ENHANCING SUPPLY CHAIN RESILIENCE BY ADDRESSING THE ACHILLES HEEL OF INFORMATION SHARING

TAN HWEE CHIN

UNIVERSITI SAINS MALAYSIA

2019

ENHANCING SUPPLY CHAIN RESILIENCE BY ADDRESSING THE ACHILLES HEEL OF INFORMATION SHARING

by

TAN HWEE CHIN

Thesis submitted in fulfillment of the requirement
for the degree of
Master of Arts

April 2019

ACKNOWLEDGEMENT

The success and final outcome of the research required a lot of guidance and assistance from many people and I am using this opportunity to express my sincere appreciation to everyone who supported me. First and foremost, I would like to express my deepest gratitude to my main supervisor, Associate Professor Dr. Wong Wai Peng, who contribution in stimulating suggestions, encouragement, financial support and helped me to coordinate my Master study. I could not have imagined having a better supervisor for her insightful comments, and provided me an opportunity to be her Research Assistance (RA) for widen my research perspectives. Without her precious support it would not be possible conduct this research. Besides, my sincere thanks also goes to my co-supervisor, Professor Tan Kim Hua.

Most importantly, none of this could have happened without my family and friends. I would like to acknowledge with much appreciation to my parents (Mr. Tan Ten Kee @ Tan Teng Kee and Ms. Ng Sew Lee) and siblings for their unconditional love and encouragement. Moreover, I am deeply thankful to all of my friends especially Ms. Ong Saw Kin, Ms. Ng Yueh Shiun and Ms. Lee Lih Kian for their moral support and delightful companionship. Special thanks to my bosom friend, Mr. Lim Yu Qing and his family members, for supporting me spiritually throughout writing this thesis over last several years.

Furthermore, many thanks go to my friends from academia and experts from manufacturing of Malaysian Multinational Corporation (MNCs) who have engaged in intellectual discussion with me that had helped me in generating fruitful ideas in qualitative study. I would also like to thanks the respondents who involved in the

validation survey for this research. Without their passionate participation, the validation survey could not have been successfully conducted. Hopefully, all the findings in this study are beneficial to relative field.

Last but not least, I would not forget to appreciate to all administrative staffs and friends at School of Management (SOM). Thank you for their encouragement, advice and support, especially Ms. Robitah Spian, Ms. Siti noorjannah bt Abd Halim and Ms. Sarina Harun. I would also like to thank you Universiti Sains Malaysia (USM) for awarding me the Graduate Assistant Scheme. Receiving this scholarship helped to reduce my financial burdens. My sincere appreciation for USM generosity.

TABLE OF CONTENTS

CHAPTER 2 - LITERATURE REVIEW

LIST OF TABLE

LIST OF FIGURES

LIST OF ABBREVIATIONS

CFI	Comparative Fit Index
df	Degree of Freedom
GFI	Goodness-of-Fit
IFI	Increment fit index
NFI	Normed Fit Index
PGFI	Parsimony Goodness of Fit Index
PNFI	Parsimony Normed Fit Index
RMSEA	Root Mean Square Error Approximation
SRMR	Standardized Root Mean Square Residual
TLI	Tucker-Lewis coefficient index
χ^2/df	Chi-square normalized by degrees of freedom
AMOS	Analysis of Moment Structures
AVE	Average Variance Extracted
BIC	Business Continuity Institute
CB-SEM	Covariance Based- Structural Equation Modelling
CISOs	Chief Information Security Officers
CMV	Common Method Variance
CR	Composite Reliability
f^2	Effect Size
FDI	Foreign Direct Investment
FMM	Federation of Malaysian Manufactures
GDP	Gross Domestic Product
GOF	Goodness of Fit
GST	Goods and Services Tax
ISC	Information Security Culture
ISE	Information Sharing Effectiveness
MDBC	Malaysian Dutch Business Council
MIDA	Malaysian Investment Development Authority

MMA	Malaysia Medical Association
MNCs	Multinational Corporations
OCT	Organizational Culture Theory
OEC	Organizational Ethical Climate
OIPT	Organizational Information Processing Theory
PAPI	Paper and Pencil Instrument
PLS	Partial Least Square
PLS-SEM	Partial Least Square - Structural Equation Modeling
PwC	PricewaterhouseCoopers
R^2	Coefficient of Determination
RBV	Resource Based View
SCR	Supply Chain Resilience
SCRM	Supply Chin Risk Management
SEM	Structural Equation Modelling
SPSS	Statistical Package for Social Sciences
UNCTAD	United Nations Conference on Trade and Development
VIF	Variance inflation factors
WEF	World Economic Forum
α	Cronbach's alpha
β	Standard Beta

MENINGKATKAN KETAHANAN RANTAIAN BEKALAN DENGAN MENGATASI KELEMAHAN PERKONGSIAN MAKLUMAT

ABSTRAK

Kebocoran maklumat telah menjadi kebimbangan utama bagi amalan perkongsian maklumat, dan pendekatan pengurusan untuk meringankan risiko dalam rantaian bekalan. Oleh itu, kajian ini menunjukkan laluan bagi daya tahan rantaian bekalan yang diperolehi daripada hubungan kebocoran maklumat kepada keberkesanan perkongsian maklumat dengan pendekatan mitigasi. Kajian ini menunjukkan keberkesanan perkongsian maklumat membolehkan tindak balas pantas terhadap kebocoran pendekatan mitigasi dan meningkatkan daya tahan yang mungkin memberikan daya saing terhadap pesaing metentasi rantaian bekalan. Pengkaji menggunakan pendekatan kajian gabungan kaedah kuantitatif dan kualitatif. Data kuantitatif digunakan untuk merumuskan hasil kajian daripada kualitatif. Pertama, kajian kualitatif (Pensampelan Bertujuan) digunakan untuk mengetahui hasil analisis kajian lima kes Syarikat Multinasional Malaysia dalam rantaian bekalan. Cara utama pengumpulan data adalah temu bual separa berstruktur dan dokumen cetak juga dikumpulkan. Syarikat pembuatan yang terpilih menyumbang untuk mengisi jurang dengan memeriksa strategi mitigasi untuk kebocoran bagi memcapai keberkesanan perkongsian maklumat. Keputusannya telah membangunkan rangka kerja penerokaan yang mendedahkan iklim etika organisasi dan budaya keselamatan maklumat sebagai faktor-faktor baru yang berguna bagi mengurangkan kesan-kesan buruk terhadap keberkesanan perkongsian maklumat. Kedua, satu kajian kuantitatif (Persampelan Bertujuan) dijalankan bagi mengesahkan kerangka empirik dengan menggunakan

borang soal selidik yang diedarkan kepada MNC Malaysia, yang kebanyakannya syarikat perkilangan merentasi rantaian bekalan. Sebanyak 278 borang soal selidik dijawab dengan lengkap oleh responden. Tujuan kajian kuantitatif adalah untuk mengkaji hubungan antara kebocoran maklumat dan keberkesanan perkongsian maklumat dengan strategi mitigasi untuk meningkatkan ketahan rantaian bekalan. Hasil kajian ini telah membuktikan kesan kuat dari kebocoran secara sengaja dan tidak sengaja ang mempunyai kesan buruk terhadap keberkesanan perkongsian maklumat. Dapatan hasil kajian menekankan peranan kritikal budaya keselamatan maklumat sebagai peranan penting dalam mengurangkan kesan kebocoran maklumat, tetapi iklim etika organisasi tidak dapat mengurankan kesannya. Ini berbeza dengan iklim etika organisasi. Akhirnya, kajian ini memberikan pandangan baru yang membuktikan bahawa keberkesanan perkongsian maklumat sebagai mediator bagi mewujudkan hubungan antara kebocoran maklumat dengan ketahanan rantaian bekalan. Kesimpulannya, ia percaya bahawa penemuan kajian ini membolehkan organisasi yang terlibat dalam perkongsian maklumat dapat menilai atau mengawal kebocoran maklumat dengan mencari penyelesaian terbaik dan mengambil tindakan pembetulan serta merta.

ENHANCING SUPPLY CHAIN RESILIENCE BY ADDRESSING THE ACHILLES HEEL OF INFORMATION SHARING

ABSTRACT

The risks of information leakage associated with information sharing across supply chains are still not well-defined. It is clear that managerial approaches in mitigating such risks are needed. Therefore, this study demonstrates pathways to supply chain resilience derived from linkages of information leakage to information sharing effectiveness with mitigation approaches. It shows the information sharing effectiveness enables quick response to leakage by mitigation approaches and increase resilience, which might provide a competitive edge over their competitor across a supply chain. This study designed a sequential exploratory mixed method approach by combining qualitative and quantitative studies. First, purposeful sampling in a qualitative study was adopted involving semi-structured interviews with five cases of Malaysia Multinational Corporations predominantly in the manufacturing sector. Interviews with managers gain deeper insights into the risks of information leakage involved and developed appropriate mitigation strategies when sharing information with supply chain partners. The main study findings are synthesized into a theoretical framework that revealed organization ethical climate and information security culture are new useful approaches to mitigate the devastating consequences on information sharing effectiveness. Second, purposive sampling in a quantitative study was conducted to empirically verify the framework by using a questionnaire distributed to Malaysian MNCs, predominately in the manufacturing sector. A total of 278 completed questionnaires were received from respondents. The purpose of quantitative study tends to examine the relationship

between information leakage and information sharing effectiveness with mitigation approaches in order to enhance supply chain resilience. As a result, this research has proven the powerful impact of intentional and unintentional leakages have devastating consequences on information sharing effectiveness. The finding also highlighted the vital role of information security culture is able to reduce the impact of information leakage, but organizational ethical climate could not mitigate its impact. This is a sharp contrast to the qualitative finding of organizational ethical climate. Lastly, this study provided new insights demonstrating that the information sharing effectiveness as a partial mediator of the relationship between information leakage and supply chain resilience. This finding appears to be of particular interest to security practitioners in protecting their information assets within organizations. It is believe that organizations involved in information sharing to make better-informed decisions concerning information sharing across their supply chain.

LIST OF PUBLICATION

Tan, H. C., & Wong, W. P. (2016). The factors of information leakage and mitigating roles of organizational ethical climate and information security culture in information sharing integrity. Paper presented at the *22nd International Society for Business Innovation & Technology Management (ISBITM): Sustainable Development Goals in Business Decision Making Model*, The Mandarin Hotel, Bangkok.

CHAPTER 1

INTRODUCTION

1.0 Introduction

In today's global supply chains were associated with increased level of interconnectedness among partners (suppliers, manufacturers, distributors etc.), which led to higher level of dependency between the two entities as well as supply chain complexity. Business environments become more instability and unpredictability may resulted in vulnerable to supply chain disruptions (Blackhurst, Dunn, & Craighead, 2011; Kamalahmadi & Parast, 2016; Pettit, Croxton, & Fiksel, 2013). A recent Business Continuity Institute (BCI) found that 65 percent of companies experienced at least one major disruption (BCI, 2017). The findings of report also highlighted that the top three causes of disruption are unplanned IT or telecommunications outages, cyber-attack and data breach, and loss of talent/skills (BCI, 2017). Interestingly, cyber-attack and data breach are expected to be the biggest concern for the next 12 months by organizations across the supply chain (BCI, 2017). It poses a serious issue of confidential information which is disclosed to unauthorized partners either intentionally or unintentionally (Anand & Goyal, 2009; Tan, Wong, & Chung, 2016; Zhang, Zeng, Wang, Li, & Geng, 2011). Leakage of proprietary information can be devastating to supply chain operations. Therefore, this research is focus intensely on the key threat of "information leakage" as refer to supply chain disruption.

In many cases, inaccurate or distorted information create havoc and disruption to the supply chain. The main reason of information gets distorted is due

to leak false information within or along supply chain network for their own benefits (Huong Tran, Childerhouse, & Deakins, 2016; Mishra, Raghunathan, & Yue, 2007). As theorized by the bullwhip effect phenomenon, as information travels farther away from the source in the supply chain, it will be distorted and eventually the final information which will be received at the other end of the supply chain will not be exactly the original form (Chatfield, Kim, Harrison, & Hayya, 2004; Lee, Padmanabhan, & Whang, 1997). Along the way when information travels, information leak to unregistered party, and this further adds to the risk and complexities in the supply chain. Hence, integral and wholesome information sharing across the supply chain is very difficult to be achieved due to information leakage. Information leakage needs to be curbed if organizations need to gain competitive advantage through information sharing (Huong Tran et al., 2016; Tan et al., 2016; Zhang, Cao, Wang, & Zeng, 2012). Thus, academics and managers have high interest to gain a deeper insight about the harmful effect of information leakage increases the difficulty level to achieve information sharing effectiveness along supply chain or within organization.

Generally, to overcome emerging problem from information leakage on information sharing practice, managerial approaches in mitigating such risk in supply chain are needed. Effective managerial approaches can increase the visibility across the entire supply chain to prevent significant risks (Busse, Schleper, Weilenmann, & Wagner, 2017). Without being fully aware of the risks and mitigation measures of information leakage, it would be an extremely difficult task to achieve information sharing effectiveness and sustain organization competitive advantages. Organization should be able to share appropriate information confidently and clearly, yet prevent

data leakage. It is therefore extremely important to be able identify and mitigate information leakage within a supply chain.

Since most published literature highlights the importance of information sharing is key collaborative working and risk reduction for improving supply chain resilience (Christopher & Peck, 2004; Kamalahmadi & Parast, 2016; Scholten & Schilder, 2015). As stated by Scholten and Schilder (2015), information sharing enables an organization to increases visibility, flexibility and velocity across the supply chain. Sharing relevant information is able to improve greater visibility by providing transparency needed in order to establish trust and foster commitment among supply chain partners (Mandal, 2012). In other words, information which is shared by the sender to the receiver remains wholesome and undistorted that is useful for making timely production, inventory management, packaging and logistics management decision. Organizations overlook the importance of investment in information sharing effectiveness can mitigate supply chain risks, prevent disruptions, and respond quickly to uncertainly in order to achieve competitive advantage. Hence, information sharing effectiveness as a driver of supply chain resilience.

To address the research questions, we designed a sequential exploratory mixed method approach by combining two studies. First, we conducted a qualitative case study to investigate the factor triggering information leakage and mitigation approaches on information sharing effectiveness. We try to fill this gap by examining how to gain deeper insights about approaches to mitigate information leakage in order to achieve information sharing effectiveness. Then, a quantitative study was conducted to examine the relationship between information leakage and information sharing effectiveness with mitigation strategies in order to enhance supply chain resilience. An understanding of overview perceptions of information leakage and its

preventive measures is key to get deeper insights into inter-organization information sharing within a supply chain.

1.1 Background of Study

1.1.1 Building a Supply Chain Resilience (SCR)

Disruptions in the supply chain can be related to any unplanned and unanticipated events that disrupt the normal flow of information, materials and/or finance (Barroso, Machado, & Machado, 2011; Craighead, Blackhurst, Rungtusanatham, & Handfield, 2007). These disruptions can lead to numerous adverse effects on organization's operations and performance (Blackhurst et al., 2011). In the past decade, supply chain disruptions have increasingly attracted the interest of academics and practitioners, which are caused by both natural disaster and intentional or unintentional human actions (Snyder et al., 2016; Tukamuhabwa, Stevenson, Busby, & Zorzini, 2015). According to Craighead et al. (2007) supply chain disruptions are inevitable and inherently risky which may reduce capacity on the whole supply chain. Therefore, organizations always seek to understand the impact of disruptions and maintain effective supply chain operations.

In 2003, Jüttner, Peck and Christopher were first to introduce a fundamental conceptualization of supply chain risk management as "quick fix" solutions of disruptive events. The prime objective of SCRM is to identifying the potential sources of risks, and implementation of appropriate strategies through a coordinated approach among supply chain risk members, to mitigate supply chain vulnerability (Jüttner, Peck, & Christopher, 2003; Manuj & Mentzer, 2008; Singhal, Agarwal, & Mittal, 2011). Organizations engage in traditional supply chain risk management

(SCRM) can mitigate the negative effects on disruption but not all disruptions can be prevented (Scholten & Schilder, 2015). There are been serious limitations of SCRM, include organization relies too heavily on risk identification and statistical information. Unfortunately, risks are completely hidden and statistical information may not exist (Fiksel, Polyviou, Croxton, & Pettit, 2015).

To address above limitations, SCR has received more attention in the past few years to enhance traditional risk management strategies (Kamalahmadi & Parast, 2016). Clearly, supply chain risk management and resilience are closely related, and to build SCR (Mandal, 2012). The idea of recovering from supply chain disruptions by constructing SCR has gained considerable support outside academic circles (e.g. Barroso et al., 2011; Brandon-Jones, Squire, Autry, & Petersen, 2014; Christopher & Peck, 2004; Kamalahmadi & Parast, 2016; Ponomarov & Holcomb, 2009; Tukamuhabwa et al., 2015). SCR is a proactive and holistic approach that builds the adaptive capability to handle unpredictable and unknowable disruptions (Scholten, Sharkey Scott, & Fynes, 2014; Tukamuhabwa et al., 2015). Resilience enables a supply chain to be prepared for a disruptive event, reduce the impact of a disruption and strengthens the ability to recover immediately by ensuring the continuity of operations at the desired level and control over structure and function (Blackhurst et al., 2011; Kamalahmadi & Parast, 2016; Ponomarov & Holcomb, 2009). As such, SCR requires a clear understanding and conceptualization in this research.

Christopher and Peck (2004) introduced principles of SCR is the most commonly cited as a basis for creating the SCR including supply chain reengineering, supply chain collaboration, agility and supply chain risk management culture, as shown in Figure 1.1 (Christopher, Mena, Khan, & Yurt, 2011; Kamalahmadi &

Parast, 2016; Mandal, 2012; Scholten & Schilder, 2015; Wieland & Wallenburg, 2013).

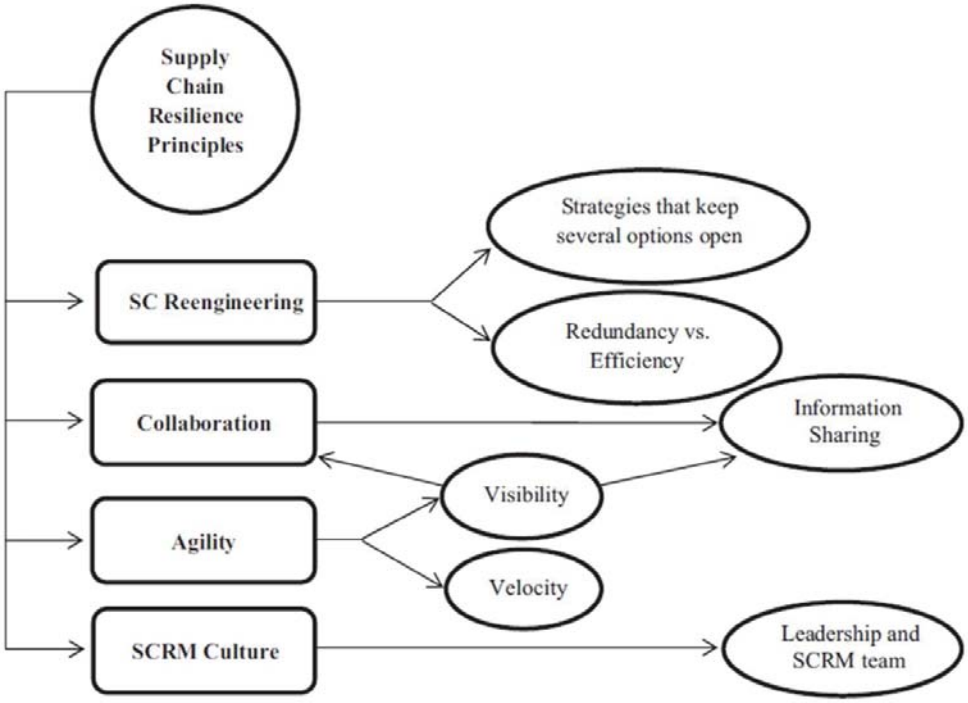

Figure 1.1. Creating the resilient supply chain. Adapted from "Building the resilient supply chain," by M. Christopher, & H. Peck, 2004, *the international journal of logistics management*, *15*(2), 1-14.

SCR definitions and principles are prevalence discussed in literature review, while some researchers focus on SCR strategy (Carvalho, Maleki, & Cruz-Machado, 2012; Erol, Sauser, & Mansouri, 2010; Kamalahmadi & Parast, 2016; Scholten et al., 2014; Tukamuhabwa et al., 2015). Tukamuhabwa et al. (2015) indicated that there are twenty-four strategies for building SCR can broadly be organized into two separate categories: proactive (pre-event) and reactive (post-event). A proactive strategy is having a plan in place to mitigate disruptions before it happen whereas, a reactive strategy is evolving to meet environmental change with practical action (Hohenstein, Feisel, Hartmann, & Giunipero, 2015; Scholten et al., 2014; van der

Vegt, Essens, Wahlström, & George, 2015; Wieland & Wallenburg, 2013). Proactive strategies or reactive strategies can be applied depending on when and why necessary response to certain situations and problems (Tukamuhabwa et al., 2015). Such strategies ability to deal with disruptions during three phases: before, throughout and after an incident (Kamalahmadi & Parast, 2016). Hence, resiliency is an effective way to deal with unexpected risks and recover quickly from a disruption across the supply chain (Blackhurst et al., 2011).

In conclusion, the idea of SCR attractive as a hot topics in operations management that highly investigated by researchers who wish to have greater impact on business (de Oliveira, Marins, Rocha, & Salomon, 2017; Sodhi, Son, & Tang, 2012). It is important for organizations cultivate resilience to deal with unpredicted disruptions for both short-term and long-term successes.

1.1.2 Supply Chain Information Sharing Risks

The topic of information sharing between supply chain partners has been on the agenda for decades, drawing attention from both researchers and practitioners (Kembro & Selviaridis, 2015). Supply chain information sharing refers to the extent of the exchange of sensitive information that may facilitate inter-organizational collaboration among supply chain partners (Li, Ye, & Sheu, 2014). Advocates of information sharing highlight the potential benefits of using valuable information to improve overall supply chain performance (Fawcett, Osterhaus, Magnan, Brau, & McCarter, 2007; Kembro, Näslund, & Olhager, 2017; Lee & Whang, 2000). Despite having potential to greatly benefits from information sharing, organizations are still reluctant to share confidential information with supply chain partners (Huong Tran et

al., 2016; Kembro & Selviaridis, 2015). This is because the critical issues and challenges associated with disclosure of confidential information, which are particularly difficult enough to overcome in a supply chain network (Sharma & Routroy, 2016; Tan et al., 2016; Zhang et al., 2011; Zhang et al., 2012).

Anand and Mendelson (1997) were among the first to explicitly model information flows in a supply chain and explore the specific components, including information sharing, information leakage, and information acquisition. If acquired, demand information is always disseminated in the supply chain, aided by leakage (Anand & Goya, 2009). Information leakage is a serious threat that inference in the supply chain systematically, when a given amount of information shared (Zhang et al., 2011). Arguably, organizations are encouraging to realize that speed up the flow of information throughout the supply chain may cause high possibility of disclosing confidential information to other parties (Ahmad, Tscherning, Bosua, & Scheepers, 2015).

In general, information leakage can be defined as organization's sensitive information is either intentionally or unintentionally disclosed to unauthorized parties (Huong Tran et al., 2016; Kong, Rajagopalan, & Zhang 2017; Tan et al., 2016). In supply chain, intentional leakage issues occur when incentives was offered. It should be noted that some organizations involve a deliberate distortion of information, as it flow across the various business entities along supply chain (Li, 2002; Mishra et al., 2007). There is a huge amount of suffering from information distortion to misguide various business entities (retailers, distributors and others) in supply chain (Sharma & Routroy, 2016). As a result, the informed business entities refused to receive any information (e.g. inaccurate or delayed information) flow within the supply chain and to conceal its information (Zhang et al., 2011).

Moreover, unintentional disclosure occurs when sensitive information is shared via poorly managed and unmonitored information flows (Manatsa & Mclaren, 2008). In particular, organizations faced increased security vulnerabilities due to lack of cybersecurity preparedness can lead to degradation in information quality and loss of confidential information across the supply chain (Madenas, Tiwari, Turner, & Peachey, 2015). Besides, security vulnerabilities often create dramatic loss of profit, market share, and credibility. The most badly, affecting the level of trust and commitment in supply chain (Zhang & Li, 2006).

In conclusion, information leakage issues are most salient when sharing such valuable information across the supply chain (Kong, Rajagopalan, & Zhang, 2013). The proprietary information is the basic for all reporting and crucial in business. It allows a business to make informed decision by analysis the data in business strategic. Therefore, information leakage issue has been proven in previous studies, organizations struggle with information leakage prevention consequences of refusal to share information across their supply chain (Huong Tran et al., 2016; Tan et al., 2016).

1.1.3 The Malaysian Scenario

Malaysia is a strategically located in the heart of South East Asia and offers a cost-competitive location for investors to set up offshore operations for regional and international markets (MDBC, 2018). Malaysia offers many advantages including, well-developed infrastructure, productive workforce (human resource), technological advancement, and also provides supportive government policies among developing countries (MIDA, 2018). According to the Global Competitiveness Report 2017-

2018 released by the World Economic Forum (WEF), Malaysia takes 23rd spot out of more than 130 countries. Which means Malaysia's policies are on the right track to sustain momentum in economic growth, in line with the government's efforts to become a high-income nation by 2020.

In Malaysia, the numbers of Multinational Corporations (MNCs) have grown tremendously due to Malaysia's geographical location in the region, multilingual capabilities and abundance skill workers (Economic Transformation Programme, 2016). According to the World Investment Prospects Survey 2016-2018 FDI by the United Nations Conference on Trade and Development (UNCTAD), Malaysia ranks as among the world's top 15 attractive countries for foreign direct investment (FDI). The report said multinational companies and global giants on the Fortune 500 and Forbes 2000 lists such as IBM, General Electric and GlaxoSmithKline consistently recognise Malaysia as a valuable centre in their global operations. In 2016, Malaysia managed to attract investment worth RM 207.9 billion in mostly high quality projects despite the challenges from external headwinds (MIDA, 2017).

As an open economy, the Malaysian economy is progressing from a position of strength. The latest East Asia and Pacific Economic Update, launched by the World Bank (2017) reported that Malaysia's gross domestic product (GDP) growth rate is predicted to rise from 4.9% in June as domestic economic activities accelerated by 5.7 year on year during first half of 2017, which is slightly above the government's current projection range of 4.3-4.8 percent. Besides, the Malaysian economy is expected to sustain its current growth momentum in to 2018 and 2019. Thus, Figure 1.2 shows Malaysia's GDP expected to grow by 4.9% next year and 5.0% in 2019. As result of perceptive foresight, Malaysia is a strong economic fundamental to attract foreign investors.

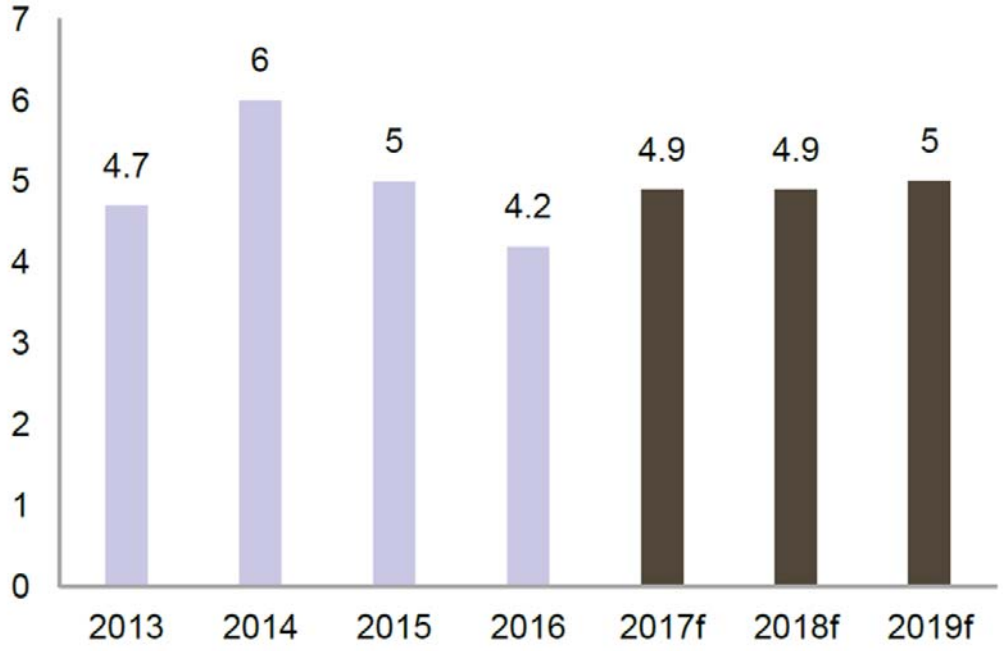

Figure 1.2. GDP growth is expected to accelerate to 4.9 % in 2017. From "Malaysia economic monitor June 2017: Data for development," by The Work Bank Group, 2017, (http://www.worldbank.org/en/country/malaysia/publication/malaysia-economic-monitor-june-2017-data-for-development).

Nevertheless, Malaysia obtained fundamentals remain strong with a stable labour market conditions and manageable inflation to support a sustained momentum in economic growth. The unemployment rate was 3.4% of the labour force, while the labour force participation rate was sustained, in Q4 2017, at 68 % of the total working-age population (The World Bank Group, 2018a). While underlying inflation moderated towards the end of 2017, there remain concerns regarding cost of living pressures due (The World Bank Group, 2018a). Malaysia's central bank is expected inflations rates remain manageable amid solid economic growth.

Furthermore, Malaysia has simple, transparent rules for registering a business, paying taxes earlier by introducing an online system for filling and paying goods and services tax (GST), getting credit to provide investors credit scores and registering property helps create a level playing field for doing business (The World Bank,

2018b). According to its "Doing Business 2018" report, Malaysia is ranked 24 amongst 190 countries in the ease of doing business (The World Bank Group, 2018b). Therefore, Malaysia is a business-friendly that provides MNCs with opportunities for growth and profits.

In conclusion, prospects for the Malaysia is well on its way to creating such a bright business landscape by its economic fundamentals. This favourable investment landscape is ripe for foreign entities and MNCs to join in on the Malaysian growth story. Thus, this is the main reason Malaysia MNCs conducted in this research.

1.2 Problem Statement

There are many examples of significant supply chain disruption in Malaysia context. Recently many media in Malaysia covered that a total of 46.2 million mobile numbers are at stake in which could possibly be the largest personal data breaches ever seen in the country (The Star Online, 2017). The Department of Statistics Malaysia (2018) indicated that the population in Malaysia is around 32.4 million. The list of mobile numbers is assumed to include all inactive numbers and temporary numbers bought by foreign visitors. Apart from that, 81,309 medical records are also leaked from the Malaysian Medical Council, Malaysia Medical Association (MMA) and Malaysian Dental Association (The Star Online, 2017). There will be challenges ahead for Malaysia has retained its 4th place ranking in the emerging markets index, which is an example of a market with an open economy that has positioned itself as a highly attractive export location (Transport Intelligence, 2018).

According to InfoWatch (2017) declared that leakages of confidential information from MNCs such as Alibaba, Amazon, Apple, BMW, eBay, Google,

Huawei, Microsoft, Samsung, Uber, Yahoo and others are been a great deal of discussion due to its fault. It is not uncommon for MNCs require close collaboration among supply chain partners in many different locations around the world. The risk associated with inter-organizational exchange information either intentionally or unintentionally disclose confidential information to any unauthorized parties that will cause massive disruptions at every node or link in the supply chain network. Such disruptions can lead to numerous problems and adverse consequences in organizational routines. Therefore, Malaysian MNCs are becoming much more interested in understanding the risks associated with inter-organizational exchange information within a supply chain.

The Global Data Leakage Report 2017 by InfoWatch presented the latest issue of information leakage in 2017 (see Figure 1.3). There were 2131 leaks of confidential information reported, has become even worse than the previous years (InfoWatch, 2017). This figure does not include data breaches or records disclosed incidents that go unreported every day. Information leakage in proprietary data can be considered as type of risks when inter-organizational exchange information across the supply chain (Anand & Goyal, 2009; Tan et al., 2016; Zhang et al., 2011). In fact, information leakage could be driven by internal and external parties to provide its data to outside organization (Tan et al., 2016). InfoWatch (2017) has been proved that among the data leaks logged, 39.5% of the cases are triggered by external attacks, while 60.5% are caused by internal offenders (see Figure 1.4). This result in there being a clear understanding the probability of insider offenders continues to cause significant damage to organization's information assets higher than external attackers.

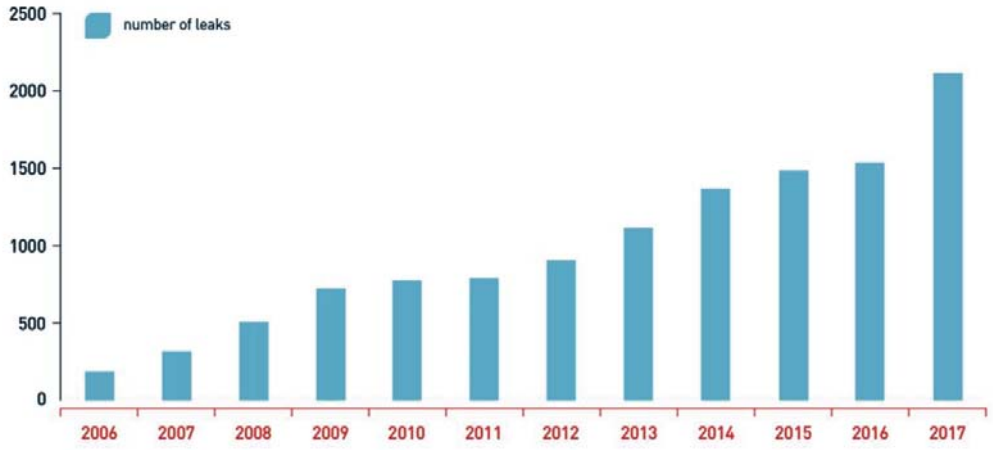

Figure 1.3. Number of registered data leaks, 2006-2017. From "Global data leakage report, 2017," by InfoWatch, 2017 (https://infowatch.com/sites/default/files/report/Global_Data_Leak_Report_2017_ENG.pdf)

Figure 1.4. Leaks by attack vector, 2017. From "Global data leakage report, 2017", by InfoWatch, 2017 (https://infowatch.com/sites/default/files/report/Global_Data_Leak_Report_2017_ENG.pdf)

Traditionally, organizations have paid considerable attention to physical assets and ignored inculcating appropriate and acceptable behaviors of insiders (Tseng & Fan, 2011). Based on a review of recent information leakage, one common thread in such ethical scandals is the insider ex-post incentives offered by external parties (Tan et al., 2016). Insiders are targeted by competitors or third parties for intentional disruptive, unethical or illegal behavior to compromise confidential

information for personal gains (Omar, 2015). This particular behavior is a deviant or unethical act that violates organization norms (formal or informal organizational policies, rules, and procedures) and threatens the well-being of trading partners within supply chain information sharing (Robinson & Bennett, 1995). Thus, ethical issues constitute a major topic that deserves more attention for the protection of information assets within a supply chain (Da Veiga & Eloff, 2010).

To achieve the national 2020 vision, the present and future quality of Malaysia's human capital refers as a composite of knowledge, skills and tools of ethics for driving inclusive and sustainable economic growth (Economic Planning Unit, Prime Minister's Department, 2017). In Malaysian organizations, a well-written code of ethics clarifies appropriate behaviour for insiders that shape the culture of an organization (Suruhanjaya Syarikat Malaysia, 2016), but most of the organization's mission and vision statements may or may not give an indicator of the ethical dimension (Yekta, 2010). All business decisions and actions have an ethical or moral dimension, yet in the process of setting vision and mission, ethical issues always poorly discussed. Organizations are striving to achieve declared vision and mission may willingly leak vital confidential information to unauthorized parties within a supply chain (Tan et al., 2016). This applies in today's work force are turning to unethical practices in an attempt to keep their jobs or derive some benefits (monetary benefits, technology acquisition etc.) for its organization (Haron, Ismail, & Na 2015; Tan et al., 2016). Hence, failure to explore ethical dimension consistent with the organization's mission and vision will leave today's business critically vulnerable to an information leakage within a supply chain.

Besides, most of the Malaysian organizations are unconcerned about cybercrimes lead to data security breach. PricewaterhouseCoopers (PwC) was

conducted a survey in Malaysia Global Economic Crime Survey 2016 (Malaysia report), only 35% of Malaysian respondents had a fully operational cyber incident response plan. With more than half (54%) of Malaysian organizations indicated that they were unsure what exactly is the risk of and what types of risks exist (PwC, 2016). Besides, the organizations are likely to be confronted with numerous security attacks when automated systems often required to temporarily remove the computer's firewall for information exchange (Anand & Goyal, 2009; Tan et al., 2016). If inter-organizational information sharing systems are not sufficiently security protected, a risk of exposure through information leakage can result in losing of trust among supply chain partners (Zhang & Li, 2006). Besides, another biggest challenge in Malaysian organizations is the lack of cyber security talent capable of responding to cyber-attacks. This translates to a drastically low number of Chief Information security officers (CISOs) within the private and public sectors in Malaysia (Cyber Security Malaysia: An agency under MOSTI, 2016). Hence, Malaysian organizations are responsible to keep confidential information undistorted, accurate and up to date across the wider supply network.

Moreover, information leakage can be caused by organizations fail to implement security standard ISO/IEC 27001 in Malaysia. ISO/IEC 27001 is the information security management approach to protect organization confidential information, minimize business damage, maximise return on investment and business opportunity (Department of Standards Malaysia, 2016). Unfortunately, Malaysia only has 35 (1.8%) companies registered under ISO/IEC 27001 certificate in 2017 (Department of Standards Malaysia, 2017). In other words, only a small amount of Malaysian organizations implement standard security practices to protect information assets. In reality, inter-organization information sharing is becoming increasingly

complex, and the information system design and implementation also costly (Huong Tran et al., 2016). These have costly repercussions for every supply chain partner (Madenas et al., 2015). Therefore, only few Malaysian organizations are willing to pay a premium prices for ISO/IEC 27001 certified to minimize security breaches and avoid fines.

In conclusion, leakages of confidential information from MNCs across the supply chain are been a great deal of discussion in most countries. Based on current scenario, Malaysia is seriously facing challenges and security risks related to the sensitive information being exchanged. Leakage of confidential information causes a disruption to supply chain operations. For the above reasons, much attention is now focused on Malaysian MNCs to mitigate information leakage in providing rich and appropriate approaches to achieve information sharing effectiveness, even better than original condition that leads to gain a competitive advantage.

1.3 Research Objectives

1.3.1 Qualitative Phase

1. To reveal factors triggering information leakage.
2. To investigate information leakage as having devastating consequences on information sharing effectiveness.
3. To explore mitigation approaches of information leakage.

1.3.2 Quantitative Phase

1. To explore the relationship between intentional leakage and information sharing effectiveness.
2. To investigate the relationship unintentional leakage and information sharing effectiveness.
3. To examine the role of organizational ethical climate is moderating the relationship between the intentional leakage and information sharing effectiveness.
4. To study the role of organizational ethical climate is moderating the relationship between the unintentional leakage and information sharing effectiveness.
5. To identify the role of information security culture is moderating the relationship between the intentional leakage and information sharing effectiveness.
6. To recognize the role of information security culture is moderating the relationship between the unintentional leakage and information sharing effectiveness.
7. To investigate the role of information sharing effectiveness is mediating the relationship between information leakage (intentional leakage and unintentional leakage) and supply chain resilience.

1.4 Research Questions

This study attempts to answer the central question, "How information leakage can be mitigated by Malaysia Multinational Corporations (MNCs) to enhance supply chain resilience?" This question was addressed by two phases:

1.4.1 Qualitative Phase

a) Why information leakage happens?
b) How information leakage could impact information sharing effectiveness?
c) How information leakage can be mitigated?

1.4.2 Quantitative Phase

a) Does intentional leakage impact information sharing effectiveness?
b) Does unintentional leakage impact information sharing effectiveness?
c) Does organizational ethical climate moderate the relationship between intentional leakage and information sharing effectiveness?
d) Does organizational ethical climate moderate the relationship between unintentional leakage and information sharing effectiveness?
e) Does information security culture moderate the relationship between intentional leakage and information sharing effectiveness?
f) Does information security culture moderate the relationship between unintentional leakage and information sharing effectiveness?

g) Does information sharing effectiveness mediate the relationship between information leakage (intentional leakage and unintentional leakage) and supply chain resilience?

1.5 Definition of Key Terms

Table 1.1

Definition of Key Terms

Key Terms	Definition
Information Leakage	The data that is leaked intentionally or unintentionally to an unauthorized party (Anand & Goyal, 2009; CWE, 2008; Sharma & Routroy, 2016; Tan el al., 2016; Zhang et al., 2011).
Intentional Leakage	The confidential information is forced transferred to any unauthorized parties either through verbal or written communication (Huong Tran et al., 2016; Tan et al., 2016).
Unintentional Leakage	The confidential information is accidentally transferred to any unauthorized parties either through verbal or written communication (Tan et al., 2016; Zhang et al, 2012).
Organizational Ethical Climate (OEC)	Shared perceptions of what is ethically correct behavior and how ethical issues should be handled (Parboteeah et al., 2010)
Information Security Culture (ISC)	A way of doing things around the information security, including creation of an environment that fosters and nurtures shared security attitudes, value and beliefs in a given organization (Chen, Ramamurthy, & Wen, 2015)
Information Sharing Effectiveness (ISE)	Two independent members satisfaction with the way of information sharing practise as well as capacity of members on both sides to absorb the shared information. (Majchrzak & Malhotra, 2004)
Supply Chain Resilience (SCR)	The adaptive capability of a supply chain to reduce the probability of facing sudden disturbances, resist the spread of disturbances by maintain control over structures and functions, and recover and respond by immediate and effective reactive plans to transcend the disturbance and restore the supply chain to a robust state of operations (Kamalahmadi & Parast, 2016)

1.6 Significance of Study

1.6.1 Theoretical Contributions

By linking separate concept of information leakage (intentional and unintentional), OEC, ISC, ISE and SCR, this research contributes to the literature in several ways. First, qualitative approach is particularly useful for eliciting in-depth understand the managers' perceptions of information leakage throughout entire supply chain. It also extends few significant contributions to the study by investigating the mitigation approaches of information leakage for achieving ISE.

Second, this study uses a quantitative approach to empirically verify a complex theoretical model of information leakage create a negative impact on ISE. Information leakage is classified into intentional leakage and unintentional leakage that occurred over the supply chain network. While, this study also shed new light on the role of OEC and ISC as moderators on the relationship between information leakage and ISE. These mitigation approaches are new disruptive supply chain strategies for organizations expanding into social aspects will utilize collaboration and integration of supply chain partners. This study highlights that, social aspects become a strategic necessity in the future.

Thirdly, this study provides new insight by demonstrating the significant relationships between ISE and SCR. It is clear that information sharing is prerequisite for building SCR (Kamalahmadi & Parast, 2016), but it remains unclear how ISE will be able to enhance SCR (visibility, velocity and flexibility). Although there has been numerous studies contribute to the body of literature on SCR by developing conceptual models, empirical research by developing theoretical models on the subject still remain scarce.

Lastly, Resource Based view (RBV) is a basis of theoretical model to demonstrate pathways to SCR derived from linkages of information leakage to ISE with mitigation approaches. Supply chain integration and collaboration are mitigation capabilities for reducing the severity of information disruption in order to enhance the resiliency of supply chain network. An extension of RBV is organizational information processing theory (OIPT), this theory defines the concept of the ISC to cope with information leakage and deliver information effectiveness in supply chain collaboration. Another extension of RBV in this study is organizational culture theory (OCT). Organizational culture developed to deal with external attackers and internal offenders by promoting appropriate behaviour. Hence, OEC as a moderating influence on information leakage and ISE.

1.6.2 Practical Implications

The insights provided important practical implications for practitioners, especially MNCs involved in information sharing with supply chain partners. Firstly, the research finding provides a model for better understanding the factors triggering information leakage. In the supply chain collaboration, it is well known that leakage of proprietary information which is particularly difficult to resolve in supply chain. By engaging in information sharing, organizations face constant high impact of information being revealed involuntarily that may disrupt operations in an unwanted and even harmful manner. Thus, it believes that the findings of this research enables organization to assess/control the information leakage which in finding a suitable solution and take corrective actions.

Secondly, the results support the managerial approaches can mitigate the threat of information leakage in order to achieve ISE. Organizations could manage this information disruption by following the recommendations of this research to maintain strong relationship, particularly in supply chain collaboration. This research finding is highlighting the critical role of OEC and ISC to reduce the effect of information leakage. Through OEC, employees are able to utilize many good practices by sharing perceptions of what is appropriate ethical behavior in the day to day operating decision of their organization. Besides, organizations need to take an active role in creating an ISC to protect any confidential information. Organizations should be prepared to develop a series of prevention policy and procedure manual to address information security breaches caused by external attacks and internal offenses. Hence, this theoretical insight is particularly relevant to MNCs, as it offers mitigation approaches to reduce the impact of possible inevitable information leakage across supply chain. These findings should be applicable to more general situation particularly organizations involved in information sharing.

Lastly, the findings can also enable employees within an organization to make a more informed decision in order to maintain the consistency, accuracy and reliability information. ISE is a new guideline for organizations to provide reliable and honest exchange of information and build a trusting partnership within a supply chain. Besides, it is important to implement real-time information transactions across the entire supply chain that is useful for making timely production, inventory management, packaging and logistics management decision. Organizations are able to keep up information is shared effectively and efficiently can improve visibility, velocity and flexibility. Therefore, ISE enables a quick response to disruptions and

increase resilience which might provide a competitive edge over their competitors within a supply chain.

1.7 Scope of the Study

The scope of this study limited to Malaysian MNCs predominantly in the manufacturing sector in one or more foreign countries. Nowadays, more than 5000 companies which include MNCs from over 40 countries have established their operation in Malaysia's manufacturing and related service sectors (CCI France Malaysia, 2017). Based on industry publications and previous expertise determined that MNCs are primarily located in Kuala Lumpur, Malacca, Johor, Penang and the surrounding Klang Valley. These regions are characterized a multitude of FIZs and high concentration of manufacturing and service sectors. This study employed mixed methods research (using both qualitative and quantitative approaches) to collect and analyze data.

The exploratory character of this study dictated a qualitative and multiple case study approach. The study involved Malaysian-based MNCs predominantly in the manufacturing sector. Before proceeding with data collection, all companies selected in this study must meet the following criteria: (i) companies are under list of Multinational Corporations (MNCs) i.e. operating in at least one country other than its home country, (ii) companies have a physical presence in Malaysia, i.e. has facilities and other assets, and (iii) companies must well understand the concept of information leakage. Hence, interviews with manger of company enable too gain deeper insights of mitigation strategies for leakages to achieve ISE within supply chain.