately defined with severe punishment imposed. So what is the position in Malaysia and being a member of the TPPA, Malaysia is obligated to criminalize both acts but how should Malaysia incorporate the requirements mentioned under Article 18.78 of the TPPA as seen below in Table 3.

Table 3: Provision in TPPA

Article 18.78
Subject to paragraph 3, each Party shall provide for criminal procedures and penalties for one or more of the following: (a) the unauthorized and willful access to a trade secret held in a computer system (b) the unauthorized and willful misappropriation of a trade secret, including by means of a computer system; or (c) the fraudulent disclosure, or alternatively, the unauthorized and willful disclosure, of a trade secret, including by means of a computer system. Paragraph 3 "With respect to the relevant acts referred to in paragraph 2, a Party may, as appropriate, limit the availability of its criminal procedures, or limit the level of penalties available, to one or more of the following cases in which (a) the acts are for the purposes of commercial advantage or financial gain; (b) the acts are related to a product or service in national or international commerce; (c) the acts are intended to injure the owner of such trade secret; (d) the acts are directed by or for the benefit of or in association with a foreign economic entity; or (e) the acts are detrimental to a Party's economic interests, international relations, or national defence or national security

In brief that 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.

5. CRIMINALIZING THEFT OF TRADE SECRET AND ECONOMIC ESPIONAGE IN MALAYSIA

In Malaysia offence against the state is govern by three different Acts and Malaysia does not have unfair competition law, instead Malaysia has competition law that has very little relation to the protection of trade secrets. In view of the above, there are several possibilities for Malaysia to adhere to the requirements of the CTTPA. Firstly under the national security laws namely Security Offence (Special Measures) Act 2012 (SOSMA), Prevention of Terrorism Act 2015 (POTA) and National Security Council Act 2016 (NCSA), second under the cyber laws especially the Communication and Multimedia Act 1998 (CMA) the Computer Crimes Act 1997 (CCA) and thirdly under Penal Code. Each and every laws, however has their own set back and weakness which may affect the adequacy of the act to protect and deter theft of trade secrets and economic crimes.

There are two important issues that must be resolved before the criminalization of theft of trade secrets and economic espionage could take place namely the issue of definition of trade secrets and the intangible nature of trade secrets. In relation to the definition of trade secrets, there is no statutory definition of trade secrets in Malaysia. This is because trade secrets protection comes under common law where definition of trade secrets is defined by case law. On this point, the Malaysian court has referred to several English cases for definition of trade secrets within the scope of confidential information such as the case of *Coco & A.N Clark (Engineers) Ltd* [1969] RPC 41, and *Facenda Chicken's* case (1986)1 ALL ER 62. Neill LJ in *Facenda Chicken's* case explains the difficulty in defining the scope of trade secrets in the following manner "It is clearly impossible to provide a list of matters which will qualify as trade secrets or their equivalent. Secret processes of manufacture provide obvious examples, but innumerable other pieces of information are capable of being trade secrets, though the secrecy of some information may be only short-lived. In addition, the fact that the circulation of certain information is restricted to a limited number of individuals may throw light on the status of the information and its degree of confidentiality." The case of *Coco & Clarke* provides the qualification for confidential information namely First, the information must be of a confidential nature, second is that the information must have been communicated in circumstances importing an obligation of confidence and thirdly, there must be an unauthorized use of the information to the detriment of the person communicating it. In the case of *Schmidt Scientific Sdn Bhd V Ong Han Suan [1997] 5 MLJ 632*, Justice Kamalanathan Ratnam J. explained "trade secrets are not limited to manufacturing processes or secret formulae but extend to information relating to the list of names and addresses of the customers and suppliers, specific questions sent to the customers, costs prices, specific needs and requirements of the customers and status of the ongoing negotiation with the customers." In *Electro Cad Australia Pty Ltd & @ Ors v Mejati RCS Sdn Bhd & Ors* [1998] 3 CLJ Supp 196 the same judge defined trade secrets as "information which any reasonable employee would recognize as secret to his employer's business and that an action for breach of confidence will lie where there is a breach of an obligation of confidence. The wide scope and the absence of statutory definition of trade secrets need to be addressed by the legislature.

In addition, Malaysia needs to have a statutory definition of trade secrets for the purpose of proving ownership and economic value of the trade secrets. These elements are important for both civil and criminal action. However for criminal case, one question may arise - does the element of knowledge of the employee that the information is a secret is sufficient to warrant criminal charges and penalty? Should the owner of the trade secrets prove the following tests to determine the secrecy or confidentiality of the information in criminal case namely:

1. The extent to which the information is known outside the owners business;
2. The extent to which it is known by employees and others involved in his business
3. The extent of measures taken by him to guard the secrecy of the information;
4. The value of information to him and his competitors
5. The amount of effort or money expended by him in developing the information
6. The ease or difficulty with which the information could be properly acquired or duplicated by others (i.e. by their independent endeavors.

In relation to intangible nature of trade secrets, Malaysia does not recognize intangible assets as property. This may pose difficulty in making stealing of trade secrets as theft under the Penal Code. This is because section 378 on theft is only applicable to stealing of tangible or corporeal property or assets. The British case of *Oxford v Moss* (1979) 68 Cr App Rep 183 illustrated the position in Malaysia where in that case the court held that the confidential information contained in a paper which a student has stolen did not amount to intangible property (which is recognized as property under the Theft Act 1968) and since there was no intention to permanently deprive the owner of the so called intangible property, the magistrate dismissed the charges on the basis that there had been no appropriation of "property" in terms of the UK Theft Act 1968**.**

Further**,** there is no specific definition on theft of trade secrets and economic espionage in Malaysia. The Penal Code and SOSMA merely described the term 'espionage' as the offence against the state which includes terrorism. But economic espionage was not mentioned and therefore cannot be said to be an offence against the state. In the absence of a clear definition and scope of offence against the state, it would be unlikely for economic espionage to be governed by any security laws in Malaysia unless the Acts are amended recognizing it as such.

5.1. The Relevant Laws

a. National Security Laws: SOSMA 2012, POTA 2015 and NSCA 2016

SOSMA was enacted to replace the Internal Security Act. However due to the threat of terrorism, SOSMA was insufficient to address the issue of terrorism. As a result POTA was enacted in 2015 especially to counter the influence of the Islamic State (IS). Despite the existence of SOSMA and POTA, the government enacted the NSCA in 2016 to further address the issue of terrorism and other related act. However all these security acts do not define or describe economic espionage as one of the crimes against the state. Therefore the national laws exclude economic espionage as national security issue. Nevertheless, the lack of specific definition may make it wide enough to cover economic espionage as crime against the state due to several cyber-attacks that happened recently as acknowledged by cybersecurity as seen in the earlier part of this paper.

b. Penal Code.

Stealing or misappropriating trade secret or acquiring without consent of the owner are criminalized as theft in the US, Japan and South Korea. All three countries regarded trade secrets not just as tangible or intangible form but the trade secrets itselfasproperty. As a result, stealing, misappropriating and acquiring without consent are punishable crime. In Malaysia, theft is regulated under the Penal Code. Section 378 defines theft as "whoever, intending to take dishonestly any movable property out of the possession of any person without that person's consent, moves that property in order to such taking, is said to commit theft." However the provision only refers to 'movable property' and section 22 of Penal Code defines it as to include "corporeal property of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth." Apparent from this provision, together with the lack of statutory definition of trade secrets, theft of trade secrets and economic espionage fall outside the terms of crime against the state and theft under the Penal Code. To make it relevant, amendment to include intangible property as property and by or for the benefit of foreign government would extend the crime of theft applicable to theft of trade secrets and economic espionage. Nevertheless it is argued that it is not the tangibility or intangibility of the trade secrets that matters but the trade secrets and the value attached to it that matters most. Once lost, the value is gone forever.

The Penal Code also lack the element of criminal liability as stated in the TTPA particularly provision 18.78 (3) namely:

(a) the acts are for the purposes of commercial advantage or financial gain;
(b) the acts are related to a product or service in national or international commerce;
(c) the acts are intended to injure the owner of such trade secret;
(d) the acts are directed by or for the benefit of or in association with a foreign economic entity; or
(e) the acts are detrimental to a Party's economic interests, international relations, or national defence or national security.

Without these criminal elements inserted into the Penal Code, prosecution may be not feasible.

c. Cyber laws: CMA 1998 and CCA 1997

With the advance of IT and digital devices, stealing or misappropriation of trade secrets and cyber espionage is made easy to both internal and external threat factors namely the employee and outsiders which includes competitors, hackers and organized crime and foreign agent (Wiseman & Appenteng, 2015)In fact the value of trade secrets attracted organized crime to sell the trade secrets or confidential information they obtained through covert practice in the dark market. Study has shown that some organized crime used counterfeit source code to new computer for the purpose of stealing information from the computer(NUS Study, 2017)The study found that there is a prevalence of malicious code (malware) found in pirated software and in PCs purchased through distribution channels which link detected malware and criminal organization. According to the study "malware in pirated software can be a lucrative vector for cyberattacks". Thus as technology

becomes more advanced, access and stealing of trade secrets becomes easier and quicker to the detriment of the corporation's (Brian, 2016).

In Malaysia the cyber laws namely the Communication and Multimedia Act 1998 (CMA) and the Computer Crimes Act 1997 (CCA) were enacted to govern the cyber environment in Malaysia. The authorities entrusted to monitor this development are the Communication and Multimedia Commission under the Ministry of Information and the Cybersecurity within the Ministry of Science and Technology with the support from the Royal Malaysian Police. The CMA 1998 establishes a regulatory framework in support of national policy objectives for the communications industry. Services regulated under the Act include traditional broadcasting and telecommunications, as well as computer networks, and content carried over those systems. The CMA seeks to provide a common set of regulatory provisions based on generic definitions of communications services. It is therefore suited to a converged environment where the same digital information can be transported over any electronic network. The Act contains a penal provision under section 211 on prohibition offensive contents and Chapter 2 of Part X on additional offences and Penalties. This includes the offences relating to use of apparatus or device without authority, fraudulent and improper use of network facilities and network service. Interception and disclosure of communications, and unlawful use, possession or supply of non-standard equipment or device are also offence under the Act.

Section 231 of the prohibits the usage of any apparatus or device with intention to obtain information regarding contents without approval and the punishment is a fine not exceeding fifty thousand ringgit or an imprisonment not more than 2 years or both. This provision may be used against both employee or external party however the punishment is too low when it involves misappropriating trade secrets which is the life blood of a company. Other relevant provisions are section 234 that prohibits interception and disclosure of communication. The provision inter alia states that a person commits an offence if without authority intercepts or attempt to intercept or procure any communication, discloses and attempt to disclose to other person the contents of the information which was obtained through such act or use or attempts to use the content.

The Act also punishes those authorized person who intentionally discloses or attempts to disclose to other person the contents of any communications, intercepted by authorized means *(a)* knowing or having reason to believe that the information was obtained through the interception of such communications in connection with a criminal investigation; *(b)* having obtained or received the information in connection with a criminal investigation; or *(c)* to improperly obstruct, impede, or interfere with a duly authorized criminal investigation. For both offences the punishment shall, on conviction, be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding one year or both. Clause 4 of section 234 nevertheless provides the safeguard allowing an officer, employee or agent of any network facilities provider, network service provider, applications service provider or content applications service provider whose facilities or services are used in communications, to intercept, disclose, or use those communications in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his facilities or services or to the protection of the rights or property of the provider of the facilities or services. Nevertheless the provider is prohibited from utilizing the facilities or services for observing or random monitoring unless it is for mechanical or service quality control

checks.

The CMA makes it an offence for a person who by any willful, dishonest or negligent actor omission, extends, tampers with, adjusts, alters, removes, destroys or damages any network facilities or any part of them commits an offence and shall, on conviction, be liable to a fine not exceeding three hundred thousand ringgit or to imprisonment for a term not exceeding three years or to both. This provision could be used against employee as well as third person who committed such act when misappropriating trade secrets information. Apart from the above provision, the CMA also criminalized fraud and related activities in connection with access devices. Section 236 provides: "(1) A person who knowingly or with intention to defraud—

(a) produces, assembles, uses, imports, sells, supplies or lets for hire any counterfeit access devices;
(b) possesses any counterfeit access device or unauthorized access device;
(c) produces, assembles, uses, imports, sells, supplies or lets for hire, or has control or custody of, or possesses any device-making equipment; or
(d) produces, assembles, uses, imports, sells, supplies or lets for hire, or has control or custody of, or possesses—

> (i) any equipment, device or apparatus that has been modified or altered to obtain unauthorized use of any network service, applications service or content applications service; or
> (ii) hardware or software used for altering or modifying any equipment, device or apparatus to obtain unauthorized access to any network service, applications services or content applications service, commits an offence."

The Act create offences for a person who without the authorization of the issuer of an access device, solicits a person for the purpose of *(a)* offering an access device; or selling information regarding, or an application to obtain, an access device. For both offences, upon conviction such person may be liable to a fine not exceeding five hundred thousand ringgit or to imprisonment for a term not exceeding five years or to both.

Thus even though the CMA does not provide the definition of cyber espionage, certain activities as seen above may amount to cyber espionage. Nevertheless to make it effective the Act should have provision that spell out clearly the activities that lead to cyber espionage and online theft of trade secrets.

The CCA makes misuse of computers as criminal offence. The offences include unauthorized access to computer material, unauthorized access with intent to commit other offenses and unauthorized modification of computer contents. Offences for unauthorized access to computer materials includes knowingly and intentionally (a) causing a computer to perform any function with intent to secure access to any program or data held in any computer and securing unauthorized access. Upon conviction, the guilty person may be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding five years or to both. For the second offences of unauthorized access with intent to commit or facilitate commission of further offence, a person shall be guilty if he with intent (a) commits an offence involving fraud or dishonesty or which causes injury or (b) to facilitate the commission of such an offence whether by himself or by any

other person at the same time when the unauthorized access is secured or any future occasion. If found guilty, the person can be liable to a fine not exceeding one hundred and fifty thousand ringgit or to imprisonment for a term not exceeding ten years or to both.

For unauthorized modification of the contents of any computer, section 5 states: (1) A person shall be guilty of an offence if he does any act which he knows will cause unauthorized modification of the contents of any computer. Regardless whether the act in question is not directed at— (a) any particular program or data; (b) a program or data of any kind; or (c) a program or data held in any particular computer. The provision applies to permanent or merely temporary modification. The punishment under this offence is a fine not exceeding one hundred thousand ringgit or imprisonment for a term not exceeding seven years or both; or be liable to a fine not exceeding one hundred and fifty thousand ringgit or to imprisonment for a term not exceeding ten years or to both, if the act is done with the intention of causing injury as defined in the Penal Code.

Lastly on wrongful communication, section 6 (1) states: A person shall be guilty of an offence if he communicates directly or indirectly a number, code, password or other means of access to a computer to any person other than a person to whom he is duly authorized to communicate and a person guilty of an offence under this section shall on conviction be liable to a fine not exceeding twenty five thousand ringgit or to imprisonment for a term not exceeding three years or to both.

Apart from this the CCA also punishes Abetments and attempts punishable as offences under section 7. The CCA presume that a person who has in his custody or control any program, data or other information which is held in any computer or retrieved from any computer which he is not authorized to have in his custody or control shall be deemed to have obtained unauthorized access to such program, data or information unless the contrary is proved. This presumption under section 8 places a burden of proof on the owner of the computer to rebut the presumption. It provides an important safeguard and protection to the owner of trade secrets.

The CMA and CCA also provide extra territorial jurisdiction for offences committed by person outside Malaysia as if that offense was committed in Malaysia if the computer program or data was in Malaysia or capable of being connected, sent or used by or with a computer in Malaysia.In brief even though cyber laws are in existence in Malaysia the law needs to be upgraded to address clearly the crime of theft of trade secrets and cyber espionage online.

6. CONCLUSION

Malaysian businesses are potential target of theft of trade secrets and economic espionage. As a member of the TTPA, Malaysia is obliged to extend the protection of trade secret through penal sanction as required under Article 18.78 of the agreement. As discussed, Malaysia has several options to criminalize trade secrets theft and economic espionage namely through the national security laws, Penal Code and Cyber laws. Nevertheless as seen above, all the laws have loop hole to accommodate the TPPA requirement. Lacks of clear definition on trade secrets, economic espionage, the scope of criminal act and elements and other issues as highlighted may hinder the process of protecting trade secrets through criminal prosecution as envisage by the TPPA. Such

lacking could be due to the archaic laws particularly the Penal Code, CMA and the CCA because the threat of theft of trade secrets and economic espionage are new threats and that most of the laws were enacted prior to IT development or during at the initial stage of IT developments. As such amendments are needed to ensure compliance with the TTPA requirements and Malaysia can rely on the US and Japanese law for guidance on this matter. However it may take sometimes before the law is revised or amended. Thus it is submitted that law alone is insufficient to address and to combat the threat of theft of trade secrets and economic espionage, therefore in the meantime, the business enterprises must take precautionary measure, both administrative and technical, to ensure protection of their trade secrets from theft and economic espionage, and to collaborate with the relevant authorities.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the contribution of the Ministry of Higher Education for their research funding under the Fundamental Research Grant Scheme.

REFERENCES

Brian, T. Y. (2016). Protection of trade secrets: Overview of current law and legislation. *Congregational Research Servi*ce. Retrieved from https://fas.org/sgp/crs/secrecy/R43714.pdf

Centre for Responsible Enterprise and Trade (CREATE). (2014). *Economic impact of trade secret theft: a framework for companies to safeguard trade secrets and mitigate potential threats*. Retrieved from https://create.org/wp-content/uploads/2014/07/CREATe.org-PwC-Trade-Secret-Theft-FINAL-Feb-2014_01.pdf

Comment. (1971). Theft of Trade Secrets: The Need for a Statutory Solution. *U.Pa.L.Rev*, *120*, 378, 380-81. Cited in Piper, J. (2008) I Have a Secret? Applying the Uniform Trade Secrets Act to Confidential Information That Does Not Rise to the Level of Trade Secret Status, 12 *Intellectual Property L. Rev. 359*. Available at: http://scholarship.law.marquette.edu/iplr/vol12/iss2/4

Cook, T. (2014). The proposal for a directive on the protection of trade secrets in EU legislation. *Journal of Intellectual Property Rights,* 19, 54-58.

Department of Defense. (2011). *Strategy for operating in cyberspace*. Retrieved from http://www.defense.gov/news/d20110714cyber.pdf

European Commission. (2013).*Study on trade secrets and confidential business information in the internal market.* Retrieved fromhttps://www.google.com/search?q=EC+Study+on+trade+secret+2013&rlz=1C1EJFA_enMY780MY781&oq=EC+Study+on+trade+secret+2013&aqs=chrome..69i57.8581j0j7&sourceid=chrome&ie=UTF-8

Japan Patent Office. (2008). Outline of the Japanese unfair competition prevention law. *Asia-Pacific Industrial Property Center.* Retrieved from https:www.jpo.go.jp>index.

Nakajima, M. (2017). Japan: Summary of Japanese unfair competition prevention law 2015 as revised aiming at strengthening protection of trade secret. *Mondaq.* Retrieved from mondaq.com/x/572206/Trade+Secrets/Summary+Of+Japanese+Unfair+Competition+Prevention+Law+2015+As+Revised+Aiming+At+Strengthening+Protection+Of+Trade+Secret

NUS Study. (2017). *Cybersecurity risks from non-genuine software the link between pirated software sources and cybercrime attacks in Asia Pacific*. Retrieved from https://news.microsoft.com/uploads/2017/10/Whitepaper-Cybersecurity-Risks-from-Non-Genuine-Software.pdf

Organisation for Economic Cooperation and Development (OECD). (2015). *Approaches to the protection of trade secrets.* Retrieved from https://www.oecd.org/sti/ieconomy/Chapter3-KBC2-IP.pd

Paik, K. & Lim, K. B. (2010). Trade secrets protection in South Korea. *World Intellectual Property Review Digest*. HTTP://WWW.KIMCHANG.COM/USERFILES/FILES/TRADESECRETPROTECTIONINSOUTHKOREAWORLDIPREVIEW.PDF.

Rollins, W. (2015). US – China cyber agreement. *CRS Insight.* Retrieved from https://www.everycrsreport.com/files/20151016_IN10376_6aaf9eb926ec5993c0b62d1a2a445f6d6bb597d1.pdf

Saunders, K. M., & Evans, M. (2017). A Review of State Criminal Trade Secret Theft Statutes *UCLA J.L. & Tech*., Fall. 1.

Searle, N. (2012). The Criminalization of the Theft of Trade Secrets: An Analysis of the Economic Espionage Act*,* 2 *IP THEORY*.

The Sundaily. (2017) *Wannacry ransonware attack in Malaysia confirmed.* Retrieved at https://www.thesundaily.my/archive/wannacry-ransomware-attack-malaysia-confirmed-YTARCH446003

US Chamber of Commerce (2013). The Case for Enhanced Protection of Trade Secrets in the Trans-Pacific Partnership Agreement*. Covington& Burling LL.P*

Wiseman, D. W., & Appenteng, K. A. (2015) , The Defend Trade Secret Act of 2015: Proposed Legislation Would Open the Federal Courthouse Door for Trade Secret Misappropriation Claims, LITTLER (Aug. 12, 2015), https://www.littler.com/publicationpress/publication/defend-trade-secrets-act-2015-proposed-legislation-would-open-federal.