EFFECTS OF CYBER SUPPLY CHAIN RISK MANAGEMENT

ON SUPPLY CHAIN PERFORMANCE

By

CHEAH KOOI BOEY

RESEARCH REPORT IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF BUSINESS ADMINISTRATION
UNIVERSITI SAINS MALAYSIA
2015

ACKNOWLEDGEMENT

I would like to take this opportunity to acknowledge the contribution of a number of people for their support and efforts in making this research a great success. First and foremost, I would like to express my very special thanks to supervisor Dr. Yudi Fernando for his guidance, feedback and suggestion throughout this research. His guidance and support are the most valued in completing this research project. Besides, I would like to express my deepest gratitude towards the respondents. I am very grateful to them for spending their precious time to complete my questionnaire. I would like to extend my greatest appreciation to my coursemates, friends, superior and colleagues who had patiently helped me in completing this research. Finally, I take this opportunity to express my profound gratitude to my parents for their continuous love and encouragement, for always believing in me, and for never failing to give full support.

ABSTRACT

Manufacturing firms are very focus on their supply chain performance in order to satisfy customer demand and increase business profit. This study examined the relationships between cyber supply chain risk management on supply chain performance as firms are highly rely on information system to execute daily task. Information system security practices as the mediator variable of the study in order test the impacts of cyber supply chain risk management on supply chain performance. A survey was done and the data was collected from 105 manufacturing firm located in Malaysia. The sampling selected was based on stratified sampling method technique. The results obtained from the data analysis indicated significant effect of cyber supply chain risk management in term of governance and operation on supply chain performance. Information system security practices also shown significant effects on supply chain performance. Limitations of this study are addressed and recommendations for future research are suggested.

ABSTRAK

Firma pembuatan sangat memberi tumpuan kepada prestasi rantaian bekalan mereka untuk memenuhi permintaan pelanggan dan meningkatkan keuntungan perniagaan. Kajian ini mengkaji hubungan antara pengurusan risiko rantaian bekalan siber ke atas prestasi rantaian bekalan syarikat adalah sangat bergantung kepada sistem maklumat untuk melaksanakan tugas harian. Amalan sistem maklumat keselamatan sebagai pembolehubah pengantara kajian bagi menguji kesan siber pengurusan risiko rantaian bekalan prestasi rantaian bekalan. Satu kajian telah dilakukan dan data yang dikumpulkan dari firma 105 pembuatan terletak di Malaysia. Persampelan dipilih adalah berdasarkan berstrata teknik kaedah persampelan. Keputusan yang diperolehi daripada analisis data menunjukkan kesan yang ketara siber pengurusan risiko rantaian bekalan dari segi tadbir urus dan kuasa pada prestasi rantaian bekalan. Amalan sistem maklumat keselamatan juga menunjukkan kesan yang besar ke atas prestasi rantaian bekalan. Batasan kajian ini ditangani dan cadangan untuk kajian akan datang yang disyorkan.

TABLE OF CONTENTS **Page**

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CSCRM	Cyber Supply Chaim Risk Management
GO	Governance
ISSP	Information System Security Practices
OP	Operation
SCA	Supply Chain Agility
SCF	Supply Chain Flexibility
SCM	Supply Chaim Management
SCRM	Supply Chaim Risk Management
SI	System Integration

CHAPTER 1

INTRODUCTION

1.1 Introduction

This chapter illustrate the background of cyber supply chain risk management at the first part. Then the problem statements will be discussed. Subsequently, research objectives for this study will be stated followed by the research questions. Next, definition of major key terms are discussed and significant of study are also shown in this chapter. Lastly, a short and simplified overview of others chapters is shown at the last part of the chapter.

1.2 Background of Study

Today's marketplace is characterized by pressure caused by uncertainty, stiff competition, short product life cycle and pressure of industrial innovation. Internet has become the most important infrastructure for firms to complete in the market. In supply chain context, the increasing use of internet helps supply network in sharing information for example the emerging uses of Oracle and SAP have shorten the information transaction time and decrease the incidents of redundancy and inaccuracy (Tang & Musa, 2011). Besides that, Internet also helps firms to manage supply chain activities by offering information related to the product such consumer's demand, the available quantity in the warehouse, the whole manufacturing process of product, and the record of inbound and outbound shipment in the physical facilities and customer sites (Lancioni, Smith, & Oliva, 2000). In recent years, information technology (IT) has turn into a major driver of supply chain management due to the supply chain partners have become more complex and integrated via IT systems and IT

infrastructure integration. It is significantly improved supply chain process integration, which led to better firm performance (Frohlich & Westbrook, 2001). Rongping and Yonggang (2014) defined cyber supply chain as the whole set of main performer using cyber infrastructure such as network, information system, system integrators and software or hardware suppliers (Rongping & Yonggang, 2014).

As a result of globalization and increasing of global competitiveness, supply chains are turning into more complicated, the possibility of not accomplishing the targeted supply chain performance grow in number mainly caused by the risk of supply chain breakdown (Rao & Tobias, 2011). Supply chain becoming more vulnerable to disruptions with large unanticipated consequences of apparently contained events. Such disruptions are due to natural risks (earth-quake, floods and tsunami) or human-made risks (terrorist attacks, accidents and cyber-attacks) (Fahimnia, Tang, Davarzani, & Sarkis, 2015).

Cyber-attacks have become an increasing threat to business and firms. Manufacturing industry is much more concerned with attacks targeted at intellectual property (IP) theft. This is assured as computer security has traditionally concentrated on protecting information. As manufacturing systems have evolved into an Internet of Things (IoT) that rely on software as a service and cloud computing. Hence, attack opportunities now stretch beyond IP theft. As industrial needs always drive research, it is important that industry becomes aware of cyber-attack threats and the full extent of their outcomes (Wells, 2014). Financial Stability and Payment System report (2014) mentioned that global economic faced monetary losses due to cybercrimes were approximated to be USD375 billion yearly. Cyber-attacks are regularly irritated by financial gain as well as driven by a purpose to generate breakdown for political and social intention. Based on the report published by CyberSecurity Malaysia (2015), the

number of security incidents referred to CyberSecurity Malaysia is increasing from year to year as shown in Figure 1.1.

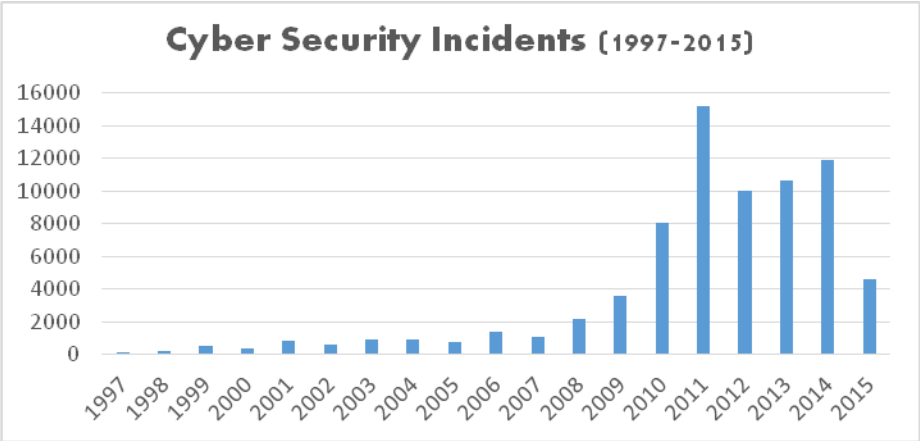

Figure 1.1 Cyber Security Incidents in Malaysia as of May 2015

Source: CyberSecurity Malaysia (2015)

Dell Penang experienced cyber security on 1st of July 2013, an unidentified parties hacked into their website to voice their support for Bangladeshi labors working at Dell manufacturing plant in Penang. The Malaysian Communications and Multimedia Commission (MCMC) chairman Datuk Mohamed Sharil Tarmizi announced that the investigations discovered the hacking had been constrained to registered websites which had the "com.my" prefix (Themalaysianinsider, 2013).

Moreover, the latest Symantec's Internet Security Threat Report as illustrated in Figure 1.2 stated five out of every six large companies were targeted with spear-phishing attacks in 2014. Manufacturing industry is the top industry targeted in spear-phishing attack in 2014.

Figure 1.2 Top 10 Industries Targeted in Spear-Phishing Attacks

Source: Symantec's Internet Security Threat Report (2014)

Cyber security threats inside the supply chain have been a major concern of purchasing, information security and risk as well as compliance teams for recent years because it will creates supply chain issues and disruptions. Supply chain disruptions may cause significant influence on firm's performance, such as after earthquake happened in Taiwan in 1999. Apple missed many orders due to facing shortages of DRAM chips (C. S. Tang, 2006). A disruption is an unanticipated incident in comparison with normal demand and supply coordination (Hendricks & Singhal, 2003). Hence, firms require agility and flexibility in their supply chains to provide uninterrupted service to customer (Braunscheidel & Suresh, 2009). Besides that, in order to compete in the business world and gain competitive advantages, firms have to achieve high performance in supply chain whereby supply chain performance is the ability of the supply chain to provide products and services with good quality, on time and with minimum costs (Green Jr, Whitten, & Inman, 2012).

A basic supply chain is pictured in Figure 1.3, it contains four echelons which are supply, manufacturing, distributions and customers (Beamon, 1999)

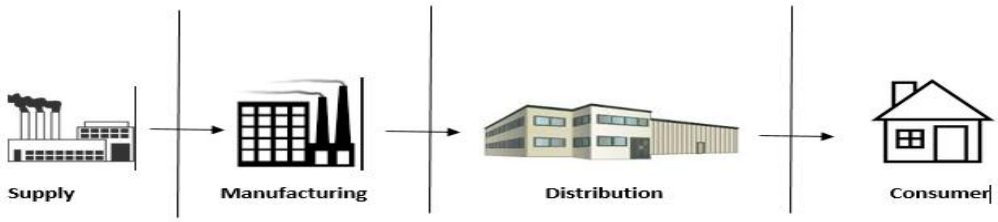

Figure 1.3 Supply Chain

Source: Beamon (1999)

For further explanation, supply chain basically is formed by manufacturers, suppliers, distributors or retailer and customers. Information flows, finances and raw material link participants in either upstream or downstream direction (Costantino, Di Gravio, Shaban, & Tronci, 2015). Whereas supply chain management is described as the integration of main business operations from consumer to original suppliers who supply goods, information and services that provides value added for customers and other stakeholders. Supply chain management can be also defined as a method of managing daily business operation and relationships between suppliers and customers (Lambert & Cooper, 2000). It basically includes demand and supply planning, integration of internal and external logistic across the manufacturers, suppliers, distributors and forwarders to gain greatest competitive advantages among the competitors in the market. Supply chain management is aimed to provide customer uninterrupted material supply and meet customer's satisfaction (Buchmeister, Friscic, & Palcic, 2014). Firms implemented supply chain management in their business to enhance the competence of the supply chain flow and logistic processes (Sentia, Mukhtar, & Shukor, 2013).

Supply chain is wide-open to various kind of risks due to technology innovation, globalization of markets and emergence of information technologies. Hence, handing risks become an key topic in the context of supply chain management (Narasimhan & Talluri, 2009). Risk can be interpreted as uncertain and unreliable resource creating supply chain interruption (Tang & Musa, 2011). Based on Christopher and Peck's (2004) research, supply chain risks can be classified into three categories and can be further sub-divided to five categories, which are internal risk, internal to the supply chain network but external to the organization and risks that external to the network environment. Internal risks consists of process risk and control risk, it manages supply chain disruptions resulted by issue inside the firms such as system failures or IT related matters. While external risks are basically divided to demand risk and supply risk which related to suppliers and customers (Christopher & Peck, 2004). Figure 1.4 describes the linkages among the five categories of risks as mentioned previously.

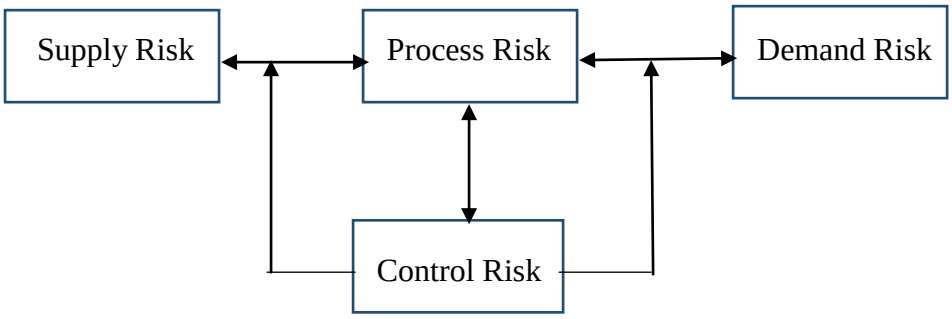

Figure 1.4 Sources of Risk in the Supply Chain

Source: Christopher and Peck (2004)

Firms are highly rely on information system to smoothen and accelerate the information exchange process throughout the supply chain. Thus, apart from the

above mentioned four types of risks, manage information risk and cyber risk are another important topics of supply chain risk management. Information risk is refer to the possibility of damage caused by incomplete, illegal or wrong access to information. It has extensive impact on supply chain, for example, information security or breakdown risks will impact on supply chain operations immediately and intellectual property rights risks is crucial for entire supply chain feasibility in the long run (Faisal, Banwet, & Shankar, 2007). Tang (2006) mentioned about information management is one of the four essential methods which includes the management of supply, demand and product that firms can apply to handle supply chain risks. Figure 1.5 shows the simple diagram of four essential methods for managing supply chain risks. Information risk management is the management of information risks in supply chain via collaboration and coordination between the supply chain partner to guarantee business sustainability (Mohd Nishat, Banwet, & Ravi, 2007).

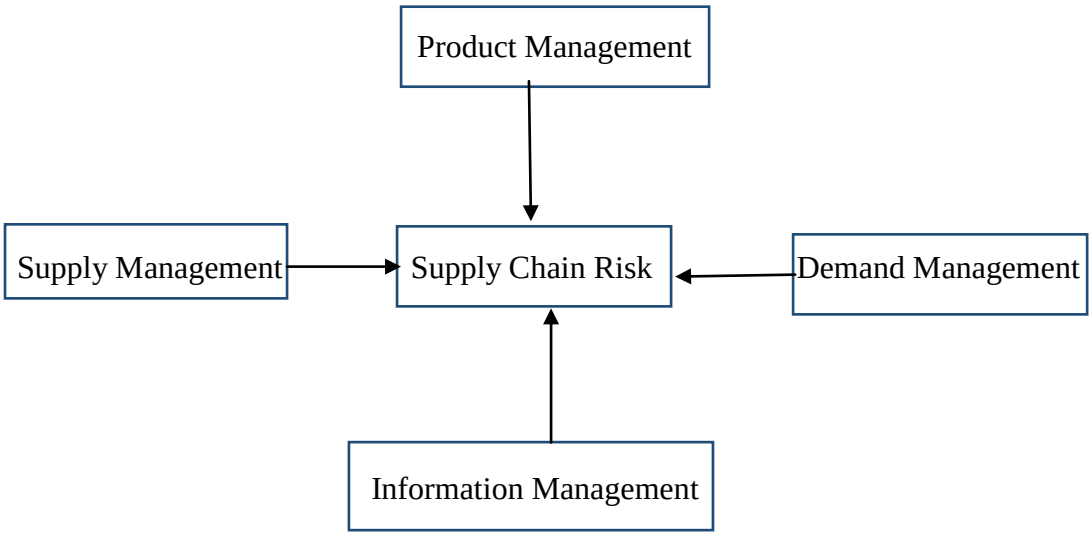

Figure 1.5 Four essential methods for managing supply chain risks

Source: Tang (2006)

In line with this, information systems protection is a critical issue faced by firms. Information system security practices implementation in firm is necessary for managing information systems security (Karydaa, Kiountouzisa, Kokolakisb, 2004). However, previous researches did not examined the relationship between risk management and information system security practices on supply chain performance.

The collaboration and integration among the supply chain business partner cause cyber supply chain risk management becomes a rising, critical and an important division of cyber security as the supply chain is more expose to cyber risk. Previous researcher did not highlight the consequences of cyber risks toward supply chain performance. Therefore, this study will be focused on the influences of cyber supply chain risk management on supply chain performance. According to Boyson (2014), cyber supply chain risk management is strategy implementation to reduce risks all the way through the processes which involve from product design stage, product development, production and deployment that form the supply chains for information technology networks as well as software and hardware systems. The complete range of cyber supply chain risk management structure is involve the whole system life cycle beginning with design and the firms' extended supply chain which is covers from vendors to clients (Boyson, 2014). It can be claimed as a tactical management action carry out in organizations that can influences operation and financial performance of firms (Narasimhan & Talluri, 2009).

This study provides comprehensive overview to enhance the understanding of the importance of cyber supply risk management in supply chain and its' effect on supply chain performance in Malaysia manufacturing sector.

1.3 Problem statement

In today business environment, firm stakeholders are working very hard to increase their performance in every aspect to increase the competitive advantages. Supply chain is very important to ensure the operations running smoothly in manufacturing organisation as supply chain disruptive will impact firm's overall performance which trigger from supply chain performance. Risk management has thus become a crucial topic for firm to increase or to retain high performance. The increasing number of journals in SCRM has recognized it as a key research area (Fahimnia et al., 2015). Therefore, this study to investigate the effect of internet related supply chain risk management on supply chain performance is limited in literature. Managing supply chain risks effectively needs a complete and quick assessment of all of the supply chain risk factors and their possible impacts on supply chain (Aqlan, 2015). A research project on cyber supply chain risk management carried out by Boyson (2014) in four years period to examine the capability or maturity for supply chain risk management in term of governance, systems integration and operation. The study aim to find out the common and the best practice related to this new field of study (Boyson, 2014). This study is extended Boyson's (2014) research and explored the influences of cyber supply chain risk management in term of governance, systems integration and operation on supply chain performance.

In additional, based on the report published by Dr. Amirudin Abdul Wahab, CEO of CyberSecurity Malaysia (2015), Malaysia ranked 9th in the top 15 countries in malware attacks, which is 1.97% out of 3,408, 112 cases between April 2013 and July 2014. The types of incidents that reported to CyberSecurity Malaysia include intrusion, intrusion attempt, Denial of Service Attack (DOS), fraud, cyber harassment, spam, content related, vulnerability report and malicious codes (CyberSecurity, 2015).

This survey outcomes showed that Malaysian network was vulnerable to cyber-attacks. In order to reduce cyber related issues that could bring negative effects and monetary lost to the nation and business, governance, firms as well as individual need to put more effort on cyber risk management.

Previous researches have proved positive effect of information technology on supply chain performance (Huo, Zhang, & Zhao, 2015). Garcia and Lambert (2003) also mentioned that application of information systems effectively has been recognized as an important enabler of supply chain agility (García-Dastugue & Lambert, 2003). Data sharing among purchasers and vendors through information technology has caused the development of theoretical supply chain which are information-based instead of inventory-based (Christopher, 2000). These researches shown information technology have positive and significant effect on supply chain agility or supply chain performance, but the studies do not highlight the existence of information risks such as information security, virus, system breakdown risks, hacker, cyber-attacks and intellectual property right risks which can harm the supply chain. Mohd Nishat et al (2007) provides numerous characteristics of information risks in supply chain and the guideline to manage information risks effectively (Mohd Nishat et al., 2007). Avelar-Sosa et al. (2014) has assessed the effects of some risk factors in the supply chain performance and concludes that infrastructure, government policies, and practices of lean manufacturing are not considered critical for the supply chain performance. Yet, they found that communication and integration with their suppliers as critical factors to improve supply chain performance. As articulated in Sodhi, Son and Tang (2012) research, it is basically difficult to classify supply chain risk management research because different researchers used different definitions, interpretations and synonyms

to explain supply chain risk management and related concepts from different perspectives.

Information technology issues and cyber-attacks are becoming growing risk to global supply chains. Cyber risks are the primary reason of supply chain disruption and monetary losses. In recent years, supply chain disruption incidents have grown significantly in recent years. For instance, breach of data invades charge an organizations an average of 5.5 million USD, while in 2012, the average loss related to wrongly placing a computer or laptop was 50,000 USD. Along with data losses, cyber-attacks can also cause the leakage of organizations' and customer's private information and cause destruction to a company's reputation. Technology is certainly a key enabler of a supply chain's operations. Thus, a cyber-attack is able to create risks to whole organization's supply chain and affect firm's performance (University Alliance, 2012).

Cyber-attacks will bring bad image and profit lost to an organization. For example, eBay faced the biggest cyber-attacks in 2014. In May 2014, eBay disclosed that hackers had managed to steal personal records of 233 million of it users. The hack took place between February and March. User's usernames, passwords and contact method compromised. Hackers successfully stole eBay credentials and managed to gain access to sensitive data. After the incident, eBay encouraged users to change their passwords and guarantee that financial information was not stolen, as it's stored separately and encrypted. Customers have complained on social media about late notification emails from ebay on the security issue and New York's attorney general called on eBay to provide free credit monitoring services to users. Such cyber incident definitely affect eBay's reputation and sales performance (Forbes, 2014).

Cyber terrorism attacks have become a pressing issue due to the shortage of a regular international agreement and the lack of international resolve. The increasing incidents of cyber-attacks against sovereign states and their critical information infrastructures require a global response. Regional and two-way agreements and local legislation are not adequate to prevent cyber-attacks (Moslemzadeh, Manap & Taji, 2013). Information systems are defenseless and it is possible for terrorists to take advantage of the vulnerabilities of information systems to attack their target opponents. Organizations that incorporate the critical infrastructure of the national economy should be aware of the potential for terrorist attack. Critical infrastructure refers to the essential assets which make society or a country function well and includes finance, telecommunication, energy, transportation, water supply and waste management, agriculture and food supply, public health and government services. Organizations which form the critical infrastructure of a national economy must protect their information systems well to avoid cyber terrorism attacks (Hua & Bapna, 2013). Therefore, cyber risk management is crucial to prevent cyber-attacks that would bring disruption to supply chain performance and negative effects on the firm economic benefit

According to Gartner, the world's leading information technology research and advisory company, investment in security is expected to reach $86 billion by 2016.1 The Internet age has raised many opportunities for cyber-criminals to attack organisations and while the motivation behind and the execution of these attacks varies, businesses and firms simply cannot afford to ignore the risks they present. In 2012, Dell SecureWorks researchers continued to observe large-scale global deployment of malware through the particular targeting of end-user systems. Email and web browsing were primary threat vectors used by cyber-criminals widely

deploying malware. Another famous cyber-attack that firms need to pay attention to is Distributed Denial of Service (DDoS). DDoS attacks tend to target shared, limited and consumable network environments. Historically, political and financial motivations drive cyber-attacks. For example, in 2012, fraudulent attempts in the financial sector where losses from $180,000 to $2.1 million. DDoS attacks were an indicator of an unauthorised wire transfer while longer attacks (lasting several hours or even days) signified fraudulent Automated Clearing House (ACH) transfers. The fraud attempts were non-trivial and were usually in the six-figure range, although some attempts reached millions of dollars (Pilling, 2013).

Information security in supply chain is an essential part to achieve supply chain efficiency and effectiveness as revealed in the past research. Basically, a business cannot get rid of the information security issues and its' effect of business performance. Thus, it is vitally important that an organization gives appropriate consideration to the information security fields, particularly its' influences on the supply chain performance. Security of information rising from different sources has becomes one of the biggest challenges in today's marketplace. Due to supply chains are claimed as a network of interconnected technology systems, it is necessary to investigate the information security practices in supply chain. However, majority of the researches done in technological, formal or informal controls of the area of information security (Dhillon, 2007). Based on Voss et al. (2008) suggestion that internal and external security initiatives supply chain will improve overall performance, a research on information security initiatives (ISI) on supply chain performance was carried out by Sindhuja (2014). The research failed to prove ISI have positive influence on SC performance. This shown that ISI could not influenced

supply chain performance directly. There are other deciding factors such as supply chain operations can act as an enabler for supply chain performance improvement.

SC performance can be improved by the selection and application of the right SC strategy. Previous studies was examining the relationships between SC strategy and SC performance suggested that effective deployment of information system into SCs is related with improved performance (Gunasekaran and Ngai,2004). Hence, manufacturing firms have to be aware of supply chain strategy is essential element to support different environmental uncertainty in order to sustain competitive advantage (Sun, Hsu & Hwang, 2009). While environmental uncertainties regularly influence supply chain performance and determine which competitive factors must be highlighted and assessed to help create a winning competitive strategy (Lee, 2002). Lee (2003) suggested an environmental uncertainty framework for organization to develop the proper SC strategy. Whereas, Sun, Hsu and Hwang (2009) conducted a study to investigate Lee's uncertainty framework and examine how alignment between supply chain strategy (agile, risk-hedging, efficient and responsive) and environmental uncertainty (supply and demand uncertainty) impacts perceived SCM performance. The results of the study suggested that an alignment between environmental uncertainties and SC strategies would positively impact SCM performance. However, SCM performance measurements involve numerous participants are difficult to describe and more variables should be included to prove and improvement SCM performance (Chan and Qi, 2003).

Thun and Hoenig (2011) revealed that the supply chain risk management has high possibility to enhance supply chains performance in the automotive industry and they mentioned that the idea could be transferred to further research on electronics industry

in order to check overall validity of the results from different industries (Thun & Hoenig, 2011).

1.4 Research Objectives

This study attempts to achieve the following research objectives below:

- To investigate the relationships between the Cyber Supply chain Risk Management and Supply Chain Performance
- To examine the mediator effects of information system security practices between Cyber Supply chain Risk Management and Supply Chain Performance
- To investigate influences of information system security practices on Supply Chain Performance

1.5 Research Questions

To achieve the above objectives, the research attempts to answer the following research questions:

1. What is the relationships between the Cyber Supply Chain Risk Management and Supply Chain Performance?
2. Does information system security practices mediate the relationship between Cyber Supply Chain Risk Management and Supply Chain Performance?
3. Do information system security practices affect Supply Chain Performance?

1.6 Definition of Key Terms

The following key term definitions are provided in order to share a better and common understanding on the concepts for future discussion.

1.6.1 Cyber

Is a prefix used to describe a person things, or idea as part of the computer and information age (Boyson, 2014)

1.6.2 Supply Chain

Is a system of manufacturers, suppliers, distributors, retailers and customers where raw material, financial and information flows connect the partners in upstream and downstream directions (Costantino et al., 2015)

1.6.3 Supply Chain Management

Is a set of methods used to connect suppliers, manufactures, warehouses and customers so that produces the goods at the right quantities, at the right time, to the right places with the objective of minimizing cost and maximize the customer service levels (Tuncel & Alpan, 2010)

1.6.4 Supply Chain Risk

An event that adversely affects supply chain operations and supply chain performance in term of service level, cost and responsiveness (Rao & Tobias, 2011)

1.6.5 Supply Chain Risk Management

Is a management of risk that implies both operational and operation horizons for short-term and long-term assessment (Lavastre, Gunasekaran, & Spalanzani, 2012).

1.6.6 Cyber Supply Chain Risk Management

Is a management of approaches, practices and methods from the fields of enterprise risk management, cybersecurity and supply chain management (Boyson, 2014).

1.6.7 Supply Chain Performance

The ability of the supply chain to offer products and services with good quality, on time and in accurate amounts and with the minimum costs (Avelar-Sosa, García-Alcaraz, & Castrellón-Torres, 2014)

1.6.8 Agility

Agility is the effective and flexible accommodation of unique customer demands (Yang, 2014)

1.6.9 Flexibility

Flexibility represents operational abilities within the supply chain functions (Swafford, Ghosh, & Murthy, 2008)

1.7 Significant of Study

Cyber supply chain risk management is an emerging topic in the risk management research. Firms are communicates with their customer, supplier and business via IT network and information system to improve supply chain performance. Previous scholars have proven that collaboration and integration among business partner can improved firm supply chain performance. Hence, managing cyber risks or information security risks is very crucial for firm to achieve highest performance. This study is among the pioneer empirical study on the effect of cyber supply chain risk management on supply chain performance. This could make several significant contributions to the industry and practitioner. Three contributions of study (i.e. theoretical, social and practitioner) are discussed as below:

1.7.1 Theoretical Contributions

Previous researches were more focus on the impact of risks assessment, risk management, the negative impact of cyber-attacks or cyber-crimes on economy performance and supply chain management on firm's financial performance and firm performance. There is limited focus and research on analyzing the risks associated with information risks and cyber risks in the cyber supply chain risk management. This study has extended the Boyson (2014) model of cyber supply chain risk management which links it to the information security best practices and firm supply chain performance. This study shall raise academic's awareness about the important of cyber supply chain risks management and its' effects on supply chain performance. This will be an emerging area for the supply chain researchers to further investigate the effects of cyber supply chain risks management on firm's supply chain

performance. Hence, this study represents one of the fresh attempts to provide a clear understanding on cyber supply chain risks management concept as well as the effects of cyber supply chain risks management on firm's supply chain performance.

1.7.2 Theoretical Contributions

As a result of globalization and high competition from the competitor, cyber supply chain shall be the proper strategy for firms to achieve competitive advantage and increase market share. The previous researches proved that supply chain risk management is very important to the firms responsiveness which is rely on information technology to manage their supply chain in order to increase supply chain performance.. This research will provides manufacturing industry, academia and government a better understanding on the influence of cyber risk management on performance as well as the contribution of information system security practices on firm's performance. Information system security practices is very critical for firms to manage information system risk or cyber threat as well as provide awareness and standardize the security practices within the origanisation. Moreover, this research will benefit to manufacturing industry such as contract manufacturer, original equipment manufacturer (OEM) and small and medium-size enterprises by providing related useful information or findings on how cyber risk management can improve their supply chain performance through a suitable risk management or the valid measurement of cyber security assessment.

1.7.3 Social Contributions

Cyber-attacks has been the discussing topic around the world due to the increasing use of information technology. There are various benefits that could experience from cyber risk management as society today is highly depend on information technology to smoothen their daily lives such as e-banking, e-commerce purchase, increasing use of social media and smart phone. If there is no awareness of risk management, users may face high possibility of hacking and cyber-attacks issue which lead to data loss and monetary loss. Implementation of cyber risk management will help to protect the business's information system from risk or minimize the possibility expose to cyber criminals. Buyers will get lower product price because of the high reliable production system as there is no extra cost or higher raw material price cause by supply chain disruption. Another benefit is job creating in cyber security specialist position as the awareness of risk is rising and firms definitely need more expert to establish high resilient control system in their organization to avoid cyber risk issue or any information system corresponding problems.

1.8 Organization of the Dissertation

This study is presented by five chapters. The first chapter provides an introduction as well as an overview and problem statement of this study. The second chapter presents the review of literature that summarizes previous studies, theoretical framework and the hypotheses development. Chapter three shows the research design on this study which consist sample collection, measurement of variables, the method of data analysis and expected outcome. Chapter four presents the findings which obtained from the results of data analysis and tested research hypotheses. Last chapter, chapter

five consists of the discussions, implications, limitations of the study and conclusion as the end of the study.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter is an overview on present and past literature on the key terms of this research (i.e. risk and supply chain management), overview of the industry in Malaysia; cyber supply chain risk management (governance, system integration and operation); Information system security policy compliance; and supply chain performance (Supply Chain Agility and Supply Chain Flexibility). Underlying theories include cumulative prospect theory and contingency theory. The theoretical framework and hypothesis development are presented as well at the end of the chapter.

2.2 Overview of Manufacturing Industry

Manufacturing industry is refers to those industries which involve in the manufacturing and the production of items in either creation of new commodities or in value addition. Manufacturing industries are basically classified into electronics industries, engineering industries, construction industries, chemical industries, energy industries, textile industries, food and beverage industries, metalworking industries, plastic industries, transport and telecommunication industries. (Economywatch, 2010). Manufacturing firms generally emphasize materials management to make sure no production disruption and sourcing activity for cost saving purpose.

A manufacturing operation can be defined as having four areas which are customers, suppliers, infrastructures and product range where interactions take place with broader supply chain networks (Tim, Gwyn, Sola, & Martin, 2005). A manufacturing

organisation is having four principal decision and it is concerned with the selection of activities carried out internally by the host company such as produce more or less for customers, purchase more or less from supplier, expand or focus product range and should buy in infrastructure to increase capabilities (Tim, Gwyn, Sola, & Martin, 2005). Figure 2.1 provides a visual aid of manufacturing operation associated with each of the four areas as per mentioned above.

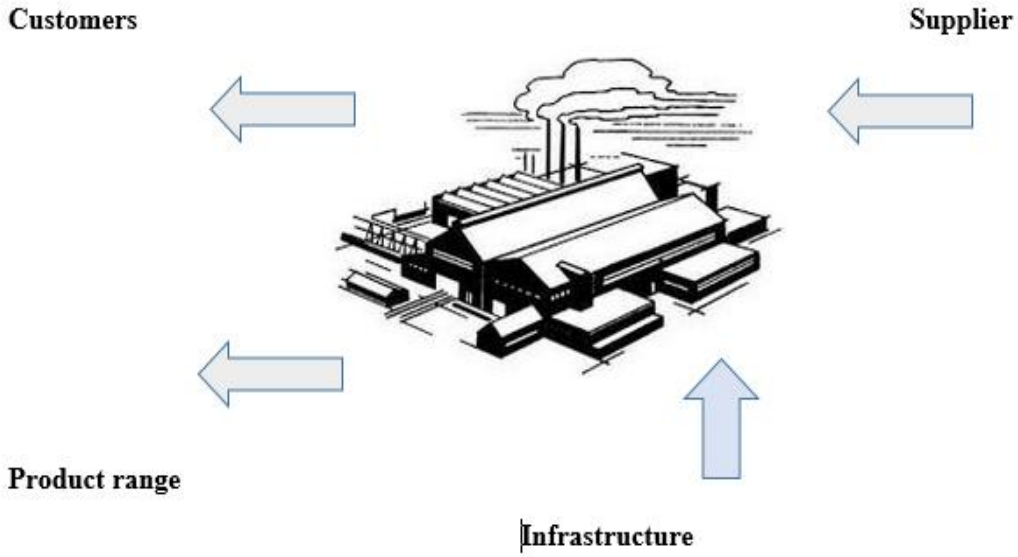

Figure 2.1 Manufacturing operation

Source: Tim, Gwyn, Sola, & Martin (2005)

The main objective of manufacturing firms is to satisfy customer's requirement and market demand. Hence, manufacturing industry require a good supply chain design to handle the whole process of the flow of material and information. They need a huge number of labor to deal with the daily business activities, suppliers to provide the requirement components and services as well as investment on equipment to allow employee to perform the tasks given which included the procuring, transporting,

manipulating the physical goods and information, and building relationships within customers or customers (Taylor, 2015).

As a result of increasing of globalization and wide use of internet or information technology in manufacturing industries, the supply chain is handled in a more effective and efficient way. However, the supply chain is facing variety of risks in daily business activities. Based on the report released by BSI and Business Continuity Institute in March 2015, approximately 35 % of firms in the manufacturing industry are very concerned about potential supply chain breakdown Manufacturing firms reported that the increasing of supply chain complexity and malicious attacks via the internet cause the business risks growing fast (MH&L, 2015).

2.3 Overview of Manufacturing Industry in Malaysia

According to Malaysian Investment Development Authority (MIDA), basically there are 11 main manufacturing industries that can be found in Malaysia. They are Non-Metallic Mineral Industry, Aerospace, Textiles and Textile Product, Basic Metal Products, Electrical and Electronic, Engineering Support, Food Technology and Sustainable Resources, Machinery and Equipment, Medical Devices, Petrochemical and Polymer Industry and Pharmaceuticals.

The electrical & electronics (E&E) industry is the leading sector in Malaysia's manufacturing industries and it plays a huge part Malaysian economy. E&E industries' significant contributions are large manufacturing output, supply of employment and high value of export business. The E&E industries can be classified into four sub-sectors, which are consumer electronics, electronic components, industrial components and electrical (MIDA,2015),.