International Journal of Business and Society, Vol. 21 S1, 2020, 205-218

PROTECTING TRADE SECRET FROM THEFT AND CORPORATE ESPIONAGE: SOME LEGAL AND ADMINISTRATIVE MEASURES

Juriah Abd Jalil[♣]
International Islamic University Malaysia

Halyani Hassan
International Islamic University Malaysia

ABSTRACT

Trade secret is a gold nugget that determines the success and survival of a business entity. It provides a business entity with a competitive value over its rival. However protecting a trade secret is not an easy task especially from current and former employee as well as from competitors. The task is made difficult with the availability of technological devises that can be used to steal the information from inside and outside of the business organization. This paper highlights the importance of protecting trade secrets from theft of trade secret and corporate espionage by business entity and to recommend the best practice on how to protect it using legal and administrative measures. This study is significant to educate business entity especially SME on the importance of protecting trade secrets in this digital age. In this regards, protecting trade secrets is equivalent to protecting the business and the economy of the country.

Keywords: Trade secrets; Misappropriation of business information; Confidential information; Corporate espionage.

Received: 11 February 2019
Accepted: 20 August 2019

1. INTRODUCTION

Business entities all over the world, whether big, medium and small scales are facing challenges from theft and misappropriation of confidential information and trade secrets from insider, that is the employee as well as from external factors i.e. the competitor, the ex- employee and third parties. Being the most important assets, trade secrets safeguard the economic value of the business's product, innovation and development (Lippoldt & Schultz 2014). It places a business entity to a secured and better position than its competitor and it guarantees the success of the business in a long run as illustrated by Coke Cola and Kentucky Fried Chicken (KFC) companies. However, both companies have faced the problem of having their trade secrets stolen by employees or the secret recipe revealed by people who knew the secret (The Telegraph News, 2016). In the case of Coke Cola (CNN Money, 2007) the employees who stole and sold the secrets to a competitor were

♣ Corresponding author. Department of Legal Practice, Ahmad Ibrahim Kulliyyah of Laws, International Islamic University Malaysia, Kuala Lumpur, Malaysia, Tel: (603) 6196 4366, E-mail: juriah@iium.edu.my.

caught, tried and jailed for stealing the information. The company only knew about the incident when the rival company, PepsiCo made a report on receiving a mysterious letter offering trade secrets to a highest bidder. The matter was investigated by the Federal Bureau Investigation (FBI) resulting in the arrest of a former assistant to the vice president of Coke trade mark division and her co-conspirator. In the case of KFC, the secrets recipe was revealed by the nephew of Colonel Sanders who found the hand written recipe during an interview with a journalist. The alleged trade secret was revealed and made viral, but the authenticity of recipe was denied by the company (The Telegraph News, 2016). The experience faced by both companies has taught them to take comprehensive measure to protect their trade secrets by physical and administrative measures. In this regard, the KFC companies kept the handwritten original recipe of Colonel Sanders locked in a digital safe that is encased in two feet concrete, monitored 24 hours by video and motion detection surveillance system at the KFC Corporate headquarters and that the secret recipe is known only by two KFC executives. While the Coke Cola recipe was safely locked in an underground safe inside a Sun Trust Bank. The measures taken equating protecting trade secret with protecting their business and generous amount of money has been spent to protect their trade secrets.

However locks and keys plays minimal role in protecting trade secret that is kept or stored in digital format. This is acknowledged by the Centre for Responsible Enterprise and Trade (Create.org) in their report that states "The rising threat of cybersecurity breaches for companies and other organizations puts the confidential technical and business information that gives companies their competitive edge—commonly known as trade secrets—at greater risk from theft and loss. (Create.org, 2016). On this aspect companies may find the threat comes in the form of cyber espionage and cyber misappropriation. With this scenario as a background, this paper aims to highlight the importance of protecting trade secrets from being misuse, abuse and appropriated by the employee, competitors and third parties (where the business has dealing with) and what are the means to protect them according to the best practices within the reasonable means of a company.

2. OVERVIEW OF THE ISSUES

Misappropriation or theft of trade secrets and corporate espionage threaten innovation, growth development and investment of business entities and national economy globally.(OECD, 2016) Such acts have tendency to kill a business entity and stop it from venturing further into business unless some measure is taken to minimize the risks. In the recent case in the US, an American Superconductor Inc. (AMSC) was nearly put out of business when its employee at another subsidiary was bribed to steal the company's source code for its wind turbine control software by their partner company Sinovel Wind Group Co Ltd, a company based in China. The theft has resulted in the fall of the value of the company's assets by more than USD 1 million, lost more than USD 1 billion in shareholder equity and almost 700 jobs too. According to the CEO, the Chinese strategy was to kill the company. The case was investigated by FBI with the assistance of the Justice Department's office of International Affairs and the US Cybercrime Laboratory of the Criminal Division's Computer crime and Intellectual Property Section (CCIPS) (Justice News, 2018). The Chinese company was charged and convicted with conspiracy to commit trade secret theft, theft of trade secrets and wire fraud. The employee and two more associates were also convicted. The Sinovel case illustrated the impact of theft of trade secrets on the company's well-being, employees' job and how important it is to have a good law and internal risk management to protect trade secrets from employee and foreign partners. This case confirmed the finding of the

US Chamber of Commerce (US Chamber of Commerce, 2013) and OECD (OECD, 2016) that trade secret theft is one of the main factors that cause billions of dollars in annual losses to business entity and national economy (Pricewaterhouse Cooper, 2014).Further in the case of *General Motors v Ignacio Lopez de Arriortua* 948 F Supp, 677-78 (E.D. Mich. 1996) and the case of *Gould Inc v Mitsui Mining & Smelting Co*. 750 F. Supp 838 (N.D Ohio 1990) the US federal district court held that the thief who steals a trade secret victimizes the owner every time the trade secret is used because the owner suffers a new loss with each use of the secrets. This decision is in line with the novel nature of trade secrets that derive independent economic value, actual or potential from not being generally known. Accordingly the use of misappropriated trade secrets has real and huge implication to the owner. This is because the stolen secrets can be used to penetrate new markets, reduce a competitor's costs and increase competitors market share (Joshi, 2010). In short every use of the misappropriated trade secrets continues to harm the owner of the trade secrets. Before we discuss on who are the threat actors we need to know what trade secret is and what the economic importance of trade secrets is.

3. TRADE SECRET DEFINITION AND ECONOMIC IMPORTANCE

Article 39.2 of the Trade Related Aspect of Intellectual Property Agreement or TRIPS defines trade secrets as information that is secrets, has commercial value because of its secret and has been subject to reasonable steps to keep it secrets. The trade secrets can be divided into three categories namely technical information which include industrial processes, blue prints and formulas, confidential business information such as customers' lists, financial information and business plan and lastly know how that includes information about method and steps or process for achieving efficient result (WIPO, 2018). Each company, depending on the nature of business, may have different type of trade secrets that put them into competitive advantage over their competitors.

There is no statutory definition of trade secret in Malaysia. The Malaysian court has this far relied on the definition of English cases and apply common law definition in dealing with cases involving trade secrets and confidential information dispute. Justice Kamallanathan Ratnam J in the case of *Schmidt Scientific Sdn Bhd v Ong Han Suan* [1997] 5 MLJ 632 observed the broad terms of trade secrets when he said " 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 question sent to the customers, costs prices, specific needs and requirements of the customers and status of the ongoing negotiation with the customers". However in the case of *Electro Cad Australia Pty Ltd & Ors v Mejati RCS Sdn Bhd & Ors* [1998] 3 CLJ Supp 196 the same judge looked at the definition from the employee perspective namely " information which any reasonable employee would recognized 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.

In relation to economic importance of trade secrets, the EC study conducted a survey on 537 business in Europe and 75% of them ranked trade secrets as "strategically important to their company's growth, competitiveness and innovative performance." The study also found that there is a consensus among economists that trade secrets play an important role in protecting the returns to innovation and that trade secrets protection is an integral and important part of the overall system of protection to protect intangible assets (EC Study, 2013). In 2017 Baker Mckenzie also conduct a study on 400 executives and make the following three findings namely first trade secret is

essential to brand value and corporate strategy. Second, trade secrets are more importance than patent and trade mark, thirdly that about 32% of these executives place risk of theft of trade secrets and cyberattacks among the top five issues thus acknowledging the existence of threats. Therefore trade secret is a growing commercial power that gives a business entity a competitive edge thus must be protected. In short protecting trade secret is protecting the business. These threats are becoming a global phenomenon that challenges the existing laws and the existence of corporate entities. But from whom should trade secrets be protected and who are the threat actors.

4. THE THREAT AND THREAT ACTORS

The threats of theft of trade secrets come from employee, ex-employee, competitors and foreign country. Survey by Baker Mackenzie found that 20% of the companies admit that they have had their trade secret stolen, while 33% reported that they have suffered trade secret theft. However there are 11% that do not know whether they have been the victims of such theft or misappropriation. The survey also indicated that the most feared theft is by former employees.

As seen in the Sinovel case earlier, the culprit is usually the existing employee or malicious insider. But this could include former employee, corporate competitors and in some cases, foreign government.These threat actors posed real risk to business entities and have potential to destroy the progressive development of the company. Once the trade secrets are divulged it will take a long time for the company to recover or restore their position in the industry (IP Commission, 2014) .So who are the threat actors then?

a. Insider threat

In brief the insider includes current employee, former employee, business partner and contractor. The information age makes it possible for all level of employees including business partner to gain access to volumes of data and pose a significant security risk. The case of Edward Snowden provides a good example of insider threat. According to Software Engineering Institute (SEI) at Carniege Melon University, insiders can pose a considerable threat to the organization. This is because the insiders know and aware of the organization's policies, procedures and technology and they also know the vulnerabilities of the organization. They can bypass the security measures using their knowledge and access to company proprietary systems. In this regards, insiders have a significant advantage over outside or external attackers. Such threat from insiders is therefore real and could be substantial. Thus to prevent harm to the company or organization assets, focus should not only be made to external-facing security mechanisms, such as firewalls, intrusion detection systems, and electronic building access systems, but also to include insiders as potential threats. In 2016, a survey conducted by the U.S State of Cybercrime found that 27% of electronic crimes were suspected or known to be caused by insiders and the insider attacks caused severe damage than caused by outsider attacks (U.S. State of Cybercrime, 2016). According to a Statistical Analysis of Trade Secret Litigation in the US Federal Courts, 85% of the trade secret lawsuits in the state and federal courts of the US found that the alleged misappropriator was either an employee or a business partner (Almeling, 2010). In 2016, survey conducted by IBM estimates that employees and other malicious or careless insiders account for 60% of cyber-attacks from unauthorized access, viruses or other malicious code, 'phishing' attempts and other means (IBM X-Force Research, 2016).

There are different types of insiders namely malicious, non-malicious or insider threats from individuals operating for different kinds of motives. According to CISC Insider Report Proceeding, "insider threats from individuals operating for monetary motives or non-malicious security slips can be as great or greater threats than those from an ideologically driven actor such as Snowden." (Insider Threat Workshop, 2013) As seen in the Sinovel case above, the insider threat i.e. an employee in a subsidiary company was driven by monetary motivation that posed a greater threat than those ideologically driven actor like Snowden who acted in violation of the organization policy and discloses restricted information to the public or a competitor (Woolley et al, 2014). In the same case foreign people has enticed the insider to steal the source code for them. In another case, the US court found two individuals guilty of conspiracy to sell trade secrets to the Chinese government (U.S Department of Justice, 2016).

An insider threat is anonymous and difficult to identify but a clue could be derived from the definition of malicious insider threat. Such threat refers to "a current or former employee, contractor or other business partner who has or had authorized access to an organization's network, system or data and intentionally misused that access in a manner that negatively affected the confidentiality, integrity or availability of the organization's information or information systems" (Cert. Insider Threat, 2017). The concerns however is growing and many company fears that their most valuable asset could leave the business premise on a thumb drive or be disclosed through an employee's use of social media by their employee.

b. External or outsider Threat actor

This category includes competitor, hactivist, foreign government and organized crime. The act of these threat actors could also be associated with data breach and data leakage through computer system, intrusion of detection system and electronic building access system. According to Almeling there are increased threats from foreign individuals, companies and government due to three factors namely internationalization of business, access to technology that allows hackers to access trade secrets from anywhere in the world and that some countries viewed stealing of trade secrets as an aid to development (Almeling, 2012). The rise of this international trade secret misappropriation could also be attributed to the difficulty in enforcement and lack of jurisdiction. Two main international treaties that protect trade secrets are Article 1711 of the North American Free Trade Agreement and Article 39 of the Trade-Related Aspects of Intellectual Property Rights. However not all member countries adhere to the rules and most have problem with enforcement and cultural norms.

In this competitive environment, countries require access to reliable intelligence that reveals the strengths and weakness of their competitors (Buchan, 2016) In order to this, countries resort to espionage act i.e. a method of gathering intelligence or 'the consciously deceitful collection of information ordered by a government or organization hostile to or suspicious of those the information concerns, accomplished by humans unauthorized by the target to do the colleting' (Damarest, 1996). In brief it refers to the practice where a state dispatches an agent or human intelligence into the physical territory of another state in order to access and obtain confidential information (Buchan, 2016). The existence of cyberspace has garner or harnessed cyber espionage. The US Presidential Policy Directive, 2012 defined cyber espionage as 'operations and related programs or activities conducted …in or through cyberspace, for the primary purpose of collecting intelligence…from, computers, information or communication systems or networks with the intent

to remain undetected' (U.S. Cyber Operation Policy, 2012). Two reasons why cyber espionage is an attractive methods is because first, there are a large amount of information being stored in cyberspace and second, that cyberspace affords a considerable degree of anonymity to perpetrators of espionage and third, cyberspace is a relatively risk free enterprise (Buchan, 2016).On this matter Edward Snowden for example has revealed through Wikileaks documents that US National Security Agency (NSA) has engaged in a global surveillance program that has collected confidential information stored in or transmitted through cyberspace. In February 2013, The Mandiant Report indicated that China has formed a Unit to organize and instigate massive cyber espionage campaign against other states and non-state actors seeking to exploit vulnerable computer system in order to access sensitive and confidential information with the aim to bolster China's position in the international political and economic order (Mandiant Report, 2013). Therefore, the threats from both internal and external factors are real and companies have become victims of theft and corporate espionage. How then could a company minimize these risks?

5. HOW TO PROTECT TRADE SECRETS?

Protecting trade secret is not easy and never simple. The challenge is much more in this digital age. In fact trade secret stored in digital format is much easier to access and also easier to misappropriate. This allows for international misappropriation of local trade secrets to take place. As regard the methods of protection, John Powell of AMSC said that no matter how secure a company thinks its computers and networks are from external technical threats, the internal threat from employee theft is always present and in many senses is more difficult to deal with. Similar concerns was raised by Michael Chertoff, the US Sectary of Homeland Security that focusing only on attacks from outside a company is like locking a door but leaving a window open. Even storing secret information in the cloud is not safe (Favro, 2016) because the threat of hacking and misappropriation may actually come from cloud service provider. Since it is not easy to protect trade secrets, the company should at least try to minimize the threat and this requires coordination from the government, industry and the company itself. Such protection can be divided into legal and administrative measures and the discussion on legal measure will look at the Malaysian legal position while the administrative measure will look at how some organization protect their trade secrets and confidential information.

a. Legal Measures through law of contract, breach of confidence and cyber laws

The law provides several options for the company to minimize the risk of trade secrets theft and corporate espionage from the employee and former employee. The first option is through contract of employment for employee and Non-Disclosure Agreement (NDA)when dealing with third parties. In the case of *Bodibasixs Manufacturing Sdn Bhd v Entogenex Industries Sdn Bhd* [2018] 9 MLJ 417, the High court recognized a mutual non-disclosure agreement as one of the ways to protect intellectual property right where it preserves the confidentiality of proprietary information and materials that to be transferred between the parties. In relation to the contract of employment, the important clause should be the confidentiality clause that imposed legal obligation on the employee who has signed it not to breach any confidential information of the company to anyone during the employment. In *Motordata Research Consortium Sdn Bhd v Ahmad Shahril Bin Abdullah & Ors*[2017] MLJU 1187, the court explained that confidentiality agreement laid out the obligation of the employee to keep confidential of the e-Vas Information that is belong to the employer, the plaintiff in this case.

The confidentiality agreement may also extend to after employment particularly when the ex-employee has used the trade secrets or has revealed to her or his new employer (*Svenson Hair Center Sdn Bhd v Irene Chin Zee Ling*, 2008). On the other hand, NDA will help to maintain the confidentiality of the information or trade secrets even when the third party knew about it. However, in both agreements, the company must clearly define what is the confidential information or trade secrets and at the same time making clear of the job scope, duty and responsibility of the employee and the third parties. In the event of breach of this provision, the employer can take action for breach of contract or the NDA and claim damages for any loss suffered.

However this clause will fail to take effect if the employer is unable to prove and to ensure that they have taken reasonable steps to protect the confidentiality of the trade secrets or confidential information. In the case of *Sigma Clove Industries Sdn Bhd & Ors v Ong Chin Kok & Anor* [2017] MLJU 2032 the court dismissed the plaintiff claim for breach of confidentiality and non- disclosure agreement when the plaintiff failed to plead confidential information or trade secrets in their statement of claim. On this aspect the Federal Court in the case of *Dynacast (Melaka) Sdn Bhd* [2016] 3 MLJ 417, at paragraphs 28 and 29 –

> "*[28] While it is true that the claim of the plaintiffs is only to enforce the contractual clauses related to confidential information entered and agreed upon by the second defendant we do not think it is sufficient in the statement of claim by merely stating that the second defendant had 'misappropriated the private and confidential information of the plaintiffs'.*
> *[29] Surely more particulars should have been given on the alleged misappropriated private and confidential information. The second defendant is entitled to know what are the private and confidential information allegedly to have been misappropriated by him. It would then allow him to contest the claim of privacy and confidentiality of those information. ...*"(emphasis added);

This *was further emphasized in the case of Repco (Malaysia) Sdn. Bhd. v Tan Tho Fatt & Ors* [2012]MLJU 4,186 where the court states *"....The Plaintiff cannot render* a *piece of information* as *trade secret, confidential information or proprietary information by merely naming it* as *such."* In other words the plaintiff or the employer must clearly explained what are the information that is consider as confidential information and must specify what are the information that has been taken by the employee or former employee in order to be successful in enforcing their right under the contract.

Apart from taking action for breach of contract, an employer may also seek for interlocutory injunction to stop the employee from using, selling or distributing the stolen information while the case is on trial. In *Sigma case* as mentioned above, the employer sought from the court an Anton Piller Order but the action was dismissed on the ground that the employer has failed to state what are the specific confidential information or trade secrets that they are looking for in their application.

In the absent of a contract, an employee may still commence a civil suit for misappropriation of the trade secrets and breach of confidence under the common law. This is because employee owes duty of fidelity and good faith to the employer. Employer must prove that the employee knew that

the information is confidential information or a trade secret of the company, and that he has breached it by taking, using, divulging or selling it to others. Again the main requirement is that the employer must prove that the information is a trade secret or confidential information. In order to be successful in this action three elements must first be fulfilled as stated in the case of *Coco v Clark (Engineers) Ltd* [1969] RPC 41. The case was referred to by the Court of Appeal in the case of *Seven* Seas *Industries Sdn Bhd v. Philips Electronic Supplies (M) Sdn Bhd & Anor* [2008] 4 CLJ 217 where *the Court of Appeal held:*

> *... The learned judge in dismissing the appellant's claim referred to Coco v A.N. Clark (Engineers) Ltd.* [1969] RPC 41, *which sets out the three elements to be established in order to succeed in an action for breach of confidence, that is to* say, *firstly, the information sought to be protected has the necessary quality of confidence; secondly, the information* was *communicated in circumstances importing an obligation of confidence; and, thirdly, there must be unauthorised use of that information to the detriment of the party communicating it..."*

In brief, an employer can protect their trade secrets by requesting an employee to sign a confidentiality agreement or enter a non-disclosure agreement. They may also imposed duty to keep confidential information or trade secret in confidence under the common law as discussed above. Both civil actions either in contract or tort law, protect the employer's trade secrets from their employee by imposing duty and obligation not to take, use, disclose, divulge to anyone especially rival or for personal gain. It can also be used against former employee and business associates.

In relation to addressing the issue of online theft of trade secrets and espionage, the Communication and Multimedia Act 1998 (CMA 1988) and the Computer Crimes Act 1997 (CCA) are two legislations that have been enacted to protect Malaysia from cybercrimes and computer misuse. For theft of trade secrets through computer or cyber means, section 234 Clause 1 (a) and (c) of the CMA 1998 may be resorted to. This provision prohibits interception of any communication and content of the communication thus may be use against cyber espionage to stop any transfer of information from one party to another. Clause 1(b) can be used to prohibits disclosure of any trade secrets that have been obtained through intercept of communication. Section 3,4,5 and 9 of the CCA can be invoked to criminalize online theft of trade secrets and cyber espionage. Unauthorized access to computer materials is governed under section 3 while unauthorized modification of content of any computer is dealt with under section 5 of the CCA. In both situations it is crucial for the employer or the business entity to make complain to the local authority for them to conduct investigation before any arrest and charged could be made.

b. Administrative Measures

Apart from relying on the law to protect the company's trade secrets from the employee (existing and former) and competitors, the company should adopt some administrative measures particularly internal measure to protect their trade secret from within. In fact protection of trade secrets should be part of the company corporate governance strategy that include the following firstly, ensuring reasonable steps exist to protect trade secrets and confidential corporate assets. Secondly, to embed trade secret protection into business operation and processes, this can be done through a code of conduct and business practice. Thirdly, to determine effective trade secrets protection plan at all

level of processing and handling including a supplier code of conduct and lastly, it is crucial to identify what are the company's trade secrets. According to the Statistical Analysis of Trade Secrets in the US Federal Court there are 8 categories of protection plan to protect trade secrets namely:

i. Creating agreements, policies, procedures and records to establish document protection;
ii. Establishing physical and electronic security and confidentiality measures;
iii. Assessing risks to identify and prioritize trade secret vulnerabilities;
iv. Establishing due diligence and ongoing third party management procedures;
v. Instituting an information protection team;
vi. Training and capacity building with employees and third party;
vii. Monitoring and measuring corporate efforts; and
viii. Taking corrective actions and continually improving policies and procedures.

Since the main threat comes from the employee and outsider, the World Intellectual Property Organization (WIPO) recommended several additional measures:

a. Educate employees about the importance of trade secrets and communicate to them the policy and the program;
b. Carefully decide and review periodically as to which employees "need to know or use" the information and restrict access to trade secrets on a "need to know" or "need to use" basis;
c. Apply physical and technological restrictions to access trade secrets';
d. Limit and monitor public access to buildings that house trade secrets;
e. Mark "secret" or "confidential" all documents containing trade secrets so as to avoid accidental or inadvertent disclosure;
f. Sign confidentiality agreements with all relevant employees and also with outsiders who in one way or another may get access to company's trade secrets.

Companies especially big giants like APPLE, SAMSUNG Electronics, TOYOTA and PETRONAS, have address this issue of protecting trade secret in their Code of Conduct and Business Ethics or Business Conduct Guideline. The code of conduct or business guideline requires the employee and any third party who has dealing with the company, to follow the safeguards for managing and protecting proprietary information and to only disclose and use sensitive information when deemed necessary or on the 'need to know' basis (SAMSUNG, 2016 & Apple, 2015). PETRONAS for example imposed confidentiality obligation as part of the Code of Conduct by first defining what are the trade secrets and confidential information of the company, followed by a restriction clause affirming that such information is strictly private and confidential and may not be utilized, discussed with, divulge to or disclosed to persons inside or outside the organization excepts by persons authorized to do so. The employees are required to take all necessary precautions with respect to the confidentiality of such confidential information (Petronas, 2013). APPLE for example highlight that information about its product and services including future product offering are APPLE's confidential assets and prohibit disclosure of confidential, operational, financial, trade secret or other business information without verification from the manager that such disclosure is appropriate. It also emphasized that the intellectual property agreement that the employee has signed when joined the company defines the employee duty to protect information. On this aspect, TOYOTA Code of Employee Conduct clearly highlight that

the company does not tolerate illegal or criminal acts in violation of the company policy and rules and mandated on all the employee to comply with the law and should always act with awareness and responsibility. It thus imposed on the employee to manage and protect the company assets, intellectual property, company secrets and personal information.

Apart from protecting the company's trade secrets, employees should respect the assets, intellectual property and confidential information of others. PETRONAS Code of Conduct for example required the employee to comply with all laws regulation, contractual obligation and not to infringe on the protected intellectual property rights of other parties. On this aspect Apple stated that it is not the company's policy to knowingly use the intellectual property of any third party while SAMSUNG highlighted that the company is committed to respect protected information of the company as well as others.

Taking into consideration of the above measures and also the digital environment, a company must establish a measure that covers both physical and virtual threats. In this digital business age, employee uses the most cost effective mechanism such as flash drive, tablet computer and clouds computing to maximize productivity. This includes using personal cloud as tool for advancing business objectives within the corporate environment (Froehlich, 2014). However, such use can implicate a range of troubles for the company particularly in relation to retention and information security to litigation readiness and cyber security (Miller, 2013). In order to strengthen the protection on trade secrets especially against employee, a company should have a policy on Bring Your Own Device or known as BOYD and Bring Your Own Cloud (BYOC) policy. Proper measure must be adopted to ensure compliance and to avoid disastrous outcome to the company especially when an employee leaves the company with proprietary materials and joined the company's competitor. As such it is necessary for the employment contract and the BOYC policy to emphasize on the obligation of the employee to maintain the confidentiality of the company's proprietary information and to return all such materials to the company upon termination of their employment. It is also most crucial to require the employee to destroy all proprietary company information stored in the cloud and to disable the account of the cloud that has been configured to the employee personal computer and to de-configure the personal computer (Favro, 2016). On this aspect it is better for the company to establish a policy on technology use that creates a protocol for the appropriate use and protection of company data by employees. It is also important to explain to the employee of the company's expectation on employees' use of cloud storage and external flash drive and other devices. The employer should retain the right of the employer to review and/or wipe external devices upon leaving the company and prohibit the sending of company email using personal accounts.

Further there should also be a policy governing departing employees. One of the recognized measures is the exit interview. This measure is one of the best ways to remind the employee of the confidentiality agreement that has been executed previously and to explain the on-going obligations. It is crucial for the company to ensure that the employee does not possess any confidential or trade secret information or materials at home and to ensure that all flash drives and personal computers containing company information is returned or wipe out.

From the above administrative measure and the practice adopted by the selected companies, it is advisable for a company to establish proactive and preventive measure to protect its trade secrets. The measures should include as follows:

Table 1: Categories of Proactive and Preventive Measure

Categories	
Policies, Procedure and Record	It is important to communicate to the employee all policy in writing relating to protection of trade secrets and place relevant procedure to implement those policies and keep record of all relevant transactions, events and actions relating to its implementation.
Information Protection Team	This information protection team should identify relevant people across the organization that is responsible for ensuring that policies are in place and procedures to be implemented.
Risk Assessment	The company must conduct risk assessment for the purpose of understanding what is the company key or main trade secrets, where they are, who have access to them, who may be interested in taking them and using them inappropriately.
Management of Third Parties	It is crucial for a company to know who are managing the third parties and how they manage their employees within the company business partners.
Security and confidentiality management	This security and confidentiality management must be conducted at both physical or real world and cyber or networking world.
Training and capacity building	This training and capacity building should focus on making clear with the employee and the third party on their roles in protecting trade secrets.
Monitoring and measurement	This is a most crucial measure to take. A company must monitor the implementation of all the relevant policy relating trade secrets protection and to measure the effectiveness of the policies and that the procedure are strictly followed.
Corrective actions and improvements	A company needs to be quick in addressing a breach or a theft of trade secrets and adopt a sensible and more efficient and effective measure to ensure no more breach of theft in the future.
Take legal action	A company should not hesitate to take a legal action against the employee or competitors especially when all the evidence is clear and good to prove that there is theft, misappropriation and breach of obligation by the employee and competitors.

6. CONCLUSION AND RECOMMENDATION

Protection of trade secrets by a company against the employee and competitors requires an integrated approach. The legal approach alone is not sufficient to protect the trade secrets from theft and corporate espionage by the employee. It must be combined with the administrative measures to ensure comprehensive protection. While the law provides the foundation for the company to protect their trade secrets through contractual obligation, the administrative approach will monitor adherence and compliance of the obligation through the code of conduct and business ethics. Such integrated approaches will create a culture of confidentiality, compliance and respect within the organization and promote healthy competition within the industry. The following five best practices could be used as guideline for a company to protect it trade secrets from theft and corporate espionage.

Firstly, selecting, interviewing and hiring process. This is an important initial process of choosing an appropriate and a suitable employee. It is advisable for the company to undertake a background checks and critically review the prospective and previous employment and experiences. At the hiring process it is crucial to explain the nature of the work, rules and procedure and the company's expectation and demand as well as emphasizing the importance non-disclosure and trade secret protection agreements.

Secondly, once hired, the employee should sign an employment contract. Contractual obligation of confidence must be clearly express in the contract of employment including prohibition to use former employer's trade secrets. Provision on prohibition to disclose, divulge, using of the trade secrets of the new employment should be emphasized and legal action can be taken in case of breach of the obligation.

Thirdly, the company should establish an on-going awareness and education campaign to remind the employee on the trade secrets protection and policy. The BOYD and the BOYC policy should be clearly explain so that employee knows the stand of the company relating to this.

Fourthly monitoring use and limits disclosure. A company must limit all type of disclosure such as physical restrictions, electronic restriction, controlling disclosures, the need to know and use the technique of partition to avoid an employee from having overall knowledge of the trade secrets. Technical measures or tools should be relied on to monitor activity of employee.

Lastly, upon leaving employment, exit interview should be conducted to remind the employee of the contractual and common obligations, to return all the documents and to ensure that the employee not to disclose any information that they have accessed to. It is also crucial to understand why the employee is leaving and where he or she will be going. One of the measures is to check employee's computer and access activities. It important for the employee to return the company hardware and devices including prohibition to use company email and company's data that has been save in the cloud.

All these best practices could be adopted as a company policy and published as a code of conduct and business ethics thus could act as important mechanism to protect trade secrets and confidential information especially from employee and competitors.

ACKNOWLEDGMENT

The authors extend our warmest appreciation to the Ministry of Higher Education Malaysia for sponsoring this research through its Fundamental Research Grant Scheme.

REFERENCES

Almeling, D. S., Darin W. S., Michael S., & Whitney E. M. (2010). A statistical analysis of trade secret litigation in state courts. *Gonz. L. Rev.* 46, 57.

Apple Inc Business Conduct. (2015). *The way we do business worldwide.* Retrieved from http://corporate.findlaw.com/contracts/operations/business-conduct-policy-apple-inc.html

Bodibasixs Manufacturing Sdn Bhd v Entogenex Industries Sdn Bhd [2018] 9 MLJ 417.

Buchan. (2016). The International Legal Regulation of Cyber Espionage. In Osula, A.M and Roigas, H (eds), *International Cyber Norms: Legal, Policy & Industry Perspective*. NATO CCD COE Publications, Tallinn. Estonia.

Centre for Responsible Enterprise and Trade (Create.org.). (2014). E*conomic impact of trade secret theft: A framework for companies to safeguard trade secrets and mitigate potential threats*. Retrieved from https://www.create.org/resource/economic-impact-of-trade-secret-theft/

Centre for Responsible Enterprise and Trade (Create.org.). (2016). *The importance of cybersecurity for trade secret protection.* Retrieved from https://create.org/resource/importance-cybersecurity-trade-secret-protection/

CNN Money. (2007, May 23). *2 sentenced in Coke trade secret case*. Retrieved from https://money.cnn.com/2007/05/23/news/newsmakers/coke/

Coco v Clark (Engineers) Ltd [1969] RPC 41.

Damarest, G. B. (1996). Espionage in international law. *Denver Journal of International Law and Policy, 24,* 326.

Department of Justice. (2018, January 24). *Chinese company sinovel wind group convicted of theft of trade secrets.* Retrieved from https://www.justice.gov/opa/pr/chinese-company-sinovel-wind-group-convicted-theft-trade-secrets

Dynacast (Melaka) Sdn Bhd [2016] 3 MLJ 417

Electro Cad Australia Pty Ltd & Ors v Mejati RCS Sdn Bhd & Ors [1998] 3 CLJ Supp 196

Favro, P. (2016). Addressing Employee Use of Personal Clouds, *22 Rich. J.L. & Tech*. 6

Fireeye. (2013) *Mandiant Report APT1:Exposing One of China's Cyber Espionage Units*. Mandiant Report APT1. Retrieved from http://www.fireeye.com/content/dam/fireeye-www/services/pdf/mandiant-apt-report.pdf.

Froehlich. (2014). The Buck Stops at BYOC, *Information Week*

General Motors v Ignacio Lopez de Arriortua 948 F Supp, 677-78 (E.D. Mich. 1996)

Gould Inc v Mitsui Mining & Smelting Co. 750 F.Supp 838 (N.D Ohio 1990)

IBM X-Force Research. (2016). *Cyber security intelligence index, a survey of the cyber security landscape*. Retrieved from http://www-03.ibm.com/security/data-breach/cyber-security-index.html.

Insider Threat Workshop. (2013, July). *Proceedings Papers and Presentations from the CSIAC Insider Threat Workshop July*. Cyber Security and Information System Information Analysis Centre.

IP Commission Report. (2014.) *Report of the Commission on the Theft of American Intellectual Property*. National Bureau of Asian Research, United States of America.

KFC Corp. v. Marion-Kay Co, Inc, 620 F. Supp. 1160 (S.D. Ind. 1985)

Miller, S. (2013). *New risk on the block: Bring your own cloud*. *GCN*. Retrieved from https://gcn.com/articles/2013/05/23/new-risk-bring-your-own-cloud.aspx

Motordata Research Consortium Sdn Bhd v Ahmad Shahril Bin Abdullah & Ors[2017] MLJU 1187

Organisation for Economic Co-operation and Development(OECD). (2016). *Enquiries into Intellectual Property Economic Impact: Approaches to the Protection of Trade Secrets,* Elsevier.

Petronas. (2013). *Code of conduct and business ethics*. Retrieved from https://gcn.com/articles/2013

Pricewaterhouse Coopers. (2014). *Economic impact of trade secret theft: A framework for companies to safeguard trade secrets and mitigate potential threats*. Center for Responsible Enterprise and Trade. Retrieved from create.org/resource/economic-impact-of-trade-secret-theft/

Repco (M) Sdn Bhd v Tan Tho Fatt & Ors [2012] MLJU 186

Samsung. (2016). *Business conduct guideline*. Retrieved from https://images.samsung.com/is/content/samsung/p5/uk/aboutsamsung/2017/pdf/about-us-sustainability-report-and-policy-business-conduct-guidelines-2016-en.pdf

Schmidt Scientific Sdn Bhd v Ong Han Suan [1997] 5 MLJ 632

Seven Seas Industries Sdn Bhd v. Philips Electronic Supplies (M) Sdn Bhd & Anor [2008] 4 CLJ 217

Sigma Clove Industries Sdn Bhd & Ors v Ong Chin Kok & Anor [2017] MLJU 2032

Software Engineering Institute. (2016). *U.S. state of cybercrime survey*. Retrieved from https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=499782

Svenson Hair Center Sdn Bhd v Irene Chin Zee Ling [2008] 7 MLJ 903

The Telegraph. (2016, August 27). *KFC's recipe: Has one of the biggest trade secrets in the world been revealed?* Retrieved from https://www.telegraph.co.uk/news/2016/08/27/kfcs-recipe-has-one-of-the-biggest-trade-secrets-in-the-world-be/

U.S. Chamber of Commerce, (2013). *The case for the Enhanced protection of Trade Secrets in the Trans-Pacific Partnership Agreement.* Covington & Burlington LL.P, Washington DC.