THE EFFECT OF CYBER SUPPLY CHAIN SECURITY TOWARDS LEAN AND AGILE SUPPLY CHAIN PERFORMANCE IN HEALTHCARE INDUSTRY. THE MEDIATING EFFECT OF ORGANIZATIONAL CAPABILITIES

NUR SYAZWANI BINTI MOHD SATAR YIP

Research report in partial fulfilment of the requirements for the

Master of Business Administration

UNIVERSITY SAINS MALAYSIA

DEC 2015

ACKNOWLEDGEMENT

In the name of Allah S.W.T, the Most Beneficent and the Most Merciful. Praise and thanks are due to Allah S.W.T. for giving me strength and knowledge to complete this study.

Firstly, I would like to convey my sincere gratitude to my supervisors Dr. Yudi Fernando for his continuous guidance and supervision without which, this project would never have been initiated, let alone to be completed. His readiness to help the students, including me, is very commendable.

In addition, I would like to express my sincere thanks to all my colleagues and friends who have assisted in managing the questionnaires distribution and collection. I am truly appreciated to all whom willing to spend their time to involve in the survey.

Last but not least, special thanks to my beloved husband for his love, patience and full support in my study. I am very grateful to have both of my daughters who serves as the motivation and source of inspiration throughout my MBA studies in University Science of Malaysia

TABLE OF CONTENTS

LIST OF TABLE

LIST OF FIGURE

KESAN RANGKAIAN BEKALAN SIBER KESELAMATAN KE ARAH PRESTASI RANGKAIAN BEKALAN CEKAP DAN TANGKAS DALAM INDUSTRI KESIHATAN. PENGANTARA KESAN KEUPAYAAN ORGANISASI

ABSTRAK

Dalam dunia yang kompetitif, organisasi kesihatan menggunakan rantaian bekalan cekap, tangkas dan siber untuk meningkatkan prestasi rantaian bekalan mereka. Walau bagaimanapun, penggunaan kemudahan ini meningkatkankan risiko serangan siber. Oleh itu, keselamatan siber rantaian bekalan adalah penting untuk melindungi rantaian bekalan siber dan maklumat yang berharga daripada dicuri oleh penggodam. Selain itu, keupayaan organisasi adalah penting untuk memastikan pelaksanaan kejayaannya tanpa mengganggu rantaian bekalan yang cekap dan tangkas. Oleh itu, tujuan kajian ini adalah untuk mengkaji kesan keselamatan rantaian bekalan siber dalam prestasi rantaian bekalan cekap dan tangkas dan peranan keupayaan organisasi dalam melaksanakan keselamatan rantaian bekalan siber ke arah prestasi rantaian bekalan cekap dan tangkas. Rangka kerja teori dalam kajian ini dibentuk berdasarkan teori sistem bersepadu yang dibangunkan oleh Hong et al. 2003. Kajian ini telah dijalankan di seluruh Malaysia dengan jumlah 104 data diperoleh. Partial Least Square telah digunakan untuk menganalisis data dan hasil kajian ini menunjukkan bahawa peranan akses asas, membuat keputusan, tadbir urus teknologi maklumat, pengurusan operasi dan ketersediaan asset memainkan peranan penting dalam prestasi rantaian bekalan cekap di samping pengurusan operasi dan peraturan dan prosedur penting dalam prestasi rantaian bekalan tangkas. Selain itu, kajian ini juga mendapati bahawa pengurusan operasi pengantara hubungan antara tadbir urus teknologi maklumat dan rantaian bekalan tangkas. Dengan pengetahuan tentang factor tersebut, adalah diharapkan lebih banyak tindakan keselamatan yang lebih tertumpu dan berkesan boleh diambil untuk

menggalakkan bekalan siber keselamatan rantaian untuk mencapai prestasi rantaian bekalan yang cekap dan tangkas.

THE EFFECT OF CYBER SUPPLY CHAIN SECURITY TOWARDS LEAN AND AGILE SUPPLY CHAIN PERFORMANCE IN HEALTHCARE INDUSTRY. THE MEDIATING EFFECT OF ORGANIZATIONAL CAPABILITIES

ABSTRACT

In this competitive world nowadays, the healthcare organizations adopted lean and agile supply chain and cyber supply chain to improve their supply chain performance. However, the adoption of cyber supply chain increase the vulnerabilities and cyber-attack threats. Thus, cyber supply chain security is crucial in order to protect the organization's cyber supply chain and the valuable information from being stolen by the hackers. Besides, organizational capabilities is important to make sure its success implementation without disturbing the lean and agile supply chain. Hence, the purpose of this study was to investigate the impact of the cyber supply chain security in lean and agile supply chain performance and the role of organizational capabilities in implementing cyber supply chain security towards lean and agile supply chain performance. The theoretical framework in this study are formed based on the integrated systems theory developed by Hong et al. 2003. This study was conducted throughout Malaysia with total of 104 data collected from the survey. Partial Least Square was used to analyze the data and the result of this study revealed that role base access, decision making, Information technology governance, operation management and assets availability play important roles in lean supply chain performance while operation management and rule and procedure are important in agile supply chain performance. Besides that, this study also found out that operation management mediates the relationship between information technology governance and agile supply chain. With the knowledge of the factors that significantly affect lean and agile supply chain performance, it is hoped that more possible security actions may be taken that are more

focused and effective to promote effective cyber supply chain security to achieve lean and agile supply chain performance.

CHAPTER 1

INTRODUCTION

1.1 Introduction

This chapter introduces the research outline of the study. It begins with highlighting the background of the study and the problem statement followed by research objectives and research questions. Definition of key terms of major variables will also be included to assist in understanding. This chapter ends with the significance of the study and will give a brief overview of the remaining chapters in the thesis.

1.2 Background

Healthcare industry are undergoing a robust changes since the technological advancement. This can be seen through the innovations of electronic health records (EHR), Hospital Information System (HIS), and Telemedicine in healthcare industry in order to provide better health services for the community (Jha et al. 2008). Patients nowadays are demanding personalized and convenient care which the new technologies allow the patients to track their own health status and generate data that this is not possible during those days. The interaction between patient and the care providers especially doctor are changing with the diffusion of digital health.

The diffusion of technology also applied to the supply chain management in the healthcare industry organizations. The healthcare industry organizations are depending on the information technology system to assist their supply chain i.e.

Hospital Information System (HIS). This is due to supply chain management is very complex to manage as this involves a lot of supply chain members in the chain. Healthcare supply chain management is more complex compared to other industry due to the impact on people's health requiring adequate and accurate medical supply according to the patient's needs (Beier, 1995). Healthcare providers unable to predict patient's need and demand for a particular items or procedures. Thus, they are unable to predict or control their productions schedules (Jarrett, 1998). This is true enough when the doctors are requesting medical consumables items or pharmaceutical drug according to the need of the patients they are treating. Despite this, it is still perceived that there is significant scope to improve the overall performance of the supply chain (McKone-Sweet et al., 2005) i.e. adopting lean and agile supply chain (Arronson et al. 2011). The Hospital Information System (HIS) which supports all the processes of the treatment, from entry to release, has intensely resulted in lead time reduction. For example, the time spent on the transference of the X-ray from one ward to another would be eliminated. This system has also caused flexibility. In this system, the doctor can visit the patient online. Both of this are congruence with the lean and agile supply chain. This improvements in the supply chain in hospitals can lead to excellent operating room and pharmaceutical management, better inventory management, enhanced vendor relationships, more satisfied patients, and more effective work flow for hospital employees (Burt, 2006), including serving the needs of internal customers (Swinehart and Smith, 2005) such as the doctors.

Prabhu (1995) noted that the Hospital Information System (HIS) not only supports the office automation functions but also is used for managing routine hospital data management operations such as maintaining records on patient admission and registration information, patient accounting data, medical records

management, patient care management, and general financial and supply chain management. This hospital information systems also include huge batch data processing systems for billing operation, payroll, procurement to management information systems that support decision making at the middle and upper management levels. This shows that data security is critically important for hospital information systems (HIS) as it hold a huge volume of data.

Besides that, the healthcare organizations also involve in the activities through the internet based electronic commerce, like e-procurement and e-banking. E-procurement in the healthcare organization are involving the activities to procure the consumable medical items, pharmaceutical products, medical devices and many more by sending the purchase order generated from the supply chain technology systems for examples Hospital information system (HIS), Enterprise Resource Planning (ERP) directly to the respective vendor through email once it generated. E-banking involving the payment of their suppliers and daily money transactions of the patient bills through internet based system like SunSystems. SunSystems is a web enabled global financial and business software to assist the organizations in their financial and accounting management.

All these initiatives and transformation that taken up by the healthcare industry organizations are involving big data which are highly susceptible to the hackers to stole these information if there is no proper cyber security in place. This can be seen in the recent report in Free Malaysia Today where 67.6% of cyber security attacks reported in Malaysia Healthcare sector was through spam mails and there is a 62 % spike in the global front (Free Malaysia Today, 2014)

Cyber supply chain security is the effort to enhance the cyber security in the supply chain network through implementing firewall to block the intruders from stealing the valuable data. Malware, cyber terrorism, advanced persistent threat and data theft are those threat that need to be managed by cyber supply chain security. Nowadays, there are a lot of data security breaches detected with the diffusion of the technology advancement like internet based electronic commerce in to the organization. (Linton et. al, 2014, Grant et. al, 2013, & Warren and Hutchinson, 2000). Although there are robust changes in the healthcare organization industry to improve the supply chain, a lot of healthcare industry organizations neglected the importance of cyber supply chain security. This can be seen in the electronic health record data entry which is done by the unlicensed individual i.e. medical scribes which is supervised by the clinician. This activity increased the vulnerabilities of the electronic health record where these group of individual are able to see and steal the patient valuable information without knowledge of the physician (Gellert et al., 2015) According to Antonelli et al., (2006), the biggest threat for the cyber supply chain i.e. electronic health record (EHR), hospital information systems (HIS), Enterprise Resource Planning (ERP) are from the internal users such as employees and other trusted constituents with access to organizational information resources. Moreover, the case study done by Mohammed et al., (2015) found that most healthcare sector organizations did not comply to the three prominent Acts by the federal government i.e. Privacy Act of 1974, Health Insurance Portability and Accountability Act (HIPAA), and Health Information Technology for Economic and Clinical Health Act (HITECH) to regulate and protect the confidentiality of personal information in the Healthcare system which resulted in information breaches.

According to the 2010 HIMSS Analytic report, it stated that the Healthcare industry organizations are actively taking steps to ensure the security of the data but this efforts seems to be more reactive compared to proactive as the organizations having more resources on the breach responses compared to the prevention of security breaches. Cyber security is important in the advancement of new technology era as a lot of organizations are moving towards electronic based information technology systems in assisting the management of supply chain.

Moreover, cyber supply chain security is also important in healthcare industry as result in the data breaches involving big data will lead to supply chain disruptions, criminal fines, financial loss and loss of reputation. Malaysia's Healthcare sectors are vulnerable to hacking due to they are less protected compared to other sectors and little investment made on this cyber security (Free Malaysia Today, 2014) This might be due to lack of knowledge and expertise in both of this sectors. Cyber security are important to maintain big data involving supply chain in healthcare industry as it is highly susceptible to threat by hackers. According to Grant (2013), organization that fail to address and plan the technological risks and issues will results in distrust, poor decision making, poor communications, poor customer service and poor material flow.

In order to be proactive and responsive to the cyber security attack, the organizations need to employ agile supply chain strategies. This is due to agile supply chain is defined as the ability to respond to unanticipated changes. On the other hand, the organization's supply chain performance can be improved by lean supply chain strategies adoption as lean supply chain is the reduction in the waste and non-valued added activity (Azevedo et al., 2012; Carvalho et al., 2012; Carvalho et al., 2009;

Azevedo et al., 2011, Marshall and Farahbakhsh, 2013). Lean and agile supply chain are a hot topic discussed in the literature review whereby these practices are successfully adopted in the manufacturing company (Arronson et. al 2011) and their supply chain performance is improved. Healthcare industry organization adopt lean and agile supply chain to improve their supply chain performance but there is lack of study to prove how does this affect the supply chain agility and leanness . However, by applying both of these concepts, it is predicted that there is a reduction in cost of the operations and increase in customer satisfaction.

From the literature on Lean in healthcare, lean is frequently associated with the material flow and not the patient flow. This can be seen from the seven Ohno's (1998) where the transportation, inventory, overproduction, waiting, processing defects and motions in healthcare are based on material management (Jimmerson, 2010). Lean management implies using less effort, investment, time, inventory to achieve greater efficiency and fewer errors (Womack et al., 1990). Through Lean management, the operational performance is improved by removing complexity from processes (Womack and Jones, 2003) Some steps towards lean for examples just in time (JIT) are already taken where some organizations in healthcare industry are implementing vendor managed inventory (VMI) to reduce excess waste, complexity ,disruptions in supply chain and thus improving their supply chain management. However, there are not much initiatives taken in Malaysia organization's in healthcare industry towards lean where most of the organizations did not implement VMI and still having excessive inventory stock in their material store. There still a lot of write off to dispose of the expired stock which lead to financial loss to the organizations.

On the other hand, in order for the organizations able to anticipate changes in the market, there need to adopt agile which is implementing information technology system (Harrisson et al. 1999, Van Hoek 2001) like HIS, and ERP systems to assist their organizations operations and supply chain to avoid any disruption of the supply chain. However, there are not all of the Malaysia's organizations in healthcare industry are implementing the information technology systems as there were only 15.2% of Malaysian public hospitals have fully or partially integrated HIS after the announcement of the Telehealth project in 1997 (MOH Malaysia, 2014, Ahmadi et al., 2015)

In order to achieve the cyber supply chain security and lean and agile supply chain performance, the organizations need to identify the important organizational capabilities. Organizational capability is defined as organization's capabilities to manage the resources like employees, assets in order to achieve competitive advantage. Organizational capability is important during the implementation of information security (Hall et al., 2011). Organizations need to focus on their most important organizational capabilities in order to manage the cyber supply chain securities and achieve success in lean and agile supply chain.

1.3 Problem Statement

The awareness of security of data in Malaysia can be seen through the implementation of the Data protection Act on 15 November 2013 in which the organizations were given three months to comply with the law and any violation of this act will lead to imprisonment maximum one year jail and fine up to RM100,000

(Malay mail, 2013). This is to protect the personal information being accessed and abused by the irrelevant parties. Organizations in healthcare industry are crucial in implementing the data protection act as they hold a huge volume of data on personal, sensitive personal data and vendor's data. An example of personal data is name, address, and examples of the sensitive personal data are physical and mental health. Besides that, examples of vendor's data are transaction history, price list of items supplied to the organizations in healthcare industry.

Recently, cyber security attacks on healthcare industry organizations are alarming and beyond control with breaches costing the healthcare provider an average of $2.4 million per year. There are 67.6% of cyber security attack reported in Malaysia Healthcare sector were through spam mails (Free Malaysia Today, 2014) while on the global front there are 62% spike in the number of data breaches which resulting 552 million of identities are exposed (Free Malaysia Today, 2014). With the evolution of the technology across the supply chain in healthcare industry, the identifiable data and other valuable data are highly exposed and susceptible to the threat, the important organizational capabilities need to be addressed while managing the cyber supply chain security in healthcare industry's organization.

Cyber-attacks against business performance will cause losses in the operational, financial and the customer will lose trust on the organization. The operation of the organizations will be disrupted if cyber-attack occurred as most of the operations are relying on the electronic and internet enabled system. Besides, the customer who is injured by the loss the security of data will seek for compensation through law suit cases. The good will and the reputation of the organization will be affected if this incidence happens. This will directly affect the supply chain performance of the particular organization that is being attacked by the hackers as their supply chain will

be disrupted which will lead to financial loss on the organization. Wolden et al. (2015) found out that the implementation of COBIT 5 information security framework will reduce the Supply Chain Management System from the cyber-attacks but there is limited studies on the impact of cyber-attacks on supply chain performance. Herzog (2010) studied on the Estonian cyber-attacks that discusses on the cyber-attack incidence in Estonian which cause a lot of disruption i.e. banking government operations, banking transactions, city power grids, and even military weapon systems. In order to enrich the literature on cyber-attack, this studies took the opportunity to link cyber supply chain security and supply chain performances.

There is lack of empirical studies conducted on the impact of cyber supply chain security on the lean and agile supply chain. However, there are few studies conducted on the lean and agile supply chain in healthcare industry's organization which is conducted by (Arronson et al. 2011, Kumar et. al 2008, Machado Guimarães and Carvalho, 2013). Most of the study on lean and agile supply chain are not survey based research and its lead to inability to generalize the outcome of lean and agile supply chain in whole healthcare industry (Fariborz and Mahdi, 2010; Arronson et al. 2011). According to Tom et al. (2009), most of the lean supply chain studies on the operation aspect and their link to performance but limited in the healthcare industry setting. Besides that, lean supply chain studies are mostly speculative work where there are no concrete evidences on lean supply chain implementation in healthcare (Luciano, 2009). Luciano (2009) also found out that most of the case study branded as lean supply chain whereby there just implement one or two metrics of lean supply chain and does not implement it as a whole. Most of the lean and agile studies in healthcare are mainly concentrate on patient and product supply chain management driven while no attention on the cyber supply chain security. On the other hand, agile

supply chain studies conducted are mainly focused on the pharmaceutical company (Mehralian et al., 2015) where this finding cannot be generalized to the healthcare industry as pharmaceutical company are only a subset of the whole healthcare industry and most of the studies are done outside of Malaysia. Besides that, most of the pharmaceutical company mainly involved in manufacturing and does not provide services to the i.e. healthcare provider to the community. Hence, this study took the opportunity to enrich the literature on the lean and agile supply chain in the whole healthcare industry in Malaysia.

On the other hand, organizational capabilities is a critical aspect need to be considered during the implementation of cyber supply chain security. Limited literature available on the cyber supply chain security in the healthcare industry provides research opportunity. Besides that, relationships between organizational capabilities towards information security implementation strategies are conducted by Hall et al (2011) but this study does not reflect the whole picture on the cyber supply chain security and organizational capabilities. Thus, this study takes this opportunity to link the organizational capabilities with cyber supply chain security and lean and agile supply chain. Moreover, the specific theoretical framework which linked of supply chain cyber security, organizational performance and lean and agile supply chain performance is limited in literature.

1.4 Research Objectives

The research objective of this study is mainly to investigate lean and agile supply chain performance and its importance in improving the supply chain performance in Malaysia's organization in healthcare industry. The cyber supply chain security

impact is addressed in order to increase the awareness among the Malaysia's organization in healthcare industry when incorporating organizational capabilities and their impact on lean and agile supply chain performance. Besides that, this study also investigate the relationship between cyber supply chain security and the organizational capabilities in Malaysia's healthcare industry organization. The research objectives are stated as follow:

1. To investigate the effect of the cyber supply chain security on lean-supply chains performance
2. To examine the effect of the cyber supply chain security on agile-supply chains performance
3. To examine the effect of the cyber supply chain security on organizational capabilities
4. To determine the effect of organizational capabilities on lean-supply chains performance
5. To determine the effect of organizational capabilities on agile-supply chains performance
6. To investigate the mediating effect of organizational capabilities on the relationship between cyber supply chain security on lean-supply chains performance
7. To investigate the mediating effect of organizational capabilities on the relationship between cyber supply chain security on agile-supply chains performance

1.5 Research Questions

To analyse the organizational capabilities and cyber supply chain security implementation effect on lean and agile supply chain in Malaysia's organization in healthcare industry, seven major questions are developed.

1. What is effect of the cyber supply chain security on lean-supply chains performance?
2. What is effect of the cyber supply chain security on agile-supply chains performance?
3. What is effect of the cyber supply chain security on organizational capabilities?
4. What is effect of organizational capabilities on lean-supply chains performance?
5. What is effect of organizational capabilities on agile-supply chains performance?
6. What is the mediating effect organizational capabilities on the relationship between cyber supply chain security on lean-supply chains performance?
7. What is the mediating effect of organizational capabilities on the relationship between cyber supply chain security on agile-supply chains performance?

1.6 Significance of the Study

Malaysia's organization in healthcare industry are growing rapidly and evolving nowadays in terms of supply chain data management and access, making the information more digital and easily accessible through the technology advancement which will lead the data to be exposed and highly susceptible to the hackers. Therefore it is vital to address this cyber supply chain security issue. Recently, the cyber security attacks on the organization in healthcare industry are alarming where there are 600 percent increase in attacks on United States hospital in the period of ten month from October 2013 to August 2014 (Technewsworld, 2014) and 67.6% of cyber security attack in Malaysia Healthcare sector and 552 million of identities are exposed (Free Malaysia Today, 2014). These incidences become a great concern in Malaysia. This can be shown by the implementation of the Data Protection Act on 2013 to create awareness among the organization who holds and deal with data. Organization also need to focus on their organizational capabilities while managing cyber supply chain security in order to achieve success in lean and agile supply chain

1.6.1 Theoretical Contribution:

Cyber supply chain security is critical aspect need to be considered during the implementation of lean and agile supply chains but there is lack of studies on the cyber supply chain security in the healthcare supply chain management. Besides that, there are studies conducted on the lean and agile supply chain in healthcare organization which is conducted by previous scholars (Arronson et. al 2011, Kumar et. al 2008, Machado Guimarães & Carvalho, 2013) that mostly conducted in qualitative such as case study method where there is only single organization

observed and unable to provide such guideline to entire healthcare industry. On the other hand, the organizational capabilities are important in implementation of cyber supply chain security and lean and agile supply chain. The impact of organizational capabilities on information securities strategies implementation success are conducted by Hall et al. (2011) where this study linked the cyber supply chain security with organizational capabilities. However, there are limited empirical studies conducted that linked of lean and agile supply chain management cyber supply chain security and organizational capabilities. Thus, the this study is attempt to fill the gap by provide the empirical finding on the effect of cyber security on lean and agile supply chain performance in healthcare industry's organization which mediated by organizational capabilities.

1.6.2 Practical Contribution:

The findings of this study will increase the awareness of the organization in healthcare industry's personnel and the top management on the importance of the lean and agile supply chain, cyber supply chain security and organizational capabilities. The organizations can use this study finding as a guide for them to develop the standard operating procedure to be implemented during the access of data and operational management in hospital information systems platform in order to secure their cyber supply chain. Besides that, the healthcare industry organization can use this study finding to identify the important organizational capabilities to achieve lean and agile supply chain while managing the supply chain cyber security. This is due to organizational capabilities is important in the organizations as this is to ensure the organizations to achieve competitive advantage against other competitor in the market. Organizations need to focus their main organizational capabilities in order to

achieve success in cyber supply chain security implementations and lean and agile supply chain.

Moreover, the healthcare industry organizations will understand the critical aspect to manage the impact of the cyber supply chain security on lean and agile supply chain performance. This will help the healthcare industry organization to better design, perform and monitor usage of supply chain technology system i.e. hospital information systems (HIS) and electronic health record (EHR) by recognizing the important organizational capabilities without compromising the data security which will lead to better supply chain performance. Lean and agile supply chain are consider benchmark to achieve better supply chain performance as these practices will lead to cost reductions and increase customer service or satisfaction level. However, there are still slow of implementation both of these practices in healthcare industry's organization in Malaysia. Hence, the organizations can learn how to achieve lean and agile supply chain performance from this study.

On the other hand, the implementation of this Data Protection Act has received a lot of responds with positive and negative view and some of the parties are still ignorant on this act implementation. However, the implementation of this act will assure that the data are kept properly and will reduce the risk of data breaches and loss incurred by data breaches. Through this study, the organizations will increase their awareness by implementing this act to secure data from the hackers with a proper cyber supply chain security in place.

1.7 Definition of Key Terms

- **Cyber supply chain: S**upply chain which is enhanced by cyber-based technologies (in other word information technology) in order to establish an effective value chain (Poirier, 2003)
- **Lean supply chain:** eliminate the non - added value activities from the supply chain workflow without disturbing the performance (Carvalho et al., 2009; Azevedo et al., 2011**).**
- **Agile supply chain:** ability to respond rapidly and cost effectively to unpredictable changes in markets and increasing levels of environmental turbulence, both in terms of volume and variety (Carvalho et al., 2009; Azevedo et al., 2011)
- **Organizational Capabilities:** intangible assets consist of competencies along with dynamics of integrating and deploying those competencies with inimitable resources across organizational boundaries to operate business. Competencies refer to differentiated knowledge, skill, ability, distinctive organizational processes, and other characteristics needed to perform a specific task (Hall et al. 2011).
- **Supply chain performance**: improvement initiatives that strive to match supply and demand, thereby driving down costs simultaneously with improving customer satisfaction (Mason-Jones 2010)

1.8 Organization of the Remaining Chapters

This study is structured in five chapters. The first chapter provides an introduction as well as an overview of this study. The second chapter presents the review of literature that outlines previous studies undertaken in relation to cyber supply chain security, theoretical framework and the hypotheses development. Chapter three will illustrate the data and variable in term of research design, sample collection, measurement of variables, the method of data analysis and expected outcome. Chapter four will illustrate the data analysis and research findings. Lastly, chapter five will present the overall findings and implications of the research will be discussed, limitation of the study as well as suggestion for future research and conclusions.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter will present the previous literature that has been undertaken. As such, this chapter will give an overview of literature on cyber supply chain security, organizational capabilities, lean and agile supply chain performance and the underlying theory. The theoretical framework and the hypothesis development will be presented towards the end of the chapter.

2.2 Overview of Healthcare Industry in Malaysia

Over the past decades, the healthcare sector has seen a robust growth. Changing demographic and more health conscious lifestyles among the people has led to the growth of this industry. This industry previously denominated by the public healthcare sector and there are tremendous growth of private healthcare services currently in Malaysia. There are 210 of private hospitals with more than 10,000 beds in year 2011 (Thomas, 2011) and approximate 130 public hospitals in Malaysia (Economic Transformation Programme, 2010). Private hospitals offer a wide range of expertise in medical fields in order to attract more people to seek medical treatment in private hospital. Malaysia healthcare systems are operating in two tier systems which consisting of government run universal healthcare systems and private healthcare systems. 70% are government run universal healthcare services which are used by majority of the Malaysian populations and 30 % are the private healthcare systems.

Malaysia is a developing country who placed the information system or information technology under the government's vision 2020 plan (Mohan & Raja Yacoob 2004) which known as Telemedicine Blueprint under the Multimedia Super Corridor Telehealth project which is launched since 1997 to reform the Malaysia healthcare system (Sibte et al., 1998) According to Li, (2010), out of 130 public hospitals in Malaysia, there are 18 public hospitals are fully equipped with the hospital information systems(HIS). HIS integrates computer systems in the whole hospitals to enhance the administrative and clinical functions of the hospitals (Kim, Lee & Kim 2002). HIS applications also developed to communicate in regards to procurement, finance and human resources in Health Ministry.

Besides that, Malaysia are offering medical tourism in order to attract foreign patients to seek healthcare treatment abroad from their origin country while having vacation in Malaysia. According to statistic published in the Malaysia Healthcare Travel Councils, there are 882,000 healthcare traveller in year 2014 that seeks for treatment while having their vacations in Malaysia (Hwei Khai & Fernando 2015) Most of the private hospital are regulated by Ministry of health and most of them have internationally recognized accreditations for examples, JCI (Joint Commission International) that accredits healthcare organizations in United States.

2.3 Reviews of relevant theories

Theory is important to understand the relationship of dependent variables and independent variables. The underlying theory would serve as the basis for measurement and help to explain and test the proposed relations among variables in a study. Integrated system theory are used in this study in order to understand the

relationships between the cyber supply chain security which is the independent variable and lean and agile supply chain performance which is the dependent variables. This study adopted the COBIT 5 (Control Objectives for Information and Related Technology) Part 5.

2.3.1 Integrated Systems theory

Integrated System theory is based on several theories which are closely linked to the purpose of this study. This theory is based on the contingency management and integrates information security policies, internal control, risk management and information auditing to form this information security architecture to meet the organizational objectives (Hong et al., 2003). This theory provides information security strategies, theories and procedures and explains the organizational behaviours towards management of the information securities and organizational management of information strategy alternatives. This theory also useful for information security decision making (Hong et al 2003).

Security policies are important in enforcing security practices in an organization. Even if the organizations employed the latest technology, there is still a need to enforce the information security policies in order for the technology adopted to run smoothly and efficiently. In this study, we adopt this dimension under the rule and procedures and role based access dimensions as this dimension is congruence with the security policy. Policies and procedures describe the generalized view of a job that govern who does what on the job (Stouffer et al. 2011) Policies are implemented in the organization ranging from organization policies to operational constraints such as access control. Access control can be implemented through role based access which is in line with this study dimension. Besides that, rule and procedure and role based

access are also part of the dimension under the COBIT 5 (Control Objectives for Information and Related Technology) Part 5 framework (Wolden et al., 2015).

Information security implementation strategy are part of the contingency theory as contingency management meant for preventions, detection and reactions to the vulnerabilities and threat from inside and outside of the organizations. Contingency approach is to recognize and responds to the situational variables in order to achieve organizational objectives (Robbin, 1994). The organizations need to deploy information security implementation strategy in order to secure their cyber supply chain and achieve better supply chain performance which are the organizational objectives. Besides that, information technology governance are also part of risk management in this theory as vulnerabilities can occur if there is a mismanagement of risk. Risk assessment can also be used to figure out appropriate actions to manage information security risks which is line with information security implement strategy objectives. Risk management theory suggests that by analyzing and evaluating the institutional risk, the vulnerabilities and threat can be estimate which can assist to plan the information security measures for the organizations.

Control and auditing theory suggests that each organizations measures the control performance of the information security control systems that already implemented in the organizations (Hong et al., 2003) Control is always defined as prevent and detect activities in the systems to avoid illegal and unauthorized access and activities in the systems. This is in line with the information technology governance as organizations need to follow the information technology governance practices as this practices is to make sure that the enterprise's information technology that implemented in the organization will sustains (IT governance institute, 2007).

There is limited literature on this theory. Suhaila and Elena 2014 adopted this theory to access the security of the supervisory control and data acquisition (SCADA) systems which are used to remotely control and monitor the critical infrastructure. The study results showed that the organizations have adequate security policy in place in order to secure their information systems and have the access control implemented for risk management. Besides that, access control is also important in determining the rules and responsibilities of the employees in the organizations. Most of the organizations having the proper security measurement systems in place to access their security performance.

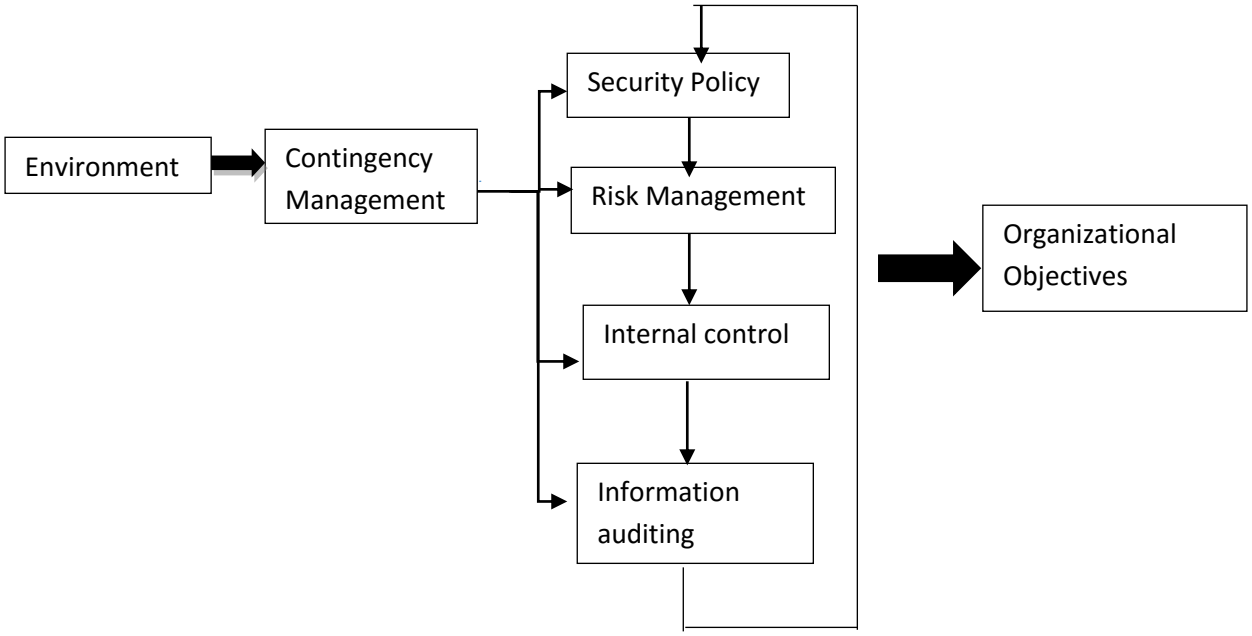

Figure 2.0 Integrated system theory schematic diagram (source: Hong et al., 2003)

2.3.2 COBIT Framework

COBIT is an information technology (IT) management model and high level guideline for IT resources i.e. personnel, applications, data and hardware to achieve

the organizational objective through balancing the risk and controlling measures (COBIT, 1998) Wiesmann A. et al., (2005) illustrated the objective and functionality of COBIT framework as a risk-management based framework and classified as an IT governance framework. It considers all aspects of information and information communication technology (ICT) infrastructure, the usage has also been expanded to the management of the organizations as it can be used to help to provide appropriate guidance for ICT governance. The guideline is meant to assist senior management to implement an appropriate information security management capability in facilitating business growth through the sensible use of technology. Wolden et al. (2015) adopt this framework in reductions of cyber-attack risks in supply chain management systems and found out that the organizations benefited from implementing this COBIT 5 security framework measures.

2.4 Supply Chain Performance

Supply chains are value chains that extends from manufacturer to the ultimate customers where a lot of members are involved in this supply chain. Due to this, the supply chain managers need to integrate all the supply chain members in the organizations i.e. marketing, production, finance, logistic and procurement with the supply chain partners. Lee (2004) contends that the success of the organizations that comprise of the supply chain are depending on the ability to meet the ultimate customer demands, response to the changing market by restructuring their supply chain, aligning the marketing, productions, and financial strategies throughout the supply chain. This shows that the supply chain performance are important in the organization’s success.

The success and failure of supply chains are ultimately determined in the marketplace by the end consumer. Getting the right product, at the right price, at the right time to the consumer are important keys to sustain in the turbulence market. Supply chain performance improvement initiatives strive to match supply and demand, thereby driving down costs simultaneously with improving customer satisfaction. The uncertainty within the supply chain need to be reduced to facilitate predictable upstream demand as this will help the manufacturer to predict the products volume need to be manufactured and fulfill the demand of their respective customers. Sometimes, the uncertainty is impossible to remove from the supply chain due to the type of product involved (Mason-Jones 2010) This is in line in the healthcare industry organizations whereby the patients volumes are unpredictable (Arronsson et al., 2011) and also the product used (Faroborz & Mahdi, 2010). This can be seen when there is an epidemic outbreak like influenza flu, the patient volume will be increased drastically and the face mask demand will be increased too. Thus, different supply chain faced with different type of situation of uncertainty and they need to develop strategy to overcome this uncertainties in order to match supply and demand and improve the supply chain performance. (Mason-Jones & Towill 1999).

The potential of supply chain performance are not maximized mainly due to failure to integrate the respective partner's need (Gunasekaran et al., 2013). There are few supply chain performance measures that are recommended which encompass both operational and financial measures. The operational measures inclusive of inventory and operating cost, delivery performance and supply chain flexibility (Ahmad and Schroeder, 2003; Gunasekaran et al., 2001; Gunasekaran et al., 2013) while financial measures are return of assets (ROA) and profit (Gunasekaran et al., 2001). Besides