School of Information System

Development of a Multi-Domain RFID Security Model for Global Supply Chains, and a Practical Framework for Model Adoption

Philip Yuk-Fai Lam

This thesis is presented for the Degree of

Doctor of Philosophy

of

Curtin University

Feburary 2020

Declaration

To the best of my knowledge and belief this thesis contains no material previously published by any other person except where due acknowledgment has been made.

This thesis contains no material which has been accepted for the award of any other degree or diploma in any university.

Signature: _____

Date: 15 February 2020

Abstract

This thesis discusses the needs of a model that describes RFID Supply Chain Security and attempts to provide one. The essential idea of this model is to identify and rank all supply chain RFID related security vulnerabilities, so that it could be applied to both academic and business worlds. The research methodology of this model is design science with quantitative methods to build artefacts. Surveys followed by semi-structured interviews were used to build the model.

A byproduct of this model is a robust and easy to use framework that is built by qualitative methods, allowing business practitioners to identify a single solution or prioritize solutions to RFID related supply chain security threats. The framework was then tested in four focus group meetings highlighting the major causes of security threats.

Finally, the members in the focus group verified the usefulness of the framework according to their application to the real world RFID related supply chain security threats, and the results were satisfactory.

To my late father, John, albeit leaving this world twenty years ago,
whose witty inspiration and confidence on me
blessed the eventual completion of my study.

Acknowledgements

I would like to express my sincere gratitude to my supervisor Doctor Paul Alexander for the relentless support of my Ph.D study and related research. His patience, motivation, and immense knowledge in the field are indispensable to the completion of my thesis. He is a tremendous mentor and his advice on both research as well as on my career have been invaluable.

Table of Contents

Table of Figures

List of Acronyms

Acronym	Stands for	Brief Description
3PL	Third Party Logistics	An organization's use of third-party businesses to outsource elements of its distribution, warehousing, and fulfillment services.
AHP	Analytical Hierarchy Process	A structured technique for organizing and analyzing complex decisions, based on mathematics and psychology.
CCTV	Closed Circuit Television	A television system in which video signals are transmitted from one or more cameras by cable to a set of monitors, used especially for security purposes.
CI	Consistency Index	In cladistic analysis, a measure of homoplasy in a phylogenetic tree (or cladogram), calculated as the number of steps (i.e. character state changes) in the cladogram divided by the smallest possible number of steps. The index therefore runs from 0 to 1. A low consistency index (less than 0.5) tends to indicate that much homoplasy has occurred.
CR	Consistency Ratio	Ratio to measure how consistent the judgments have been relative to large samples of purely random judgments.
DoS	Denial of Service	A cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.
DQSA	Drug Quality and Security Act	A law that amended the Federal Food, Drug, and Cosmetic Act to grant the Food and Drug Administration more authority to regulate and monitor the manufacturing of compounded drugs.
EAS	Electronic Article Surveillance	A technological method for preventing shoplifting from retail stores, pilferage of books from libraries or removal of properties from office buildings. Special tags are fixed to merchandise or books.
EDI	Electronic Data Interchange	The electronic interchange of business information using a standardized format; a process which allows one company to send information to another company electronically rather than with paper.
EMI	Electro Magnetic Interference	The interference caused by one electrical or electronic device to another by the electromagnetic fields set up by its operation.
eP	electronic Pedigree	An electronic document that satisfies a pedigree requirement. As a product moves through the supply chain, each company that handles the product must carry forward all of the previous e-pedigree information.
EPC	Electronic Product Code	A universal identifier that gives a unique identity to a specific physical object. This identity is designed to be unique among all physical objects and all categories of physical objects in the world, for all time.
ERP	Enterprise Resource Planning	The ability to deliver an integrated suite of business applications. ERP tools share a common process and data model, covering broad and deep operational end-to-end processes, such as those found in finance, HR, distribution, manufacturing, service and the supply chain.
FDA	Food and Drug Admission	A government agency established in 1906 with the passage of the Federal Food and Drugs Act.
FMCG	Fast moving consumer goods	Products that sell quickly at relatively low cost. These goods are also called consumer packaged goods.
HA	Hacker Attack	The process of an unwanted individual or group gaining access to your computer or network in order to steal or destroy information, often by installing malware.
HE	Human Error	Someone makes a mistake which causes an accident or causes something bad to happen.
HF	High Frequency	A radio frequency between very high frequency and medium frequency.
HRM	Human Resource Management	The strategic approach to the effective management of people in a company or organization such that they help their business gain a competitive advantage. It is designed to maximize employee performance in service of an employer's strategic objectives.
HZMB	Hong Kong-Zhuhai-Macau Bridge	A 55-kilometre (34 mi) bridge–tunnel system consisting of a series of three cable-stayed bridges, an undersea tunnel, and four artificial islands. It is both the longest sea crossing and the longest open-sea fixed link on earth.
IoT	Internet of Things	The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.
IP	intellectual property	Intangible property that is the result of creativity, such as patents, copyrights, etc.
ISECOM	Institute for Security and Open Methodologies	An open, security research community providing original resources, tools, and certifications in the field of security.

ISO	International Standard Organisation	A voluntary organization that gets together to create international safety standards.
LF	Low Frequency	A radio frequency between medium frequency and very low frequency
LFSR	Linear Feedback Shift Registers	A linear-feedback shift register (LFSR) is a shift register whose input bit is a linear function of its previous state. The most commonly used linear function of single bits is exclusive-or (XOR).
LSP	Logistics Services providers	A company that provides management over the flow of goods and materials between points of origin to end-use destination. The provider will often handle shipping, inventory, warehousing, packaging and security functions for shipments.
MCDM	Multi Criteria Decision Making	A discipline in its own right, which deals with decisions involving the choice of a best alternative from several potential candidates in a decision, subject to several criteria or attribute that may be concrete or vague.
MIM	Man-in-the-middle	A form of eavesdropping where communication between two users is monitored and modified by an unauthorized party.
MRP	Materials Requirement Planning	A production planning, scheduling, and inventory control system used to manage manufacturing processes.
OBM	Original Brand Manufacturing	A company that retails their own branded products that are either the entire products or component parts produced by a second company.
ODM	Original Design Manufacturing	A company which designs and manufactures a product which is specified and eventually branded by another firm for sale.
OE	Operating Equipment	An equipment that is operating in the environment, in this thesis refers to all electronic equipments operating in the RFID environment.
OEM	Original Equipment Manufacturing	Traditionally is defined as a company whose goods are used as components in the products of another company, which then sells the finished item to users.
ONS	Object Naming Service	A mechanism that leverages Domain Name System (DNS) to discover information about a product and related services from the Electronic Product Code (EPC).
PKI	Public Key Infrastructure	A set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.
PoD	Point of Dispense Authentication	A place where vaccines, antibiotics, and other medications or supplies can be quickly dispensed to a large number of people.
POS	Point of Sale	The place at which a retail transaction is carried out.
PPRDLH	Pan Pearl River Delta Logistics Hub	The region comprises nine provinces and the Hong Kong and Macao Special Administrative Regions.
PUF	Physically Unclonable Functions	A physical unclonable function (sometimes also called physically unclonable function), or PUF, is a physically-defined "digital fingerprint" that serves as a unique identifier for a semiconductor device such as a microprocessor.
RF	Radio Frequency	A frequency or band of frequencies in the range 104 to 1011 or 1012 Hz, suitable for use in telecommunications.
RFID	Radio Frequency Identification	A system for remotely storing and retrieving data. An RFID tag may be a little sticker that can be attached to an object.
RI	Random Index	A measure of the similarity between two data clusterings.
RO	Read Only	Memory, data, or a file able to be accessed but not modified.
RQs	Research Questions	A research question is an answerable inquiry into a specific concern or issue.
RSJ	Responsible Jewellery Council	A council that helps companies of all sizes, throughout the jewellery supply chain, meet the rising ethical demands of peers, consumers, financial institutions and civil society.
RW	Read-write	A system that is capable of reading existing data and accepting alterations or further input.
SC	Supply Chain	The sequence of processes involved in the production and distribution of a commodity.
SCC	Supply-Chain Council	Supply-Chain Council (SCC) is an independent non-profit organization that helps the supply chain companies.
SCM	supply chain management	The management of the flow of goods and services and includes all processes that transform raw materials into final products.
SCOR	Supply-Chain Operations Reference-model	A management tool used to address, improve, and communicate supply chain management decisions within a company and with suppliers and customers of a company.

SCRV	SC RFID Vulnerability	The quality or state of being exposed to the possibility of being attacked or harmed, either physically or emotionally.
SDLC	System Development Life Cycle	A structured approach to creating and maintaining a system used in information technology. It can be applied to networks and online services, but is most often used in software development.
SKA	Symmetric Key Algorithm	Algorithms for cryptography that use the same cryptographic keys for both encryptions of plaintext and decryptions of ciphertext.
SQL	Structured Query Language	An abbreviation for structured query language, and pronounced either see-kwell or as separate letters. SQL is a standardized query language for requesting information from a database.
SREB	Silk Road Economic Belt	An initiative represents an ambitious Chinese vision to promote infrastructural development and connectivity, and stimulate economic integration across the Eurasian continent.
SSL	Secure Socket Layer	A secure protocol developed for sending information securely over the Internet.
SZSC	Shenzhen-Zhongshan Corridor	A highway that runs between Shenzhen-Zhongshan and expected to open to traffic in 2024.
TDMA	Time Division Multiple Access	A channel access method for shared-medium networks.
TQM	Total Quality Management	A system of management based on the principle that every member of staff must be committed to maintaining high standards of work in every aspect of a company's operations.
UAT	User Acceptance Tests	The last phase of the software testing process.
UHF	Ultra High Frequency	A radio frequency in the range 300 to 3,000 MHz.
UU	Unethical Usage	Usages of things that are not conforming to a high moral standard, morally wrong, not ethical
VHF	Very High Frequency	The range of radio frequency electromagnetic waves (radio waves) from 30 to 300 megahertz (MHz), with corresponding wavelengths of ten meters to one meter.
VMI	Vendor Managed Inventory	Inventory replenishment arrangement whereby the supplier either monitors the customer's inventory with own employees or receives stock information from the customer.
WORM	Write once, read many	A data storage technology mechanism that stores unerasable and/or unmodifiable information after it has been written on a drive.
XRL	Pearl River Delta Express Rail Link	A railway that interchanges passengers at Shenzhen / Humen / Guangzhou, with destination in cities beyond the Pearl River Delta region.

1 Introduction

As early as 2006, Radio Frequency Identification (RFID) has already been identified as a practical technology to transform supply chain management (SCM) (EPC Express, 2006) and drive supply chain (SC) innovations (Abdelkafi and M Pero, 2018). It serves to automate data transfer and integrate logistics operations at a global level, yet at the same time its usage can cause security vulnerability issues along the SC. As the use of RFIDs grows exponentially and globally, security vulnerability issues also grow in scope and scale, with potential major and wide spread implications. So far industry concern and related research on this phenomenon has only been focusing at the technical and device level, instead of broader operational or even legislative levels, where standards and laws are facing a fast growing need to catch up with the industry changes in order to ensure RFIDs are used securely across the entire global SC.

There is an increasing urgency for practitioners to refine best practices and develop new policies to prevent breaches along the SC, from product and package production, through global distribution paths and intermediaries, reaching final consumers, to eventual disposal. The aim of this research is to develop an RFID security model that incorporates both processes and technology, and can be used to help develop better end-to-end security practices. In the following sections, background and context of relevant aspects of this concept are introduced.

1.1 Context and Background

Common uses for RFID technology and systems in SCs include asset monitoring, control and payment. Using RFID allows improvements to commercial operations across the SC, including anti-theft, anti-tampering, anti-counterfeit, product integrity, among other benefits. While applying RFID to SC has management and operational advantages, RFID systems are also highly vulnerable. For example, security issues could arise due to highly automated asset monitoring and control tasks which this technology enables, or the ability to read and write to RFID devices remotely without line of sight (perhaps even from outside secured areas). In some cases, the cost of potential security breaches in SCs could even outweigh its application benefits. A more detailed discussion will follow in section 1.4 below.

1.2 Supply Chains

A formal academic definition of SCs will be given in Section 2.2, and it refers to the operations of how a particular product flows within a company, in other words it includes all materials that flow into, through, and out of a company. SCM commonly incorporates sourcing of materials and fulfilment of products and associated services requests. As uncertainties of business grow, such as volatility of customer orders and varying suppliers' material delivery schedules, SCM also deals with materials or production bottlenecks, in order to ensure smooth and continual

flow of products and services with the original goal and reduce such SC volatility impacts on customers (Ali and Musaka, 2018). Relevant aspects of SCs are considered in detail in Section 2.2.

1.3 Security and Privacy

Merriam-Webster Dictionary (n.d.) defines the term "security" as "the quality or state of being secure from danger, fear or anxiety". RFID systems fundamentally store and serve data, which can be remotely (and often silently) diverted for unauthorized actions. Its security concerns focus primarily on the protection of associated RFID-related assets (RFIDs are diverse and distributed systems), including data stored in RFID readers (units that extract information from the RFID device itself) temporarily or in RFID central databases. More on RFID systems are further explained in section 2.5.1.

Merriam-Webster Dictionary (n.d.) defines the term "privacy" as "freedom from unauthorized intrusion". The word derived from Latin "*privatus"*, which is to be *separated from the rest, deprived of something* (ISECOM, 2010), and can be seen as a basic need of most people (Introna, 1997). Privacy is also an important part of RFID systems. Intuitively, privacy seems to be a primitive concept. Fulfilling such needs has led to the fundamental requirement in the social and commercial worlds that information about an individual can only be obtained with his/her own permission. In today's society, due to technology advancement, privacy issue is becoming more complicated. Information is stored in various databases connected to the Internet, how to use or share them depends on the organization that maintains these databases. As a result, privacy concerns have been a popular topic for researchers, aiming to understand it, and to develop standards and other protections. Examples of such include privacy and freedom (Westin and Ruebhausen, 1967), privacy protecting models (Sweeney, 2002), privacy and morality (Parent, 2017), importance of privacy (Rachels, 2017), rights in personal information (Murphy, 2017), and other similar topics from many other scholars. Privacy is in fact broader than security in definition and includes the concept of appropriate usage and protection of information (Tsai et al., 2011).

Data security and privacy (and their interaction) have been widely investigated over the past 30 years. Hence varied research directions appear on challenges arise from increasing privacy concerns due to the increase in the amount of data collected, and the growing importance of reconciling privacy and the use of data. Petronio (2001), agreeing with Warren & Laslett (1977), with an original idea developed by Westin (1967), suggested privacy involves the control of transaction, and that its goal is to standardize access to information about us and our activities, space, and possessions. It applies to individuals, groups of people, and organizations/institutions. Modern principles of privacy now also address data analytics and

security of huge amounts of data collected by the use of technologies such as Internet of Things (IoT), social networks, cloud computing (Bertino and Ferrari, 2018).

There are also potential new areas targeting the emerging new data collection and processing devices, such as those used in IoT systems, increasing the range (and the importance) of exploring new research directions. For example, Zalud (2016) reported that in one of the largest known data breaches due to privacy in SCs, a hacker attacked a supplier of Target's supply network, which has invaded the privacy of 110 million computer records[1]. This has resulted in a damage of hundreds of millions dollars.

1.4 Costs of Security Breaches in Supply Chains

Few organizations have highlighted the global cost of security breaches[2] in SCs, but Holste (2013), citing the United States Department of Commerce, noted that the occurrence of security related issues is increasing globally, and among various such issues, for just "employee theft" item alone, is costing companies in the United States more than US$ 40 billion a year.

A significant part of the overall SC is the logistics (i.e. transport and storage) component, in terms of activities, costs and focus. This is the most common part targeted by organized crime groups as reported by various authors.[3] A total value of US$ 89.5 million was stolen in cargo theft incidents in 2014, a huge increase from average value of 42 million in 2013[4]. Brandman (2015) summarized this situation and alerted that there is an average logistics lost for over "hundreds of millions of dollars" annually, with loses from employee-related thefts exceeding US$ 10 billion each year.

In 2015, there were 794 cargo thefts recorded by Freight Watch International throughout the United States. On average, there are 66 cargo thefts per month, or 2.2 per day (Kilcarr, 2015). Holste (2011) alerted that vulnerabilities in the SC not only lead to loses of individual company in monetary sense, but these can also threaten the SC security of the entire country.

---

[1] On December 11 2013, Target, the second-largest discount store retailer in the United States had 40 million credit and debit cards of shoppers who visited its stores during the first three weeks of the holiday season 2013 stolen by hacker. This mark the largest amount of data stolen in history, and accounted 1/3 of all Americans.

[2] For example, IBM reported breach in 2018 is $3.86 million from 13th annual Cost of a Data Breach study, source: https://www.ibm.com/security/data-breach, last accessed: 27 September 2018.

[3] Source: Home Office, Government of United Kingdom, source: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/611752/crime-against-businesses-factsheet-transportation-storage-2016.pdf

[4] Reported by Cargo Net (2016) "Cargo Theft Declines in 2014, Average Value Increases, 2015"

Year	Criteria	Value of Loss	Researcher
2014	Logistics Loss	89.5 million cargoes	Cargo Net (2016)
2014	Employee Theft	US$ 10 billion	Brandman (2015)
2014	Logistics Loss	“hundreds of millions of dollars”	Brandman (2015)
2013	Electronics Loss in SC	42 million	Cargo Net (2014)
2014	Electronics Loss in SC	54 million	Cargo Net (2014)
2011	Global SC Loss	> US$ 40 billion a year	Holste (2011)

Table 1 Estimated Value of Global SC Loss with Loss Criteria

A well-coordinated and effective effort to protect the industry is therefore required. Although there is not any study that can clearly identify the loss of global SC, the researchers do give a good direction of an estimated impact that reflects the importance of the loss. Such large thefts place a significant impairment on global trade.

RFID is a valuable in addressing these attacks, but as a front line tool it is also a priority target for the attackers. Security imperatives have been recognized from the early stage in RFID’s development. Data within RFID systems has to be protected from unauthorized access of intruders, and systems should also be constrained from any unauthorized actions, even as simple as registering their presence in particular locations at particular times, as this would trigger privacy intrusion. Privacy is an issue because RFIDs contain data that can provide secondary location information, which links products and people to times, places, and events, and can be used to assert other interactions.

1.5 Sources of Vulnerability

Vulnerability, in terms of computing technology, is a weakness, which allows an attacker to reduce a system's information assurance. The United States Department of Defense (2010) defines vulnerability as “the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw”. In RFID systems, as air is used as the medium of data transfer, the above three elements are harder to detect because it is easier to eavesdrop and tamper with radio frequency signals in the air than intercepting wired data transfer.

1.6 Privacy of RFIDs

From 2005 to 2010, this privacy issue has been a major focus being examined by many scholars. For example, a conceptual “RFID Guardian” device was introduced by Rieback, Crispo, and Tanenbaum (2005), which enables the user to scan RFIDs and provide a mechanism to destroy the transponder (Components of the RFID system are further defined and diagrammed in Figure 3). Other scholars stress on consumer education. These two solutions require additional actions to be taken on the consumer side (Ohkubo, Suzuki, and Kinoshita, 2005). Other published papers suggest obtaining consumer’s approval in data

collection: requiring that data generated from RFID transponders can only be accessed by those with licenses (Cha, 2010), and creating applications to limit RFID data that can be released to authenticated information users (Chen et al., 2018). Cryptographic solutions such as hash functions, private-key algorithms, public-key algorithms and various authentication methods have also been incorporated into Electronic Product Code (EPC)[5] and International Standard Organisation (ISO) systems. Such measures have not focused on consumer side actions to stop transponders from continuing to be read (Lee, Batina, and Verbauwhede, 2010). These aspects will be addressed in Section 2.9.

Privacy in RFID systems can be placed into two major categories, downstream SC actions from product's ultimate consumer side or upstream from the product supplier side. For example, a device to destroy product's RFID permanently or consumer approvals of data collection can be considered as downstream SC actions. Downstream systems protect consumer information from being associated with the RFID that is being consumed. For example, a consumer of certain cosmetic product, say a facial day cream, can be targeted for further upsell of a related product, say a night cream. This would compromise the privacy of the consumer. On the other hand, encryption based solutions to prevent RFID systems' data from being unintentionally read can be considered as upstream protection systems. For example, reading of all products' quantities being sold in a supermarket each day could lead to competitors' intrusive actions, say a nearby convenience store may be able to sell related products that are missing from that supermarket. By providing more comprehensive and related products to the consumers, the convenience store could become a one-stop shop that might eventually gain business from its competing neighbour. These data peeking actions would intrude the privacy of suppliers, such as the supermarket in this case.

1.7 Possible Attack Vectors of RFID systems

RFID systems refer to the system with RFID as a component and are enabled by RFIDs (discussed in section 2.5). If the RFID systems associated assets are valuable, then the RFID systems can be an attack vector[6] that exploits system vulnerabilities. Data being unintentionally read from RFID is just one example of privacy being invaded and security systems being tempered by this attack vector. Vulnerability of RFID systems can further be categorized as eavesdropping, relay attacks, unauthorized tag reading, tag cloning, people

[5] Electronic Product Code, abbreviated by EPC is a universal identifier that provides a unique identity for every physical object anywhere in the world

[6] An attack vector is a path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload or malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities, including the human element. Definition from WhatIs.com, last accessed 23 Nov., 2019, source: https://searchsecurity.techtarget.com/definition/attack-vector

tracking, replay attack, tag content changes, malware, RFID system breakdown, tag destruction, blocking, jamming and back-end attacks. The list of possible attack vectors was first identified by Peris-Lopez in 2006, and later categorized by Rotter in 2008. This list represents a super-set of those that are relevant for study of RFID vulnerability in SCs. However, these attack vectors could also be shortlisted, as a starting point for identifying a list of security vulnerability through the SC. Researches on all these attack vectors should be further studied and occurrence (i.e. case studies) should be examined. This is considered in detail in Section 2.6.

1.8 Security Vulnerability of RFID through the Supply Chain

Based on the study of Rotter (2008) in relation to security vulnerability of RFIDs as they apply to SCs, an attempt was made by Lehtonen (2008) to identify security likelihood to exploit RFIDs threats, as presented in Table 2. However, the study focused too much on one single RFID standard, the EPC.

RFID Security Vulnerability	Likelihood
Tag cloning	Higher
Tag removal and reapplying	
Attack against internal IT system	↕
Manipulation of product data	
Manipulation of testing equipment	Lower
Attack against RF communication	

Table 2 RFID security likelihood to exploit RFID threats described by Lehtonen (2008)

Likelihood of security threats being exploit is important, as financially justified prevention should be in place for these security attack vectors. Security requirements have to be well implemented in all industrial or closed application of RFID, and in public application that connects with money and material (Finkenzeller, 2003). While the likelihood of these RFID attack vectors is ranked in the use of EPC, other RFID technologies could result in a different list, and these are missing from Lehtonen's (2008) study. For example, the EPC requires middleware systems to further access RFID information that are stored in remote servers, but offline reading can be performed with information gained from previous RFID reads, tag cloning can be easily achieved in between middleware connections as no real time updates are provided. However, for other real time RFID systems, tag cloning could easily be detected since multiple reads in different locations are reported immediately after read. In addition to general RFID security concerns, RFID security was also examined focusing on EPC tags in multi-domain systems (Kim et al., 2007). Multi-domain systems are defined as systems that include SC partners (domain A) interacting with the tag owner's system (domain B).

1.9 Research on Integrated Supply Chain RFIDs Security

Previous academic studies on RFID security have primarily been single angle focused. Literature review shows that many studies focus on any of these three angles: technological

approach such as hardware or software, user management such as training, or forecasting model such as quantitative modelling. There were some academic studies on RFID security based on two or more angles, but they do not cover the entire SC. For example, Kim et al. (2007) has a multi-domain system for RFID tags but is too convinced to EPCGlobal tags (further discussed in section 2.7.8).

1.9.1 Pan Pearl River Delta Logistics Hub and its Importance to Global Supply

In this study the author focuses on one of the world's most active centres of global supply, the "Pan Pearl River Delta Logistics Hub" (PPRDLH), which is located in the Guangdong Province of China. To understand the extent of SC activity, the potential for security breaches and the impact of these on global SCs, it is useful to give a more in-depth study of this region and its SC activities.

Guangdong Province is the southern coastal gateway into China, and PPRDLH is considered a pioneer in China's reform. To attract foreign direct investment and move towards a more market oriented economy, Shenzhen, Zhuhai, Shantou and Xiamen were designated as special economic zones by the Chinese government in 1980 (Li, 2009). With a surface area of 41,698 square kilometres and a population of 40 million, the economic importance of PPRDLH started to grow in the 1980s, when the area began to transform from an agriculturally based economy to a manufacturing based one. The highest growth in the area was between 1980 and 2000, in which the GDP of PPRDLH region has grown an average of 17 percent per year (Li, 2012). The PPRDLH accounts for 35 to 40 percent of China's foreign trade, with a total exports amount to US$ 84 billion in 2000. In the following decade (2000-2010) the area has a stabilized growth and had a significant role to play in the world's manufacturing arena – this huge manufacturing giant affects the life of nearly all individuals in the world, as in 2004 the area had accounted for more than 70 percent of all the made-in-China goods sold in Wal-Mart (Jiang, 2004). All these products moved out of this region and played a vital role in global SC. Until 2009, it had reached the record-high economic output of over RMB 3 trillion in the year in spite of the global economic crisis (China Knowledge, 2010). This RMB 3 trillion occupies 33.8 percent of the total export volume in China, with light industry capturing export value of RMB 93.7 billion. After the crisis, the area still has an average yearly 8.3% growth recorded in 2016, representing 9.1% of China's GDP and 26.9% of China's total export[7]. From the above figures, the area of PPRDLH represents 30% of China's total export in the past three decades.

---

[7] Hong Kong Trade Development Council Research, http://china-trade-research.hktdc.com/business-news/article/Facts-and-Figures/PRD-Economic-Profile/ff/en/1/1X000000/1X06BW84.htm, last accessed 27 September 2018

A typical SC model in PPRDLH is the Build-to-Order model, which means PPRDLH manufacturers begin manufacturing the customer's order almost immediately upon receipt of the order, enabled by having component manufacturers widely available in the PPRDLH areas. Inventory reduction[8] is benefited from this type of SC. However, the supply of components requires just-in-time[9] manufacturing which results on a relatively more complex SC.

Looking into the future, PPRDLH will continue to be pivotal in the global trade arena. According to the latest Five-Year Plan[10] (13th, covering 2016–2020) of China, the main plan for the region is innovation-driven and efficiency in terms of production inputs such as labour, capital, land, technology and management (Section III). It is an intention in this plan to include the Yangtze River Delta in addition to the PPRDLH (Brødsgaard 2016).

The Mainland Chinese government realizes that China would need to improve in research and development as well as innovation, and therefore groups of national key scientific and technological programmes are given strong support. The goal is to break into the development of core technologies in fields such as "next-generation information communications, new energy, new material, aerospace, biology, medicine, and intelligent manufacturing" (Xinhua 2015c: 7). China Briefing News (2018) expected that according to the plan, one of the initiative developments is to transform the region from "The factory of the world" to become and innovation and services dynamic hub, with an estimated GDP of US$ 4.62 trillion by 2030.

One of the major Chinese economic development strategies is the "One Belt, One Road" initiative. The strategy is to connect Europe, Asia, Africa and Oceania nations just like the land-based Silk Road Economic Belt (SREB) and the ocean-going Maritime Silk Road in the 20th century. This will help open up new international pathways between China and the countries to its South and West, which could greatly promote the flows of materials and information, plus business cooperation.

Logistics development is also an important national strategy in China. It acts as an important way to build logistics capabilities, and to develop the two-way international logistics system (Liu 2016). To achieve this goal, massive infrastructure projects impacting the Pearl River Delta are rolling out.

---

8 Reducing inventory gives benefits such as reduce material maintenance (carrying cost) and capital cost.

9 "Just-in-time" system is an inventory management strategy that aligns raw-material orders from suppliers directly with production schedules. In theory, 100% just-in-time system requires timing and quality of products delivery has to be 100% correct which constitute a more complex supply chain.

10 Five Year Plans of China: Social and economic development initiatives shaped by the Communist Party of China through the plenary sessions of the Central Committee and national congresses.

These infrastructure projects include the Hong Kong-Zhuhai-Macau Bridge (HZMB), the Pearl River Delta Express Rail Link (XRL), and Shenzhen-Zhongshan Corridor (SZSC). The opening of HZMB in 2018 has reduced the travel time between Hong Kong, Zhuhai and Macau. And it does not just link up Hong Kong to Zhuhai by land transport, but also the land distance with Zhongshan and Jiangmen (both are neighbours to Zhuhai) is greatly shortened, increasing competitive advantages and efficiencies in cargo handling. In terms of logistics, the bridge is able to geographically turn the two previously dead ends (Hong Kong and Macau) into an open loop. Together with the newly operational XRL , which links Hong Kong to Shenzhen and Guangdong, and SZSC that links up Shenzhen-Zhongshan, transport time for factories in PPRDLH will be significantly reduced by the resulting eight-lane highway (China Briefing News, 2018).

1.9.2 PPRDLH Hub and its Role in the RFID Lifecycle

An RFID system (defined in 2.5.1) for products manufactured in the PPRDLH has a typical life cycle starting from tagging in raw materials, sending to the supplier and manufacturing factories. Depending on the stages required by individual products, work-in-progress goods could be transferred from one factory to another, and this process could repeat a few times. Afterwards, finished goods would go through distribution channels via various mode of transportation: air, sea, and land to the customer's side. The customer could be importers, wholesalers, distributors, or retail shops depending on the sales details. Finally, the goods are handed to the consumer and the RFID tag could be disposed by the consumer. This is illustrated in Figure 1. There is a definite start to end of the RFID usage, and this study introduces a lifecycle concept of the RFID (will be discussed in section 2.5.3).

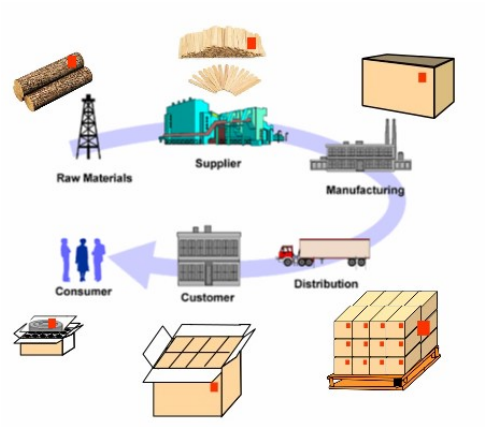


Figure 1 Possible life cycle of RFID used in SCM.

The inner circle is a commonly used figure to illustrate the multi-domains in supply chain, adapted from http://www.theprogressgroup.com/publications/wp_images/fite1.gif, accessed 14th Jan., 2018. The outer circle added is typical product handled in various supply chain domains, with the red square indicating locations of RFID tags that can be attached.

1.9.3 The PPRDLH Production Structure and its impact on RFIDs

The PPRDLH manufacturing structure is shifting from Original Equipment Manufacturing (OEM)[11] to Original Design Manufacturing (ODM)[12] and even towards Original Brand Manufacturing (OBM)[13] (Wonglimpiyarat, 2018). The major reason for this shift is that OBM firms are more profitable; gross margin for OEM products is 19% on average, while the margin for OBM goods is 27%. This implies that there will be more finished goods made in PPRDLH than semi-finished[14] products. RFID tags applied in PPRDLH to finished and semi-finished goods therefore travel with the products all the way from manufacturing source down the SC, to the final consumer's hands.

Not only consumer products are tagged with RFIDs, industry practitioners like Walmart and United States Department of Defense are also mandating RFIDs tagging from product manufactures (Nair and Anbuudayasankar, 2018). As components are made to be as modular as possible to standardize and shift work upstream in the SC, some of these modules and components are now tagged with RFIDs before shipping to downstream processors and manufacturers. This type of modularization of components can bring SC benefits such as inventory reduction, achieved by postponement strategies, or reducing production rework (Chung et al., 2018).

Including components and finished products, the volume and percentage of China's top 10 exports published from PRC General Administration of Customs, China's Customs Statistics are listed in Table 3. This table describes clearly products exported from China. Raw materials do not normally require RFID tags, and so the top three RFID-requiring products, accounting for over 70% of all products produced, would be in the order of (1) Electronic Machinery and Equipment, (2) Power Generator Equipment, and (3) Apparel.

With over US$ 600 billion transaction amounts for just the top three export commodities (i.e. Electronic Machinery and Equipment US$ 301.1 billion, Power Generator Equipment US$ 236.0 billion, and Apparel US$ 100.5 billion), the amount is lucrative enough to attract

---

[11] Original Equipment Manufacturing (OEM): A company that manufactures products to be sold under another a brand name owner

[12] Original Design Manufacturing (ODM): A company that designs and manufactures products to be sold under another a brand name owner

[13] Original Brand Manufacturing (OBM): A company that sell goods under own brand name, apart from design and manufacturing, the company may be responsible for other operations including supply chain, delivery and marketing.

[14] Semi-finished goods, or intermediate goods, or producer goods - A product that has not been completely assembled or manufactured

intruders to plan for illegal RFID attacks. Apart from the top three, Table 3 below lists other Chinese export commodities that constitute the remaining of the top export list, which are also subject to security breaches.

Commodity Description	**Volume**	**Percentage**
Electronic Machinery and Equipment	301.1	34.25%
Power Generator Equipment	236.0	26.85%
Apparel	100.5	11.43%
Iron and Steel	47.3	5.38%
Furniture	38.9	4.43%
Optics and Medical Equipment	38.9	4.43%
Inorganic and Organic Chemicals	32.0	3.64%
Ship and Boats	28.4	3.23%
Footwear	28.0	3.19%
Vehicles, excluding Railways	27.9	3.17%
Total	879.0	100.00%

Table 3 China's Top Export 2009 (US$ billion)

Source: PRC General Administration of Customs, China's Customs Statistics

In terms of destinations of PRD-sourced products, Workman (2018) reported the top 15 countries totalled to only 67.9% (note that from Section 1.9.1, the PPRDLH provides 30% of all of China′s export in the past three decades). Of course one can argue that the destinations were not final, as transhipment[15] hubs like Hong Kong were counted as direct shipment from Chinese Mainland, or due to political reasons where Chinese Mainland were not allowed to ship directly to places like Taiwan. However, it is clear from the study that export from Chinese Mainland is global, that it has been growing and becoming more diversified. Table 4 lists the destinations of goods exported from Chinese Mainland in 2009 and 2017.

[15] Transshipment is the shipment of goods or containers to an intermediate destination, before another (final) destination.

Destination	Volume	2009 %	2017 Rank	Volume	2017 %
United States	220.8	29.96%	1	431.7	19%
Hong Kong	166.2	22.55%	2	281	12.4%
Japan	97.9	13.29%	3	137.4	6.0%
South Korea	53.7	7.29%	4	102.8	4.5%
Germany	49.9	6.77%	6	71.2	3.1%
The Netherlands	36.7	4.98%	8	67.3	3.0%
England	31.3	4.25%	9	57	2.5%
Singapore	30.1	4.08%	10	45.7	2.0%
India	29.7	4.03%	7	67.9	3.0%
Australia	20.6	2.80%	14	41.6	1.8%
Vietnam			5	72.1	3.2%
Taiwan			11	43.9	1.9%
Russia			12	43.1	1.8%
Malaysia			13	42	1.8%
Thailand			15	38.8	1.7%
Total	736.9	100.00 %		1543.5	67.9%

Table 4 China's Top Export Destination 2009 (US$ billion)

Source: PRC General Administration of Customs, China's Customs Statistics and Workman (2018)

In addition to direct contribution, indirect contribution is also a vital consideration in this study. Imagine what would happen if an RFID container seal (A secondary electronic seal that is resealable complimenting the primary metal seal that is not resealable, with the ability to record time and place of being unsealed) has been broken and the goods inside have been substituted to weapons for terrorist attack. Indeed, SC security has been a top concern of national security of many countries after the incident of 911 attacks. 100% air freight container screen, and advanced shipping information supplied for customs to provide pre-clearances are required to enhance SC security, and RFID has been identified as a major SC security driver (Richardson, 2017). Blackstone et al. (2014) reviewed health and economic consequences of counterfeit drugs have on the United States public and its healthcare system, and highlighted that counterfeit drugs is the direct cause of an annual loss of US$ 200 billion and losing more than 750,000 jobs in the country. The study further recognized that public health hazard, consumer income wastage, and incentive of research and development reduction being the top three indirect contributions. To apply the same concept in the Chinese environment, the impact of PPRDLH contribution is higher than just the direct contribution of goods moving, but also includes other indirect contributions too.

1.9.4 Supply Chain Performance

The performance of SCs is of intense interest to the SCM discipline, and affects the quality and SC cost bases. SC Performance refers to the SC's activities in meeting consumer requirements (Kluwer, 2004). A high performing SC directly reduces the cost of business, which can be up to 75% of the product's final cost to consumer. The largest buying office in the world, Li & Fung, addressed SC performance as "tackling the soft $3" in the cost structure (The Economist, 2001). Li & Fung estimates a typical consumer product leaves the factory at price of $1 and ends up on the retail shelves at $4. Instead of tackling the $1 from production, Li & Fung tackles costs spread throughout the SC, which includes product design, procurement, logistics, wholesale and information collection. The $3 spread is coined by the term "soft 3 dollars" by the company, and directly influence the landed cost[16] of the product. Measuring performance includes controlling SCM effectiveness and efficiency as the SC is complex in nature.

The dominant full-scale SC performance model over the past 30 years is the Supply-Chain Operations Reference-model (SCOR). SCOR is a process reference model developed by the management consulting firm PRTM and the only model that is adapted and endorsed by the Supply-Chain Council (SCC) as a standard diagnostic tool for SCM (SCC, 2003). The model recognises the most important features of a SC as three "pillars". "Process Modelling" pillar describes SCs based on six distinct management processes, including plan, source, make, deliver, return, and enable. "Performance Measurements" pillar attempts to measure SC performances by over 150 key performance indicators. "Best Practices" pillar consists of performances of companies who have been measured by the performance measurements pillar, for SCOR model users to identify operations that can close the gaps between their performances and best practice companies.

SCOR is further explained based on five distinct management processes, namely "Plan", "Source", "Make", "Deliver", and "Return". "Plan", being the first process, has the ability to balance aggregate demand and supply in developing a solution that meets sourcing, production, and delivery requirements. "Source" is the second process in the chain where procured goods and services will meet planned or actual demand. "Make" being the third process that would transform raw product to a finished state to meet planned or actual demand. "Deliver" on the other hand would deliver the finished goods and services to meet planned or actual demand. The final process "Return", finally yet importantly, is a process associated with returning or receiving returned products for any reason. The model of SCOR is illustrated in the below diagram.

---

[16] Landed cost is the total price of a product arriving at the buyer's facility. It includes fees such as the price of the product, transportation, customs, duties, taxes, tariffs, insurance, currency conversion, crating, and handling.

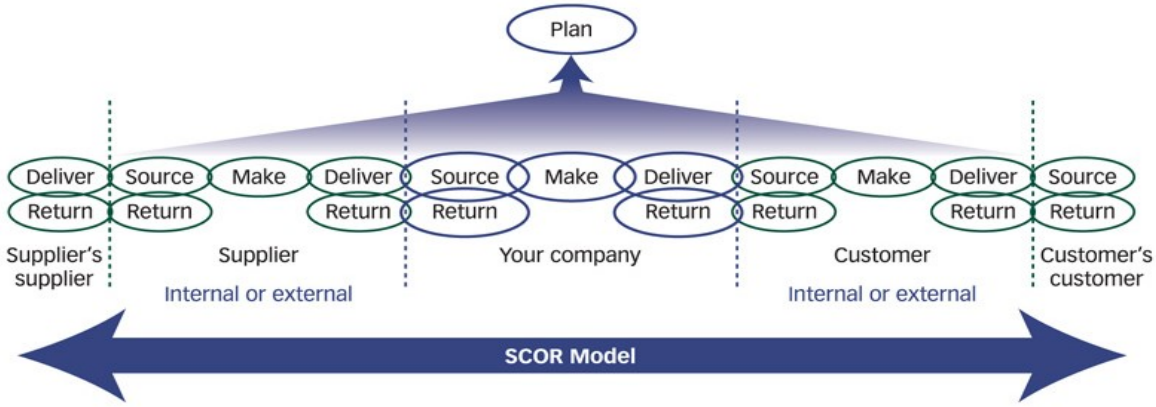


Figure 2 Current Scope of SCOR Model, adopted from Supply Chain Council: SCOR 9.0 Overview Booklet, 2008.

The SCOR model as illustrated in Figure 2 has been used as a common language for SC partners to communicate, while providing standard and points to note when evaluating supply chain members. This study will adapt this idea and aim to provide points to evaluate for security breaches for RFID in SCM. The management tool starts from the supplier's supplier and the customer's customer, and so as this study: to focus with that spectrum for an RFID to present in a supply chain. This study will further suggest a lifecycle of RFID, which will be discussed in section 2.5.3.

1.10 Retailing and Global Supply Chains

SCs start with manufacturing, through various domains, to effect final distribution to end consumers, and retailers have become very dominant in controlling SCM activities and structures upstream of them. This is a major change from the time when manufacturers made to stock and retailers were much more passive in the supply process.

SC should be managed as a whole, with products manufactured and then shipped to retailers to sell. Simchi-Levi et al. (1999) explained that "pull logistics" for demand replenishment is based on consumer demand, and this is serviced and indeed driven by retailers, who consequently take an active role in SCM. Abernathy et al. (2000) supported this theory through noting that point-of-sales information, shared with suppliers, puts control in the retailers' hands and drives order replenishment based on actual sales. Manufacturers therefore adjust planning methods, cost models, inventory practices, production operations, and sourcing strategies to fit the demand; they become the passive (reactive) members of the SC (Sorensen, 2016). Global SCs can therefore be envisaged as being driven by retailers even though they are at the end of the SC. The effect of this is that in order to meet their needs, retailers tend to deal with companies in other countries that are part of the SC, instead of dealing with the local importer of the goods, and such dealing requires involvement in politics, trade and tariff laws, quality control, and international relationships. The difficulties in these long distance trade dealings

have encouraged the use of information technology in the SC, which standardises and effects ready transfer of information (Hugos, 2018).

The increasingly powerful and prevailing of eCommerce changed and further complicated the retailing environment. Otto and Chung (2000) suggested a framework for cyber-enhanced retailing combined with brick-and-mortar (traditional) retailing. Ngyuen et al. (2018) recognized eCommerce as a vital driver of the growth of the global SC, and that this results in having the end consumers themselves driving transactions, with retailers controlling that process. The manufacturer will have to be dealing with the consumers directly in addition to the retailers. The use of RFID can help in facilitating information sharing in the SC, and automate certain processes. For example, Muzellec and O'Raghallaigh (2018) studied the use of mobile computing systems in consumer decision-making in the SC. Mobile computing systems with the ability to detect RFIDs improve quality of information involved in buying decisions, increasing the interactivity of the retailing environment.

1.11 The Pharmaceutical and Jewellery Industry Supply Chain

Lee and Whang (1999) defined SCs where products pass through multiple sites located in series, before reaching customers, to be multi echelon SCs[17]. The pharmaceutical and jewellery SCs are both multi echelon SCs. This type of SCs involves individual companies serving multiple customers and having multiple vendors. They are generally more complex than SCs with companies that serve single vendor or supplier. Many SCs are represented by the multi echelon SC, particularly those with a global reach. Authors have studied the complexity of this SC design, for example Tsiakis et al. (2001) saw it as a complex network under demand uncertainty; Chen and Lee (2004) optimized complex SC situations; Schmitt and Singh (2012) performed quantitative analysis on complex variables during supply disruption; Laumanns and Woerner (2017) used a quantitative model to estimate prices in complex multiple sourcing and dynamic inventory allocations scenario; Yu et al. (2018) established complex negotiation model.

1.11.1 The Jewellery Supply Chain

Jewellery SC, partly because of the high unit value of its products, potentially represents an extreme example of multi echelon SCs. A final jewellery product that sells to end users is the result of a complex and fragmented SC process. In order to enjoy economies of scale, the jewellery retail industry participates in global sourcing of raw materials (precious and other materials) for manufacturing the products. Their value is often reflected in their rarity and limited geographical source. This however serves to increase the SC complexity more than

[17] Supply chains having multiple inputs and outputs.

many other manufactured products, where sourcing can be aligned with other parts of the SC (Ganesan et al. 2009).

Raw materials for the manufacture of jewellery items can only be sourced in major diamond manufacturing countries such as Botswana, Namibia, and Mauritius (Palumbo, 2015). Jewellery brands deal directly with mine operators with prearranged agreements to source rough stones. The SC is also complex, just the manufacturing steps include marking – specifying the cut and shape, bruiting – cutting the stones to round shape, cutting – cutting the stones to final shape, polishing – smoothing the stone, and quality assuring – distinguishing features of the stone such as weight, quality, clarity, and colour. These steps are likely to be performed by different companies and therefore semi-finished goods already involved few logistics operations.

After the manufacturing step, 90% of the world's diamonds are shipped to Antwerp of Belgium, the world-renowned diamond capital of the world (Palumbo, 2015). Jewellery industry has a tightly controlled shipping process as import or export of diamonds involve only officially sealed packages. This is done not only to protect the diamonds against theft, but also to avoid trading or trafficking diamonds mined in war zones (called conflict or blood diamonds). Buyers of diamonds are ensured their purchase did not contribute to aggression around the globe, nor financing any rebellion movements.

Comunian and England (2017) pointed out that the jewellery industry is transforming from industrial production into creative cluster industries. By providing unique techniques, creativity and knowledge in making jewellery, brand cluster retailers are setting up stores all around the world. Brands are becoming more internationalized and are expected to expand the market share of the jewellery industry extensively in the future. Dauriz et al., (2014) further expected there is likely to be a raise to 30% to 40% by 2020 of internationalized brands with more complex and longer SCs. These are done by replacing less internationalised brands (only 10 percent of jewellery brands in 2003), which feature simpler and shorter SCs.

The design of jewellery provides competitive advantage for companies in the jewellery industry, and the speed for designers to turn their conceptual ideas to products is the area of competition. Hashim et al. (2018) asserted this value creation is also integrated with customer experience, not only between the designer and retailer, but also to capture individual needs and enhance customer satisfaction. Suneetha and Megharaj (2016) believed that jewellery retailers should provide high value delivery to customers despite affecting profitability. For instance, value adding delivery actions such as gathering post-purchase feedback immediately to improve product development allows jewellery brands to stay on trend. Of course, jewellery is generally a high value product, and SCs emphasise (in that environment) reduction of lead time

to avoid over-stocking of inventory and reduction of carrying cost. Again, information systems, particularly RFID, can play a vital role in this aspect.

eCommerce marketing has changed the pattern of jewellery industry operations in the past decade; business to customer transactions are formed between retailer and end customer (Centobelli et al., 2016). Jewellery products are not limited to offline purchases but also available for online purchase. As a result, they are becoming integrated into the daily life of end customers. Customers can design and purchase jewellery online, whereas custom made jewellery was previously limited to luxury sector in the past. Traditional marketing and planning strategy of jewellery industry will likely change to an integrated market, as the SC for jewellery becomes more and more connected due to eCommerce.

The jewellery industry is vulnerable based on its shipped value to volume/weight ratio, which is as the highest of all products (FedEx Declared Value Advantage, 2018), to the extend of US$ 100,000 per shipment on jewellery versus the standard maximum declared value of US$ 1,000. In addition to the outright value transiting through the SC, jewellery is small and relatively easily pilfered.

1.11.2 The Pharmaceutical Supply Chain

Pharmaceutical SC represents a channel to deliver essential drugs to end-users at right time to right place with right quality and quantity (Enyinda and Tolliver, 2009). The SC involves the planning and execution of the entire pharmaceutical logistics functions. These functions include traditional SC functions such as transportation, warehouse, inventory management, and other functions with main goals to ensure continuous drug flow to patients at the lowest price, with the shortest delay time, low rate of shortage, and error in fulfilment (HDMA, 2009). Besides, the delivery time is one of the main concerns for the distribution logistics of the pharmaceutical industry. The timely supply of drugs helps to meet the growing demand and prevent basic medicines and consumer healthcare products from running out of stock.

The pharmaceutical SC operates in a mainly critical environment, as it is extremely time sensitive. This phenomenon has introduced complexity and quality controls as basic features of pharmaceutical SC. The complex hierarchy in the pharmaceutical SC can be demonstrated in biotechnology industries; intra business transactions in pharmaceutical manufacturing and distribution environment are common and they also interact with healthcare industry. The interaction between the industries includes a variety of processes across the upstream and downstream in the pharmaceutical SC. Narayana et al. (2014) claimed every single company in the pharmaceutical SC can have severe impact to the final delivering value , and suggested better communication can allow better management of the overall pharmaceutical SC.

In addition to traditional SC functions, reverse logistics is also an uprising issue in pharmaceutical SC (Kumar, Dieveney, and Dieveney, 2009). The potential serious consequences of using expired or ineffective drugs are an important issue in the pharmaceutical SC. It is critical for pharmaceutical companies to equip with reverse logistics functionality right from the start of SC planning stage. Companies must respond quickly to problems and clean up the SC of substandard materials, therefore appropriate supplies can be reissued to the patients who are using the product.

Pardal et al. (2013) and Narayana et al. (2014) both observed the rise of illegitimate or counterfeit products in pharmaceutical markets and the need for increased awareness of the importance of SC security across the SC. As a means of addressing this, for pharmaceutical SCs most European Union countries are adopting Point of Dispense Authentication (PoD). In the United States of America, the electronic Pedigree (eP) is used to trace the chain of ownership of these products. However, since about 2010, due to data visibility and confidentiality, it has become more popular to use RFID to ensure integrity (Pardal et al., 2013). With easier tracking and tracing of information in RFID systems, pharmaceutical products can be protected and stored with built in RFID tags with temperature sensors (Pardal et al., 2013). To maintain quality of the pharmaceutical products, many require a stable temperature during transportation of the goods and storage throughout the SC. These sensors also lead to integrity in the "cold chain"[18] (Kumru et al. (2014). Kartoglu and Milstien (2014) both emphasised the importance of cold chain for vaccines.

There is a rising trend in cold chain services globally, but particularly in the pharmaceutical industry, in which RFIDs can work alongside other cold chain technologies to determine the temperature of the product to be transported or stored. According to Pharmaceutical Commerce (2017), the growth of temperature-controlled products is still more than twice of non-temperature-controlled products. In 2017, non-cold-chain pharmaceutical logistics' costs rose from 4-5% to US$ 66.5 billion, and cold-chain logistics grew 10.7%. Cold-chain logistics will become US$ 16.6 billion and non-cold chain US$ 76.5 billion by 2021, with a total goods value of almost US$ 1.2 trillion in pharmaceutical industry globally. Between 2015 and 2021, the pharmaceutical logistics projects will increase 41%, which will include US$ 283 billion of cold chain projects. There is a growing knowledge based on how to manage pharmaceutical cold chain efficiently (Pharmaceutical Commerce, 2017), incorporating RFID technology in that cold chain management.

Pharmaceutical industry is a highly vulnerable industry. For example, interlocking gates[19] and hazardous materials suits[20] are examples of protection from contamination. In addition, it is not

---

[18] Cold chain - a temperature-controlled supply chain.

[19] A door that does not open until another one is closed

uncommon for pharmaceutical production facilities to produce medicine or vaccine being targeted by terrorists to contaminate products that are distributed. Standard technologies such as video monitoring and surveillance, biometric identity authentication, vehicle license plate recognition, security (also interlocking) gates are common to these facilities. Disgruntled employees or just plain civilians may also attack pharmaceutical SCs for a variety of reasons and such attacks usually are executed without planning, which can make prevention more difficult. The United States of America Food and Drug Administration requires an entire pharmaceutical manufacturer to be shut down if as little as one single batch of pharmaceutical product (it produces) is contaminated. There is a recognition that enormous damage can be done if such product goes into the market, uncountable non-financial loss can happen.

Espionage is another vulnerability that is not uncommon in pharmaceutical industries. Mobile or desktop computing devices can be a target of theft, and backend servers can be a target of hacking. Riley and Walcott (2011) reported the pharmaceutical industry suffered US$ 500B in harm from intellectual property (IP) and trade secret theft. Detica (2011), in a report to the UK government estimated pharmaceutical, biotechnology and healthcare sector loss of IP, and reported the loss worth BPS1.8B. Such vulnerabilities were infringed by back-end attacks (discussed in Section 2.6.13) and physically tempering pharmaceutical samples.

1.11.3 The Jewellery and Pharmaceutical Industries and the PPRDLH

The largest jewellery markets worldwide in 2016 are China, the United States and India. The trade volume of jewellery in China is US$ 111.5 billion[21]. For the pharmaceutical industry, the largest market is the USA. However, local US manufacturers dominate the market and a short SC is featured. China is the second largest pharmaceutical market in the world in 2015, where its market size was US$ 108 billion, with a forecasted growth of 9.1% per annum until 2020 with a total market of US$ 167 billion[22]. As discussed in Section 1.9.3, PPRDLH occupies 30% of the entire China market exports; as an estimation, the PPRDLH has a US$ 50 billion pharmaceutical and US$ 30 billion jewellery market, which is highly significant in the world.

---

[20] Hazardous Materials Suits, also known as decontamination suit, is a whole-body garment that protects human body against hazardous materials

[21] Statista, Largest Jewellery Markets by Country https://www.statista.com/statistics/718856/largest-jewelry-markets-by-country/, accessed July 3rd 2018

[22] World Atlas, Countries with the Biggest Global Pharmaceutical Markets in the World https://www.worldatlas.com/articles/countries-with-the-biggest-global-pharmaceutical-markets-in-the-world.html, accessed July 3rd 2018

1.11.4 The Differences between the Jewellery and Pharmaceutical Supply Chains

The two industries, while both important SCs representative of a large and increasingly pervasive group of modern global PRD-sourced SCs, have significant differences. They are both connected with high value products (each making security and integrity an important factor), but the jewellery industry is more fragmented while the pharmaceutical industry is more connected. However, there are also significant differences in the two industries, as the unit value of the products is different. In pharmaceutical industry, products have low financial value but non-financial value (impact of corruption of the SC) is high; while in the jewellery industry the products are high in value but more easily replaced without irreversible customer impact.

Different SCs need to be handled differently. For instance, Hugos (2018) emphasized different SCs have different strategies; Cavinato (1992) contrasted cost and value for SC competitiveness; de Treville (2017) analysed SC in high cost environment; Swaminathan (1998) categorized SCs by constituent control elements (like inventory policy) and Carbone (2018) categorized different SCs by coordination modes and the kind of governance. It is therefore not surprising that the application of RFIDs in the two SCs is also different (will discuss further in section 7.4.9).

1.12 An Understanding of Whole-of-SC RFID Security: Potential Contributions

Research on cross-SC RFID system security contributes can be used to develop a generalized RFID security model that better recognises the end-to-end nature of global, diverse SCs. Such frameworks can better address vulnerability not yet identified in lists such as those from Rotter (2008) and Multi-domain SC idea from Kim et al. (2007).

For practitioners, there is a need for a policy framework, which makes a crucial contribution to a safer production environment in factories and across the whole SC, from parts and materials suppliers all the way through to the end consumers. Buyers will be assured that all items (they) acquire have secured across the entire SC, reducing direct and indirect financial impact on services and products. For SC system designers, such frameworks, informed by theoretical models, provide an effective and efficient guideline to direct technology and application development.

2 Literature Review

This chapter reviews and interprets the existing literature that is significant to the understanding of the phenomenon to be investigated. As this is a Design Science study, the literature review itself is treated as an artifact addressing research questions, and the implications of this are also addressed

2.1 Introduction

As stated in the title of this thesis, the research objective of this thesis is "Development of a Multi-Domain RFID Security Model for Global Supply Chains, and a Practical Framework for Model Adoption". The thesis objective is examined in chapter 3 and background information is needed before it is examined. This chapter gives a narrative review on scholarly papers consist of current knowledge and findings, as well as theoretical and methodological contributions to the study. The professional foundation for doctoral dissertation guidance Academic Coaching and Writing highlighted four important criteria in writing a literature review in 2017, namely qualification, neutrality, credibility, and worth. This advice has been followed in selecting the topics considered in the literature review. Sources are carefully examined for the qualification by examining authors' credentials. Neutrality is applied as much as possible to counter the author's perspective bias, such as using sources from various points of view. Credibility is asserted by examining author's past studies or papers published, including considering academic journals statistics rankings. Finally, whether the author's conclusion is worth to this study is the last decisive factor based to decide if the literature would be included in the literature review.

2.2 The Supply Chain

SC is defined by the Council of Supply Chain Management Professionals (CSCMP, 2018) as "a set of three or more entities (organizations or individuals) involved in the upstream and downstream flows of products, services, finances, and/or information from a source to a customer" (p.1). The definition has been updated throughout the years to align with its dynamic nature.

SCs do not run autonomously. They must be managed in a highly integrated way. SCs are therefore almost always approached from a SCM perspective. This is typically defined as:

> "Supply Chain Management encompasses the planning and management of all activities involved in sourcing and procurement, conversion, and all logistics management activities. Importantly, it also includes coordination and collaboration with channel partners, which can be suppliers, intermediaries, third-party service providers, and customers. In essence, supply chain management integrates supply and demand management within and across companies. Supply Chain Management is an integrating function with primary responsibility for linking major business functions and business processes within and across companies into a cohesive and high-performing business model. It includes all of the logistics management activities noted above, as well as manufacturing operations, and it drives coordination of processes and activities with and across marketing, sales, product design, finance and information technology." (p.1)

Together, the companies on a SC work to supply the materials and fulfil the requirements of customers, where the objective of a SC is to coordinate the materials to be put in and out of the firm.

2.3 Supply Chains and Role in Modern Business

Handfield and Nichols (2002) stated that managing the SC is a strategic operation in a corporation, involving operations and integrated logistics. Companies do not just compete with each other on the basis of their products but also on how well their SC for a particular product works, where the competition is all rounded from the outsourcing of materials (Turban et. al, 2018), management of bottlenecks (Ali and Mukasa, 2018), reduction of impacts on customers (Bhagwat and Raut, 2018), to the coordination of the smooth and continual flow of products and services into, through, and out of the firm (Braunscheidel and Suresh, 2018). In order to complete this task effectively, developing strong relationships with SC members, ensuring high-quality products and services, and sharing timely information among SC members are necessary. If information sharing is effective, the company can reduce order cycle time, minimize inventory levels across the SC, reduce the number of suppliers and carriers, and allow partners in the SC to build commitment to that SC (Sell, 1999).

Turban (2018) categorized SCs into four different types, namely "integrated make-to-stock", "continuous replenishment", "build-to-order", and "channel assembly". These represent a vast percentage of modern SCs. The integrated make-to-stock SC model restocks the finished-goods inventory efficiently by analysing customer demand in real time. The continuous replenishment SC model constantly replenishes the inventory by continuous shipments. The build-to-order SC model is to begin assembling of the customer's order after the receipt of the order. Channel assembly SC model is a slight modification to the

build-to-order model: the parts of the product are gathered and assembled as the product moves through the distribution channel.

2.3.1 Logistics and its Role in Supply Chain

The Council of Logistics Management (2001) defines logistics as "the integrated planning, control, realization, and monitoring of all internal and network-wide material, part, and product *flow*, including the necessary information flow, industrial and trading companies along the complete value-added chain (and product life cycle) for the purpose of conforming to customer requirements".

Manufacturers have important roles in various types of logistics management and will greatly impact the performance of an integrated SC because upstream SCs (suppliers, purchases and production lines) are more involved in the integrated planning (joint planning that ensures participation of all members in SC are benefited as a whole), while downstream SCs (flow of information and goods to clients and customers) carry out operations according to the planning. Failure to plan ahead thoroughly in the SC would affect the whole performance of the SC.

2.4 Security and its Importance in the Supply Chain

As the SCs purpose is to fulfil customer needs, successfully performing this task in a secured manner is a major concern. Christopher & Lee (2004) explained the importance of SC security as it affects the survival of a company. Colicchia & Strozzi (2012) suggested complex business situations are the source of SC security risk, in additional to operational risk. Despite these recognitions, security in SCs is not in practice, well addressed, and has caused huge losses; examples include Boeing, Cisco and Pfizer, which suffered lost up to US$ 2 billion, US$ 2.25 billion and US$ 2.8 billion, respectively (Hult et al., 2010).

2.5 RFID Systems and the Supply Chain

RFID is increasingly used in SCs to provide real time tracking of products. This provides operational benefits (tracking and managing location) as well as being integrated into security aspects (check if we still have the product, for instance). Real time tracking can be done without the need to see the product directly, as it is communicated wirelessly between tags on the products and readers, and are far more efficient and reliable than traditional stock checking and tracking.

2.5.1 What is RFID?

RFID has become ubiquitous and diverse in SCs. Its usage includes inventory monitoring and control, asset monitoring and management, electronic payment through smartcards, access

control, anti-theft, anti-tampering, anti-counterfeit, product integrity, recording of product conditions through the SC; and the list is constantly growing.

The RFID Journal website in 2006 defines RFID as

> ".. a generic term for technologies that use radio waves to automatically identify people or objects. There are several methods of identification, but the most common is to store a serial number that identifies a person or object, and perhaps other information, on a microchip that is attached to an antenna (the chip and the antenna together are called an RFID transponder or an RFID tag). The antenna enables the chip to transmit the identification information to a reader. The reader converts the radio waves reflected back from the RFID tag into digital information that can then be passed on to computers that can make use of it."

IDTechEx (2018) estimated that 16.4 billion tags have been sold solely in 2018 with a market size of US$ 11 billion. Since 2007, the number of tags have grown to US$ 26.88 in 2017, indeed, it is a proven technology for its application.

RFID is a generic term for technologies that use a microchip attached to an antenna (together it is called an "RFID transponder" or "RFID tag"). The transponder transmits identification information to a reader via electromagnetic radio frequency. The reader converts the radio waves from the RFID tag into digital information that can be passed on to computers for handling. There are two basic categories of RFID tags – active and passive (discussed in section 2.5.4). Active tags have an on-board power supply, on-board memory, sometimes a CPU, and in some specialized devices, various sensors, and a microchip antenna, which allows the chip to be recognized at a much greater distance (than passive tags), of up to 30 meters. (RFID Journal FAQ, 2010). Passive RFIDs, on the other hand, is not equipped with power source and therefore are passively dependent upon RFID reader's power to function.

As of 2018, over 104,000 research studies have been performed in RFID usages in SC (Google Scholar, 2018). In those 104,000 studies, 67,300 articles are in security, 39,300 in innovative use of RFID in SCs. Abdelkafi and Pero (2018) identified RFID as the driver of supply innovations and said it should be used in all SCs.

In SCM, RFID transponders carry data to identify products and their location. As a system, together with a network of readers, they form a series of "intelligent machines". Examples include automatic check out on retail shops, automatic replenishment from refrigerators, detecting missing food items. These are very valuable activities, but RFID transponders can also disclose information to unauthorised personnel (eg. hackers) using "long range RFID

interrogators", or data logged by the readers and saved in a company's database can be a leaking source for privacy intrusion.

2.5.2 Uses of RFID Systems in Supply Chain

RFIDs share information across the whole SC. Indeed, while their apparent active life may end with delivery of products, to which they are attached for ultimate customers, the devices themselves may continue to be functional until both product and packaging are destroyed, not just disposed of. In addition, RFIDs may be attached to products by different parties at several domains through the SC, so there may be multiple devices being active concurrently at any one time, as tabulated in Table 5.

Uses of RFIDs	Subject	Year	Detailed Usage	Examples
Item Track and Trace	DHL, UPS, TNT, and FedEx.	2003	Tracking and tracing[23] of goods sent within logistics fulfillment is a basic function	Standard feature provided by major logistics companies, including DHL, UPS, TNT, and FedEx (Swedberg, 2003).
Inventory Monitoring and Control	Decision Making	2004	Data in RFID tags are automatically collected which feed data models of decision support systems	Large amount of data generated (Lewis, 2005). Use of data to back up a decision support system and allow management to make decision (Louis et al., 2018)
Asset Monitoring and Management	Containers	2005	Reusable containers passing through logistics channels	Byproduct of logistics includes reusable containers and material handling systems can be monitored. (Roger, 2005)
Electronic Payment	Octopus	1994	Electronic payment by reading RFID tag, storing electronic cash value in the tag	Octopus system used in Hong Kong (founded 1994) utilizes an RFID tag in a plastic identification card for electronic cash transactions and identity verification (Octopus, 2010).
Access Control	Various	2003	RFID Pass card for all activities to be recorded, including time and location	Automatically detection can be achieved (Colvey, 2003). Electronic Article Surveillance alarms placed in entrances of department stores to prevent theft.
Anti-Theft	Mercedes Vehicle	2005	Recover of two Mercedes vehicles	MTrack (UK), AutoToll (HK), Tracker (UK), installed active RFID VHF tags in automobiles and recovered two Mercedes vehicles on June 23, 2010
Anti-Tampering	Electronic Seal	2010	Embedding RFID into electronic container seals for security initiatives	Placed in the gate of the container in place of a lock, with an alarm for subsequent anti tampering actions (Ward, 2006). Over 7000 patents embedding RFID into electronic seals that lock containers for anti-tampering, also serving antiterrorism initiatives from US and EU (FreePatentsOnline, 2010).
Anti-Counterfeit	Gillette Fusion Razor	2010	RFID tag to be a second source of genuine product authentication	Duplicate or invalid RFID data considered as a counterfeit or parallel imported item. Gillette tagging EPC standard RFID tags to their Fusion Razor for spotting parallelly imported goods (O'Conner, 2010).

Table 5 RFID Uses, with Examples and Year of Application

2.5.3 The RFID Lifecycle

Focusing in the lifecycle of RFID from its application(s) in the SC to when responsibility is relinquished to the ultimate customer is important in understanding potential uses – and

[23] A standard function of logistics companies to report location and audit trail of product from interface of computers, normally a website and mobile phones applications.

breaches. For example, a product that was tagged with an RFID in manufacturing domain could carry information identifying the product. When the product is passed on the SC, the product would be in the control of the next domain in downstream SC. This was called "transfer of cargo ownership" in traditional SC (Carrer, 1952). The manufacturing domain could receive product information from the SC RFID information systems but the physical handling of the RFID tag would be done by operators in the next domain.

This process will last until the product with RFID reaches the final customer, or "consumer", then the tag could be disposed. From the time the RFID is tagged onto the product, which marks the start of the RFID lifecycle, until the RFID tags are finally disposed, marking the end of the RFID lifecycle, is the scope of this study. RFID attached to products are passed on the SC, from one domain to the next, and there are different security issues. For example, for a single domain RFID system in upstream manufacturing, an RFID was passed along with the tag, and then the RFID can be used by the downstream SC operators as a "free-rider" (Whang, 2010), having RFID tagged in the products they carry, without the need of purchasing and tagging of the RFID tags. However, if one thinks of this usage of pre-tagged RFID in a conspiracy way, then the tags (and information that linked to them) can be used maliciously to attack the original upstream SC company (by hacking the number IDs of the tags, or subsequently reprogramming the tags). This type of hacking can temper the control of anti-counterfeit or anti-parallel imported goods, where RFID tags are (reprogrammed and) tagged onto goods which weren't meant to. Harrison et. al (2004) studied information management in product lifecycle and the role of networked RFID, but did not focus their study in RFID.

2.5.4 RFID Hardware

As with all information systems, RFID systems contain both hardware and software. These have been designed for different usage within the SC. RFID systems consist of three components: transponder (the RFID tag), air as the communication medium, and the host application (Piikivi, 2004). Figure 3 shows an example of RFID tag with an antenna and the integrated circuit[24].

[24] Integrated Circuit: An electronic circuit formed on a small piece of semiconducting material, which performs the same function as a larger circuit made from discrete components.

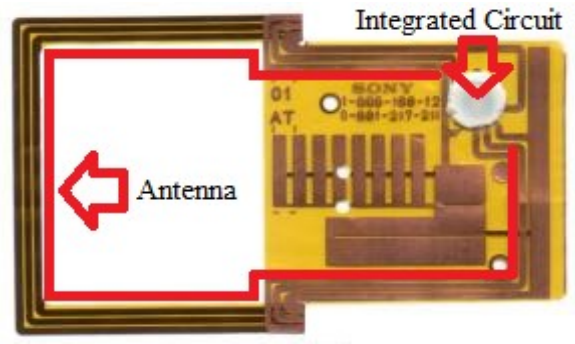


Figure 3 RFID Tag, the credit card sized Octopus Card used in Hong Kong as electronic cash, source: Octopus Card Limited (2001), modified by red line indicating antenna and integrated circuit labeled.

Active and Passive Tags

Tags may be divided into two fundamental types – active and passive (Lahiri, 2005). The major difference between passive and active RFID tags is that active tags have an on-board power supply, and on-board electronics in additional to microchip antennas. This device can then be recognized at a distance of up to 30 meters. The transponder has a remote memory (for example: ROM, PROM, E2PROM.) to store data from the application, which is located inside the reader (Paret, 2005). Air forms the communication medium between the RFID reader and the transponder: electrometric radio frequency (RF) waves carry the data while air is the coupling between the antennae of the transponder and the base station (RFID Tribe, 2005). Devices can be separated by most structures found in built environments, including both buildings and vehicles.

The base station is an analogue part used for receiving and transmitting RF signals, the circuit controls the protocol for communication with the transponder and the communication management interface to the host system (Colvey, 2005). The host system is an application that controls the system in which RFID tags (and readers) participate.

The two RFID tag categories can be further differentiated into Fully Passive, Fully Active, Semi-Active and Semi-Passive. Passive Power tags require no internal power source, whereas active tags require a power source. Fully Active tags are equipped with power sources and thus can actively send out RF data to signal its existence. Semi-Active and Semi-Passive tags are the same in most installations, where once the tags are located within the range, the reader's power will be used to perform all the intended actions (Finkenzeller, 2003) such as reading the memory chip.

Another way to distinguish the tags is by the ability to write data to a tag. A read only (RO) tag has data written on the chips where it cannot be modified in any way; it simply transmits this data (say, a product name) on command from the reader. A write once, read many (WORM)

chip is blank when it is manufactured, and then a device writes the data onto the tag for readers to read later. Read-write (RW) tags enable multiple read and write and allow data in the device to be amended during the course of use (Lahiri, 2006). The above read/write specialties are tabularized in Table 6.

RFID Tag IC Types	Typical Usage
Read Only (RO)	Data written on the chips where it cannot be modified
Write Once, Read Many (WORM)	Blank when manufactured, a device required to write data
Read-write (RW)	Multiple read and write, allows data to be amended

Table 6 RFID Tag IC Types, tabulated from Lahiri (2006)

Antennae are normally used for long-range applications, Chen at al (2013) explained RFID systems with various antennae can read RFID tags at a distance from 10 feet to 600 feet (depending also on frequency range, discussed in 2.5.4). RFID antennae can cover large amount of RFIDs where more than one transponder may be presented simultaneously (Colvey, 2005). There are two types of antennae; the first is a synchronized antenna, in series and parallel operating simultaneously, in which their magnetic fluxes can be in phase or in phase opposition. The second is a multiplexed antenna, which carries numerous magnetic fields that lengthen the recognition times of the transponder (Paret, 2005). The transponder can only operate if it is supplied with power, either internally or with an external source.

Frequency Ranges

RFID chips can also be divided according to their transmission frequencies, into five different types, namely Low Frequency (LF), High Frequency (HF), Very High Frequency (VHF), Ultra High Frequency (UHF), and Microwave Frequency. Except for VHF which has no particular application at the moment, the others already serve specific purposes, and contain special features that make them suited for particular implementations (Heinrich, 2005). The antenna length is proportional to the frequency utilized, and the higher the frequency is, the longer transmission distance it provides, though at a cost of being easier to be interfered with metal and liquids (Electromagnetic Interference, or EMI). The above frequencies and their specialties are tabularized in Table 7.

	Low Frequency (LF)	High Frequency (HF)	Ultrahigh Frequency (UHF)	Microwave Frequency
Typical Max Read Range (Passive Tags)	< 0.5 m	approx. 1 m	2 - 10 m	1- 2m
Pricing	Relatively expensive, even at high production volumes. Least susceptible to performance degradations from metal and liquids, though read range is very short.	Less expensive than LF tags. Relatively short read range and slower data rates when compared to higher frequencies. Best suited for application that does not require long read ranges.	Potentially lower cost than HF and much lower than LF tags. Offers good balance between read range and performance.	Similar characteristics to UHF. A drawback to this band is that microwave transmissions are the most susceptible to performance degradations due to metal and liquids, among other materials.
Rates	30-300KHz	3MHz to 30MHz	300 MHz to 1 GHz	Over 1GHz
Major Systems	125 to 124 KHz	13.56 MHz	915 MHz in US and 868 in Europe, 315 and 433 MHz US Department of Defense	2.45 (more common) or 5.8
Advantages	Good for metal liquids	Works with metal and liquids		Fastest data-transfer rate
Disadvantages	Low data transfer rates	Slow rate		Poor with metal and liquids
Remarks	Passive tags in general. Problems even with dirt, snow or mud.	Hospital being the major user		Antenna length is proportional to the frequency
Tag Power Source	Generally passive tags only, using inductive coupling	Generally passive tags only, using inductive coupling	Active tags with integral battery or passive tags using propagating E-field coupling	Active tags with integral battery or passive tags using propagating E-field coupling
Typical Applications Today	Access control, animal tracking, vehicle immobilizers, POS applications	"Smart Cards", Item-level tracking including baggage handling, libraries and perishable foodstuffs	Pallet tracking, electronic toll collection, baggage handling (US), asset management and high value item tagging	SCM, electronic toll collection
Notes	Largest installed base due to the mature nature of low frequency, inductive transponders	Currently the most widely available frequency worldwide as it is globally allocated to ISM. Used for contactless smart cards	The USA has the most radio spectrum available, Europe, Japan and the Far East have limited spectrum resulting in slower data rates and the need for smarter system design for dense reader environments.	This band is shared with Blue Tooth, wireless LANs and a plethora of license free devices. Power is limited in most regulatory environments which mean reduced read ranges.

Data rate (Slower «----------» Faster)

Passive tag size (Larger «----------» Smaller)

Ability to access under interference (Better «----------» Worse)

Table 7 Comparison of Properties of RFID Frequencies, Composed with Various Sources

Types	Power Source
Passive Tags	No battery
Active Tags	External power source
Semi-Active / Semi-Passive Tags	Battery in the RFID tag to notify existence, actual read / write is performed by external battery

Table 8 RFID Tags Types based on Power Source, Composed with Various Sources

2.5.5 Properties of RFIDs and their application in the Supply Chain

RFIDs often participate in systems based on barcodes. Barcodes are optical, machine-readable, usually represent the object carrying the barcode. Before, and still as an alternative to RFIDs, barcodes consist of a paper-based tag, which can be scanned by optical line of sight[25] readers.

Hong-Ying (2009) studied various applications of barcode technology in SC. General usage of barcode in SC includes point of sale scanning, logistics and warehouse management. Item and carton level can be tagged using traditional labels, or included in RFID tag information as illustrated in Figure 1. At each single step of SC operations scanning a barcode can serve as a real time confirmation of location and identity. For example in warehouse management, inventory acceptance, changes in warehouse location, and finally at product dispatch, carton/box/item scanning can be performed to verify the operator's action. Similarly, in supermarket or convenience stores, item level scanning at checkout counters has been in place for 30 years and allows stock and sales notifications.

RFID system functions are comparable to those of barcode systems in various ways, but the RFID technology provides major advantages over the older technology (Lahiri 2006), as summarized in Table 9.

[25] In terms of supply chain items identification, RFID systems are always compared to barcoding, which are generally printed in every single consumer items. One of the major differences of the two systems would be line of sight: RFID systems do not require the RFID tag to be "seen" by the RFID reader in order to scan the data within it. On the other hand, the barcode reader would need to "see" each and every barcode with the infra-red light beams to scan the data stored within. Being able to read the tag from a distance is important for RFID implementation in supply chain, as detectors can easier detect the tag and report the location of the tag. Such systems can work throughout large and diffuse installations such as warehouses and manufacturing plants.

RFID property	Benefit as compared to Barcode Technology
Contactless	The technology utilizes wireless technologies where there is no contact between the reader and the tag. Air is the communication medium.
Writeable Data	"RW RFID tags" enable multiple read and write of data during the course of the RFID's lifetime.
Absence of line of Sight	The RFID tag does not need to be "seen" by the RFID reader as do barcode systems.
Variety of Read Ranges	Passive RFID tags are readable up to the range two meters. If active tags are used, this extends to hundreds of meters.
Multiple Tag Reading	A single reader can communicate with many different (sometimes hundreds of) tags, one by one, all within a single second.
Rugged	RFIDs are rugged because they can be embedded and further protected
Perform Smart Tasks	RFIDs have memory and can store complex data in a format easily integrated with applications in scanning systems.
Accuracy	Multiple scans of multiple RFIDs can be conducted to increase accuracy approaching 100%

Table 9 Benefits of RFID Systems Comparing to Barcode Technologies

The technical benefits of RFID systems over barcode technologies provide even more potential benefits in SCM. A *wireless connection* between the reader and the tag, without copper wire or metal as a medium, allows no physical contact being made between SCs goods and its reader. It is then possible for goods to be access without stoppage in logistics exchange points say warehouse gates. *Writeable data* allows recording of large range of useful transactions; for example the properties of the SC goods (purchase order, location, shelf life, best before dates), monetary value (e.g. suggested retail price), and other details (e.g. taxable item, dangerous goods). Virtually all SC goods can be tagged, then data being read and write unlimited number of times throughout the lifetime of a products movement, conversion and storage in the SC.

Another property of RFID tags is the *variety of read ranges* which determines the best uses for the devices. While passive RFID tags are readable up to a range of two meters, suitable for individual SC goods, active tags can be read from hundreds of meters away, and allow readers to detect the tags over an entire location; a stock take for instance can be fully automated at a single command, with location and unit information read from one location and in seconds. This approach provides a major improvement in potential productivity over pre-existing (barcode) systems, as well as allows parallel-based designs for RFID systems; for example retailers can scan all sales items in one go in customer baskets at the checkout (or even at the doorway as they leave).

RFID are *rugged* and tags can be placed within two layers of materials (e.g. paper or plastics). These properties allow them to be used as an "RFID inlay", in which the tag chip and antenna are mounted on a substrate, sandwiched between two pieces of self-adhesive papers, and made

into a human-readable label. When the label is printed with barcode or other information, the corresponding number or barcode data is written to the RFID tag.

RFIDs can also be attached to other smart systems such as sensors (e.g. temperature) and RFID tag can also be used to record data measured using the sensor(s) (e.g. temperature changes) during logistics movements. This allows RFID to perform relatively complex monitoring tasks that serve to enable alerts or trigger actions from connected systems. It is partly for this reason that RFIDs have become very important in cold chains.

RFID are also *accurate* and approach 100% reading accuracy through the use of redundant readers at different reading angles in a location. Placing a number of cargo items on a pallet with a rotating plate could also allow a single reader to read all tags, guaranteeing a 100% read accuracy.

2.5.6 Disadvantages of RFID Systems Used in Supply Chain

RFID systems have certain disadvantages as well, and businesses need to consider the limitation of RFID systems as compared to barcode. Table 10 shows the major limitations of RFID over barcode.

Limitations	Description
Costly	Typical RFID costs US$ 0.07-0.15, while barcode has no variable cost on packaged products
Radio Interference	Liquid and metal gives Electro Magnetic Interference (EMI) with RF-Opaque and RF-Absorbent effect. Older wireless LANs and RFID reader also interfere with RFIDs.
Tag Collision	When more than one tag tries to communicate, tag collision occurs. When more than one reader tries to communicate, reader collision occurs.

Table 10 Limitation of RFID Systems Compared to Barcode Systems

These RFID technical limitations are multiplied when applied across the SC. For example, systems that use RFID for identification (e.g. staff cards) would not suffer from the costly issue the same degree as SC goods item level tagging - Goods tagged by RFIDs are variable cost and most RFIDs are not reusable in such SC application. Compared to barcode systems, especially for products having printed materials (e.g. box, manuals, or labels) accompanied, inclusion of barcode on the printed material is free of charge. On the other hand RFID systems would at least cost US$ 0.05 (RFID Journal, 2010), while one with a typical passive 96-bit EPC inlay costs from US$ 0.07 to 0.15 (RFID Journal, 2017). If RFIDs are tagged in every single piece of goods in a SC, every single product produced would incur a US$ 0.05 ex-factory cost; since this additional amount applies to each unit, this would represent a high percentage overhead, especially on low cost items.

In addition to costs, another limitation of RFID tag is the limitations to range imposed by the presence of liquids and metal (Heinrich, 2005; Poirier, 2006). These are the major examples of "RF-Opaque" objects; those that prevent communication between RFID transponders and readers (RFID Journal, 2010). Such interference is caused by various environmental factors; for example, RFID used in areas where older 900MHz wireless LANs exist. At present, many offices or warehouses are full of wireless LAN access points; the interference introduced there would require selection of an RFID frequency in a clear range (Bacheldor, 2007).

Reflection of RF signals is also a problem: for example multipath issues, where RF signals arrive at a tag in multiple wave paths. To further complicate this situation, the human body itself, being somewhat RF-Opaque limits the use of this technology where there are intensive groups of people and animals. Imagine a warehouse with boxes stacked on a pallet. The actual RFID tags read would depend on how RF-opaque materials in the stacked boxes/pallets are.

While interference is one of the hurdles in providing 100% RFID read reliability, *tag collision* is also a major limitation on RFID usage. Given that a reader can only communicate with one tag at a time, when more than one tag attempts to communicate, tag collision occurs. There has been considerable attention paid to developing anti-collision algorithms, including ALOHA for HF, Tree Walking for UHF (Taghaboni-Dutta, 2006). These have reduced (but not eliminated) this collision problem. Also, when two or more readers overlap, the reader cancels out the RF energy from one antenna of the other reader; this is called reader collision. These effects have been mitigated with anti-reader signal collisions devices such as Time Division Multiple Access (TDMA) that is used in most general RF application (Shin et al., 2009).

Finally, tag readability is also a concern, where read robustness depends on the number of times a particular tag can be read, and on the distance between reader and tag. In a typical warehouse environment, the case with multiple readers overlapping each other is extremely common and installation of RFID readers needs additional calculation on reader's energy zone (Engels and Sarma, 2002).

2.6 Practical Vulnerabilities of RFID Systems

Academics researches have considered theoretical and technical approaches to reducing vulnerability. These have been used as the basis for developing practical tactics to deal with vulnerabilities. Security imperatives have been recognized from the early stage in RFID's practical development as being critical, and there is hence a need for encryption and authentication. Data within RFID systems has to be protected from unauthorized access by intruders, and constrained from any unauthorized actions, including simply registering their presence in particular locations at particular times, which itself has management implications. Privacy is also an issue because RFIDs contain data or provide secondary location information

which can link products and people to times, places, events, and can be used to assert other interactions. It is critical that security must be well ensured for any application or product to be designed for public use, particularly as it involves money and material (Finkenzeller, 2003). Rotter (2008) identified a framework for assessing RFID system security and privacy risks. His framework categorizes RFID system vulnerability with the following criteria: eavesdropping, relay attacks, unauthorized tag reading, tag cloning, people tracking, replay attack, tag content changes, malware, RFID system breakdown, tag destruction, blocking, jamming, and back-end attacks.

Breach	Details	Updated scholar solutions
R1	Eavesdropping	Huo, Mitran, and Gong (2016)
R2	Relay Attacks	Tu and Piramuthu (2017)
R3	Unauthorized Tag Reading	Zumsteg and Qu (2018)
R4/I1	Tag Cloning	Lehtonen et al. (2009)
R5	People Tracking	Hutabarat et al. (2016)
R6	Replay Attack	Piramuthu and Doss (2017)
R7	Tag Content Changes	Ishida et al. (2017)
R8	Malware	Rodríguez (2017).
R9	RFID System Breakdown	Siewiorek and Swarz (2017)
R10	Tag Destruction	Raven et al. (2017)
R11	Blocking	Wang et al. (2017)
R12	Jamming	Khan and Ma (2017)
R13/I2	Back-end Attacks	Williams and Dabirsiaghi (2016) Zheng et al. (2017)
I3	Manipulation of Testing Equipment	Cassel, Piégay, and Lavé (2017)
I4	Tag Removal and Re-applying	Mullis, Gonzales and Olanoff (2017)
I5	Antenna	Su, Huang, and Chen (2017)
I6	Forgery of Product Data	Gandino, Montrucchio, and Rebaudengo (2017).

Table 11 List of Elements of Security Breaches in RFID from Literature

R items are described by Rotter (2008) and I items are reported from semi-structured interview (discussed in Chapter 6)

2.6.1 Eavesdropping

The term eavesdropping came from the legal field. The most widely used law dictionary, Black's Law Dictionary, defines eavesdropping as "secretly or stealthily listening to the private conversation of others without their consent" (The Law Dictionary, 2018). RFIDs are prone to eavesdropping like other wireless communication (eg. Wi-Fi and Bluetooth) technologies.

Eavesdropping is the most powerful route to acquire the majority of data from an RFID tag. To avoid eavesdropping attacks, cryptographic instruments which encrypt messages can be used (Juel 2006). Notable eavesdropping strikes have been exhibited against RFID frameworks as first described by Francis, Hancke, and Markantonakis (2009). Agreeing with these scholars, Hancke (2011) revisited the topic of RFID eavesdropping attacks and determined eavesdropping as the most relevant RFID attack. In the study a low-cost eavesdropping device was constructed using easy to obtain parts and reference designs, demonstrating ease of access

to such breaches. Huo, Mitran, and Gong (2016) validated a generalized framework for active eavesdropping attacks in Passive Freuency-hopping Spread Spectrum[26] RFID Systems.

2.6.2 Replay Attack

Piramuthu and Doss (2017) studied replay attack in sensor-based RFID systems for simultaneous presence of multiple RFID tags. Replay attacks capture RFID data and then replay it at a later time to the receiving device in order to achieve benefits such as stealing information or gaining access to prohibited areas.

2.6.3 Relay Attack

Relay attack is similar to replay attack except the message is used instantaneously instead of replayed later; Tu and Piramuthu (2017) defined RFID relay attacks as "attacks related to man-in-the-middle and immediately replay". Silberschneider et al. (2013) demonstrated how to perform a relay attack with the use of a modern smart phone acting as a mole to interrogate a victim's card in an RFID system. In SCs, RFID security breach includes a card that is present in an RFID controlled zone that waits for the reader's signal. Once the reader's signal is received it is transmitted to another RFID device that is close to a genuine product. By capturing the signal response of the RFID transponder in the genuine product and replaying it immediately in the RFID controlled zone, fake product existence data can be signalled and manipulated. Such breaches are more consumer related and reports of loss of cars by theft in the keyless go systems using relay attacks are not uncommon (CNET, 2006).

2.6.4 Unauthorized Tag Reading

Rotter (2008) considered attackers using a fake reader to read tag information as "unauthorized tag reading". A fake reader's range can be extended several-fold through technical modification. Rotter (2008) suggested a way to eliminate the problem: the genuine user has to initiate the reading through an activity, an example of which would be pressing a button. Zumsteg and Qu (2018) suggested improvement of security of the tag to avoid unauthorized reading by studying RFID tags reading patterns and configuring RFID tags to be read in spatial locations.

2.6.5 Tag Cloning

Lehtonen, Ostojic, and Michahelles (2009) defined copying of an RFID tag, with all the data being the same when read by reader as "tag cloning". By using an RFID reader it is feasible to

---

[26] Freuency-hopping Spread Spectrum, or more commonly abbreviated by FHSS, is a radio signals transmitting method done by rapidly switching carrier among frequency channels.

copy data in an RFID and then write it to an empty tag. For this tag to be treated as the original tag, it is necessary for the copied tag to use the same tag frequency. In SCs there is considerable variation in tag system frequency, which does help to make this more difficult.

2.6.6 Human Tracking

Human tracking is an RFID security vulnerability that has been identified by Rotter (2008). Rotter (2008) defined human tracking to be RFID Implant-based medical information systems and access-control systems, with examples of e-Passports which targets RFID tags built into human body instead of goods. To date such RFID tracking is not used in SC systems.

2.6.7 Tag Content Changes

Unauthorized changes made by writing to RFID tags are considered as "tag content changes". For example, unethical staff working for a manufacturer in the SC may make changes to the contents of an RFID tag by using retired RFID devices. Likewise, a logistics transport service provider can make changes to the content while the product is in transit. Ishida et al. (2017) have proposed security systems to avoid unwanted tag content changes.

2.6.8 Malware

The installation of Malware in RFID information systems hosting servers or databases is considered no different from a general information system security breach, and can be addressed by well-established security and anti-hacking solutions. The largest server computer operating system manufacturer Microsoft (2009) defined Malware to be "the short form of malicious software, which includes computer viruses, worms, Trojan horses, ransomware, spyware, adware, and scareware". RFID readers are installed on mobile handheld device, the largest mobile operating system manufacturer Google further explains that Malware has the ability to take control of and damage handheld computers (Google, 2013). Some malware is not purposely installed to breach a particular computer. For example, Symantec (2013), the largest security solution provider, announced that there are social media methods that utilize the functions of online social networks to disseminate malware to the other typical activities such as offering fake gift cards or tricking online social networks users to share the appealing, malware-embedded videos, websites or messages. Malware writers could also disguise malware as another particular type of file that an individual would download (Jaishankar, 2011). Therefore, if SC operators use RFID systems for their personal (entertainment) needs, malware can infiltrate these systems as well.

Solutions have been identified, and categorized by authors such as Misra et al. (2014), who analyzed the effectiveness of anti-malware in an infected network. Servers in the cloud with

virtualization technology[27] are tackled by blocking software (Li et al., 2012), detection software (Stübing, 2013) and hardware (Marnerides et al., 2013; Watson et al., 2013), as Malware can attack virtual machines too (Stewin and Bystrov, 2012). Shahin (2014) suggested cloud computing suppliers should limit propagation and directly minimize malware in their cloud networks. Without these anti-malware measures, malwares can affect physical machine performance in resources such as memory, storage, and processor (Wueest, 2012). An incident of malware in virtual machine in SC was documented (Rodríguez, 2017) for the point-of-sale RAM scraping malware.

2.6.9 RFID System Breakdown

RFID system breakdown is a generic term that refers to a malfunctioning RFID system being maliciously engineered, for example through hardware or software problems resulting from malware or Backend attacks. Different problems could require different solutions and therefore the RFID system breakdown is addressed based on the detailed causes and sources in the study.

2.6.10 Tag Destruction

RFID tags can be destroyed or simply untaged from the product. Other physical destruction methods of RFID tag include applying extreme pressure to the tag, chemical exposure, electrostatic discharge, or destroying the antennas with a knife. Raven et. al (2017) proposed an RFID tag with anti-tamper assembly to prevent its destruction. There are also software approaches; so called KILL commands that permanently destroy an RFID tag. These are useful and are inserted by the RFID system designer, but this command, if used in an unauthorized way, can be malicious.

2.6.11 Blocking

RFID signal blocking reduces the signal strength by blocking the electromagnetic field with barriers. This barrier is a physical object and can be made of conductive or magnetic (RF-opaque) materials, and is therefore professionally referred to as electromagnetic shielding. Wang et al. (2017) studied RFID systems for real-time activity recognition using radio patterns to avoid RFID signal blocking. Individuals can easily penetrate RFID systems by attaching a piece of metal that surrounds the RFID in order to block RFID signals.

---

[27] Virtual machine is an emulation of a computer system. Virtual machines are software emulating computer architectures and provide functionality of a physical computer.

2.6.12 Jamming and Interference

Traditionally the use of the term jamming has two different meanings. In the past there was unintentional jamming, which occurs when a busy frequency is transmitted to make practitioners unable to verify whether the frequency is being used. Currently this phenomenon is described by the term “interference” and the use of the term jamming is applied when there is deliberate use of a radio signal to disrupt communications or prevent people from listening to broadcasts.

RFIDs are vulnerable to radio frequency interference through Radio Frequency Opaque or Radio Frequency Absorbent interventions. Metal is the most common example of an RF-opaque object that impedes RF signals by blocking, reflecting, and scattering them. On the other hand, liquids are common RF-absorbent material as it allows radio signals to propagate through the material with a tremendous loss of energy. These situations are included in the general term “electromagnetic interference” (EMI). EMI vulnerability is commonly exploited as a RFID security breach as such implementation is considerably easier than other breaches. For example, a piece of metal covering an RFID tag (blocking) is easier than complete destruction of an RFID tag. Sometimes a closed RFID system can also jam the signals it uses, or between readers. Khan and Ma (2017) proposed reflective nonlinear transmission lines for single-antenna non-self jamming.

2.6.13 Back-end Attacks

Back-end attacks are those of RFID systems that are hosted by computer servers. The attack impacts those parts of systems that exist behind the scenes (TeskaLabs, 2016), that are often used for data storage or communication. These attacks are not limited to RFID systems but also other information systems. Usually the server side database is penetrated, for the purpose of stealing information, manipulating data, or disrupting operations of the system.

Backend attacks usually cause more severe damage compared to front-end, which is only the part that the user interacts with; in most cases, an attack to the front-end could only impact design features in the website or application, links, transactions, images, content, but not the entire system database. Williams and Dabirsiaghi (2016) suggested that such attacks could be avoided by introducing a different method and system of attack detection and protection in computer systems. Zheng et al. (2017) implemented a mutual authentication protocol for RFID to avoid back-end attacks.

2.6.14 Manipulation of Testing Equipment

Manipulation of testing equipment of RFIDs includes tampering with the reader by hardware systems such as antenna coils, or replacing software codes in the RFID environment to perform

unintended operations upon scanning of the RFID. RFID equipment manipulation includes insertion of RFIDs into existing RFID systems in order to achieve benefits (Cassel, Piégay, and Lavé (2017).

2.6.15 Tag Removal and Re-application

Tag removal is the act of simply removing the RFID tag. Preventing the RFID tag being reapplied is the general remedy, and includes physical protection such as covering the RFID tag or technological means including RFID systems that attach to power source for keeping RFID data. Tag removal is different from tag destruction as suggested by Rotter (2008); the tag itself is not destroyed, and maybe even reapplied to other goods for another security breach.

Mullis, Gonzalez, and Olanoff, E. (2017) considered RFID tag removal and reapplying as taking away a genuine RFID tag and reapplying it on another good. There could be many reasons to breach a RFID system by doing so, for example, to remove an RFID tag in an expensive product and apply it to a cheaper product for checkout, or just simply exchanging two products' identity in order to manipulate information such as the expiry date of the product.

2.6.16 Attack against RF Communication

Attacks against RF communication include blocking and jamming as suggested by Rotter (2008), and tampering with RFID antennas. By modifying antennae the RFID data can be sent to an intruder's unauthorized device instead of the intended RFID reader. Modern antennas are harder to hack as they can be printed or stamped with conductive ink or vapor deposited onto RFID labels (Fang et. al, 2018). Su, Huang, and Chen (2017) protected RFID antennae by through design, using ellipse-shaped with slanted slot circularly polarized monopole antenna for UHF RFID readers.

2.6.17 Manipulation of Product Data

Tag content changes can lead to manipulation of product data, but these two RFID vulnerabilities are not the same. Manipulation of product data can be done without physically tampering with the RFID tag itself, but changing data that is associated with the tag, from database servers or data that is stored locally in handheld devices. Gandino, Montrucchio, and Rebaudengo (2017) included traceability features in RFID against manipulation of product data.

2.7 Research of RFID Vulnerability Solutions

The RFID vulnerability issue has been examined by many authors; from technological aspects including hardware and software solutions (Bi and Mu, 2010; Lee et al., 2005; Lee, Batina, and

Verbauwhede, 2010; Liu, 2010; Osaka, 2009; Rieback, Crispo, and Tanenbaum, 2005; Sarma et al., 2003; Ustundag and Tanyas, 2009; Whang, 2010), user management which focuses on how trusted lists of RFID data interchange are established (Cha, 2010; Cai, 2011; Mahinderjit-Singh and Li, 2010; Lehtonen, 2008; Ohkubo, Suzuki, and Kinoshita, 2005), forecasting modeling approaches to forecast vulnerability by various mathematical models (Cai, 2009; Luo et al., 2008; Wang, 2011; Zhang, 2011), and case study based research which raises issues that focus on specific products (Cheung and Choi, 2011; Kumar, 2011; Lao et al., 2011; Li and Becerik-Gerber, 2011; Moreno, 2010; Qu, 2011). This issue has been examined by many authors. These approaches are categorized and summarized.

2.7.1 Technological Research

Most technological studies examine vulnerability problems with the physical RFID tag. For example, a device has been introduced by "RFID Guardian" which enables the user to scan the RFID and provide a mechanism to destroy the transponder if a breach is detected (Rieback, Crispo, and Tanenbaum, 2005).

Vulnerability can also arise from insecure wireless channels of RFID communication. These studies focus on impacts and defence against counterfeit-RFID tag attacks, relay attacks, eavesdropping attacks, and various other similar attacks (Liu, 2010).

Assessments of the impact and likelihood of these threats have been examined using a simulation model incorporating security level effects, in addition to taking other factors such as efficiency, accuracy, and visibility into consideration. It has been used to calculate the expected benefits of an integrated RFID system on a three-echelon SC obtained through performance increases (Ustundag and Tanyas, 2009).

Encryption incorporating hash functions and a symmetric key cryptosystem have been proposed to solve five RFID security problems, including the ability to authenticate RFID devices (coined by the term "indistinguishability"), forward security, resistance against replay attack, resistance against tag killing and ownership transferability (Osaka, 2009). Another practical solution is the attempt to solve this problem with cryptographic primitives such as hash functions, private-key algorithms, public-key algorithms and various authentication methods defined by the EPC of the ISO systems. A weakness in these approaches is derived from a lack of consumer side action to stop transponders from reading (Lee, Batina, and Verbauwhede, 2010). These studies look at protecting the RFID system by additional hardware either embedded in the specific tag being used or installed in the specific RFID reading environment. While this does address the vulnerability issue, such approaches are inefficient in areas that cannot be controlled and areas typical of diffuse SC environments.

Cost is always a major concern in RFID tags used in SCM, owing to the large quantity of consumer goods involved. This requirement has generated low-cost RFID tag hardware security studies (Sarma et al., 2003), examining authentication issues particularly with low cost passive RFID tags (those that do not have built-in power supply) (Bi and Mu, 2010). Further studies of low-cost tags focus on approaches to a total quality management (TQM) model (Lee et al., 2003). “Free lunch” uses of RFID tags by downstream logistics derived from upstream logistics attached tags has also been studied (Whang, 2010), with a focus on the timing issue in applying the tag.

For high-cost RFID tags, the research is either missing in most areas, or assumes products do not carry high-cost RFID tags at all (hence implying high-cost RIFD tags do not contribute consequentially to security problems).

2.7.2 User Management Research

Consumer education is a focus for security improvements in RFIDs. These solutions require additional actions on the consumer side (Ohkubo, Suzuki, and Kinoshita, 2005). Other studies suggested obtaining consumer’s approval in data collection, that data generated from RFID transponders should only be undertaken by those with licenses (Cha, 2010) in order to control RFID data to be accessed by authenticated parties (Mahinderjit-Singh and Li, 2010). “Symmetric secret” and honesty of third party logistics (3PL) parties are also important and studies have suggested this “trusted list” should be evaluated in a symmetric manner (Cai, 2011). However, these studies have not addressed the security issue in situations where the consumers or 3PLs are not cooperating.

2.7.3 Forecasting Model Research

There are numerous models developed to forecast RFID system's vulnerability. However most of these models examine either a subset of RFID systems or specific products only. SC co-ordination, technology application, risk management, and reliability assurance are the only solution measures studied as noted by Zhang (2011). Wang (2011) acknowledged Zhang and related the studies to short-term forecasting models but considered only total inventory cost, inventory turnover and bullwhip effect. A value analysis framework to evaluate the business value of RFID is built (Luo et al., 2008) but it does not provide any risk management in RFID security. Only three elements appear to have been considered; security, visibility, and efficiency in a two level mode security for RFID system (Cai, 2009). None of these studies provide a forecasting or evaluation model for long term and comprehensive security elements.

2.7.4 Integration Models of RFID Security

Kim et al. (2007) has named them "multi-domain" systems for RFID tags used by two or more different RFID domains (will be discussed in section 2.7.7), and considered security and privacy problems in such systems. A security framework based solely on tags that carry the globalized EPC, or in short EPCGlobal tags, in an RFID multi-domain system was produced and could evaluate authentication and authorization for RFID. Lehtonen (2008) has addressed chains of trust, threats, and risk in product authentication on predefined SC partners. Both studies consider the use of RFID tags with various parties, reflecting the practical issue of addressing RFID security in a system with SC partners.

2.7.5 Case Study Attempt to Solve the Vulnerability Problem

There are also a lot of studies attempted to address the issue by examining case studies, but they focused only on specific products. Containerized SC was examined (Moreno, 2010), as well as food supply (Li, 2011), pharmaceuticals (Kumar, 2011), EPCGlobal (Alfaro et al., 2011), Anti-counterfeit (Cheung and Choi, 2011), Hospital (Qu, 2011), and Manufacturing (Lao et al., 2011). A single framework with elements that are general to all consumer products has not been examined.

2.7.6 Causes or Sources of Information Systems Vulnerability and Solutions

The RFID vulnerability can be categorized into causes and sources (discussion in section 7.4.11). Various authors have tried to tackle such causes and sources, for example Reason (2000) attempted to manage human error; Possible solutions to hacker attack has been analyzed by various scholars including Lee (2015), Mandhare, Sen, & Shende (2015), Raju and Parwekar (2015), and Apiecionek, Czerniak, and Dobrosielski (2015). Hikage et al. (2015) defined essential components for realizing the ubiquitous society that relates to radio frequency operating environment; while Stylianou et al. (2013) and Guo (2013) attempted to reduce unethical usages to technology equipment.

Human Error

Reason (2000) explained that the human error problem can be viewed in two ways: the person approach and the system approach. The person approach focuses on the errors of individuals, while the system approach concentrates on the conditions under which individuals work and tries to build defences to avert errors. As human error can exist in various scenarios in an RFID system it is believed the human error in the context should be managed by the system approach as suggested by Reason (2000). System approach concentrates on the conditions under which individuals work and tries to build defences to avert errors or mitigate their effects. For example, a system approach could reduce recurrent error traps in the workplace and the

organizational processes by minimizing or omitting incidents where workers can directly deal with RFID tags, including applying or reapplying, reducing “upstream” systemic factors of human error. However, eliminating human interaction of RFID, for example the use of fully automated end-to-end robots in the SC is impossible in practice due to its complexity, particularly in the multi-domain SC.

Therefore, human error in multi-domain SC's RFID security breaches cannot be tackled by system approaches, and can only concentrate on the conditions under which individuals work and try to build defences to avert errors or mitigate their effects. Defences for human error should be implemented without the elimination of the human involvement. Since individual work is essential in a multi-domain SC, training must be emphasized in order to minimize the RFID security breaches.

Training is described as the “extensiveness of formalized programs to develop knowledge, skills and abilities” (Evans & Davis, 2005, p. 760), and it is an important asset for SC operators. Fitzgerald (1992) defined that understanding the distinctions will avail you to understand the processes that characterize training and development and the ways in which they affect the short and long-term prosperity of an organization. Developing an efficacious employee performance and development plan is one of those processes.

In the case of RFID security breaches, systems that are implemented with RFID should have financial budget reserved for training. It is suggested that reserving 10-15 percent of the total IT implementation budget for training will give an organization an 80 percent chance of prosperous implementation (Umble et al., 2003).

There are also side benefits on proper training being done. For example, there are significant and positive effects on work performance by the employee training (Russell, Terborg and Power 1985; Dastmalchian and Blyton, 1992), and employee training can enhance leadership development (Ladyshewsky, 2007) and employee learning (Hasan, 2006). SC is an always evolving business and it is essential for operators to maintain overall SC performance, and therefore leadership development and employee learning are also important. Management goals can be shared with employees through training, as employee training’s likely outcome is a highly motivated work force whose goals are proximately aligned with those of the management (Thomas and Velthouse 1994).

Key performance indicators are often used in SC to measure overall SC effectiveness, usually reviewed in the business world during contracts renewal. Training would also improve the performance of SC. Studies by Kalleberg and Moody (1994), Delaney and Huselid (1996), and Harel and Tzafrir (1999) suggested that training has a positive result on recognized organizational performance.

Training depends on correct candidates in human resources, and researches have suggested that implementing HRM practice, including employee training, can enhance firm performance (Arthur 1994; Pfeffer 1998; Birdi, Clegg and Patterson 2008). From the training and the HRM practice, it could enhance the performance of the employee such as knowledge, skills and abilities. Besides, it helps to motivate and strengthen commitment to the tasks of the organization (Jackson and Schuler 1995; Birdi et al. 2008).

Peretz & Rosenblatt (2011) noted the importance of training for organizational effectiveness, and scholars also further emphasized that motivation and cognitive ability seem to contribute most to the effective transfer of training to actual job tasks (Bell & Kozlowski, 2008; Blume et al., 2010; Colquitt, LePine, & Noe, 2000; Noe, Tews, & McConnell Dachner, 2010)

After motivation to SC operators is emphasized through HRM and company vision based training, performance needs to be re-evaluated. Boselie et al. (2001) related various HRM practices with impact on performance, and d'Arcimoles (1997) highlighted that training is connected with effects on both productivity and profitability. Such improvements will be reflected in the reduction of unethical usage in RFID systems.

Hacker Attack

Various scholars have taken active approaches to reduce hacker attack possibilities based on the system to be protected, including using proxy server authentication for HTTP (Lee, 2015), data fortification for cloud computing based system (Mandhare, Sen, & Shende 2015), dual encryption for passwords (Raju and Parwekar 2015), and quality of services methods as DDoS protection (Apiecionek, Czerniak, and Dobrosielski 2015). Wealth of policies has been defined based on systems to be projected. These studies suggest that the use of security protocols such as HTTPS system is required on all internet connected servers, with the installation of firewall devices between the internet and intranet. Encrypted data communications through the use of Secure Socket Layer (SSL), while properly implemented, can ensure data security.

Operating Environment

Hikage et al. (2015) has implemented a step-by-step electromagnetic interference (EMI) assessment of RFID interrogators, showing examples of interrogators operating in various RF bands and experimental evaluation results for practical devices. The assessment defined civilian wireless devices as "*essential components for realizing the ubiquitous society*", such as mobile phones, radio frequency Identification (RFID), Electric Article Surveillance and wireless power transmission. Similar assessment can be set as standard policies to assess the RFID EMI issues in SC operating environment. An assessment should be made and re-evaluated monthly to avoid EMI of civilian wireless devices against RFID tags on products.

Shall assessment report any possible EMI, detectors should be installed in RFID operational environments and require such civilian wireless device to be turned off.

Unethical Usage

Stylianou et al. (2013) proposed a way to understand the behavioural intention of unethical information technology practices. The study could be used to improve understanding of the emergent ethical issues existing in the SC RFID related environment. Behavioural intention of unethical information technology practices should be highlighted, and application to a framework for implementing security-related policies can be achieved. Guo (2013) conducted an extensive review of security-related information system usage behaviour in the workplace by delineating and synthesizing the differences and proposed a framework for conceptualizing security-related behaviour. The framework developed consistent and comparable terms and concepts for further imposing security policies.

Users perform unethically to the system either because they do not accept new IT systems or they do not share the same visions with the company in applying new IT system, as a result they use the system in a rebellious way. Acceptance of new IT systems by frontline SC operators are important, as the benefaction of a new technology to a firm performance can only be realized when and if the new technology is widely accepted (Hall and Khan, 2003).

Many research articles have been found to determine factors that restrain the acceptance of new technologies by workers (Nah et al., 2001; Nicolaou, 2004; Bradley, 2008), and Venkatesh et al. (2003) had a study that focuses on the four critical factors related to technological use in organizational context: perceived attributes of change, social influence, facilitating conditions and individual characteristics.

Nicolaou, A.I. (2004) explained that the success of the IT system implementation depends on user participation and whether users are involved in the system development process, business needs from the assessment and data unification into the new system. Therefore, user acceptance is important in system deployment, and to promote such user acceptance, benefits to the user for using new IT systems must be presented. For example, Bruque, S. and Moyano, J. (2007) examined case studies of the factors investigated that end-users would adopt the new IT system better by reducing the time for system being totally launched.

Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F.D. (2003) analysed technology acceptance literature, and categorized theoretical models to explain technology acceptance, including the theory of reasoned action, the technology acceptance model, the motivational model, the theory of planned behaviour, a model combining the technology acceptance model, the model of PC utilization, the innovation diffusion theory, and the social cognitive theory. Apart from introducing benefits to end users, factors leading to resistance of using new systems

must be avoided. Kim and Kankanhalli (2009) evaluated attributes where end users may adopt or resist IT systems when there is technological change implemented.

In addition to increase user acceptance in new IT systems, ethically use of IT system can be improved by proper use of human resource management and training on company vision. Motivating staff and sharing company vision to SC operators have been a traditionally difficult task, and company vision based targeted training and best practice in human resource management (HRM) should be applied to solve this problem. While positively motivating staffs can be a prevention of further RFID security breaches, for every unethical usage of RFID system found, the loophole should be closed for a quick fix to the problem. This is particularly the case when RFID security breaches are found in multi-domain SCs, where certain RFID system operators are in an uncontrolled area where HRM and motivation of staffs cannot be easily achieved.

2.7.7 Multi-domain Models of RFID Security

Kim et al. (2007) defined the term "Multi-domain RFID systems" as a domain in a SC communicating to or from RFID systems owned by another domain in a SC. Focusing in RFID systems, Kim et al. did not explicitly address the scope of a "domain"; whether it represents a single company or different companies in a SC. In real world scenario, different RFID systems run by different companies working within the SC tend to have more security problems compared to those run by the same company. Furthermore, a domain can be seen to encompass one or more companies with the same function in a SC, and multi-domain therefore refer to companies with more than one function in the SC. For example, a retailer represents one "domain" in a SC, whereas a typical SC consisting a supplier, an importer and a retailer, forms a "multi-domain SC", with the constituent domains interconnecting throughout the SC.

Kim et al. recognized the RFID tag-owning organization which implements the RFID tag for its own use in the SC to be a "single-domain" system. They raised that these single-domain systems may interact with the RFID systems of other SC members (e.g. the manufacturer's RFID tag being read by a retailer), and terms this as a "single multi-domain" system which, because this interaction may be potentially less controlled than a simple single-domain system, or even a multi-domain system, can introduce RFID data security vulnerabilities. Lehtonen (2008), while not specifically recognizing multi-domain systems, has addressed chains of trust, threats, and risk in product authentication on predefined SC partners. Both studies consider the use of RFID tags with various parties, reflecting the practical issue of addressing RFID security in a system with more than one SC partners.

However, while these researchers come closest to recognizing SC complexity with respect to RFID security, none of them address the real world complexity of global SCs for a product and

its associated packaging and transportation for the total time it exists in that SC. Such a system could perhaps be seen as a network of disjointed large scale multi-multi-domain systems.

2.7.8 Attack Vectors of RFIDs in Multi-Domain Supply Chain

EPCGlobal defined "EPC Network" that starts from a product being manufactured and ends with a consumer acquiring that product (Kim, 2009), which is illustrated in Figure 4. Defined by EPCGlobal to identify every single manufactured physical object in the world, that organisation published an open standard, the EPCGlobal Tag Data Standard. The typical usage of EPC involves the use of Object Naming Service (ONS) and EPC Information Systems (EPC IS). An illustration is given in Figure 5, where a manufacturer has manufactured a product. Tagged by an EPC RFID, the attribute of the tag is uploaded to the local ONS with an EPC IS. Synchronizing with the root ONS, any party on the SC can request information about this EPC RFID through the party's EPC IS, via EPC discovery services hosted in the EPC Network. As of 2018, EPCGlobal has SC industry leaders[28] joining their board of governors and the aim of the EPCGlobal is to operate the standard for EPC RFID with Internet as the hub to share information among the EPCGlobal Network.

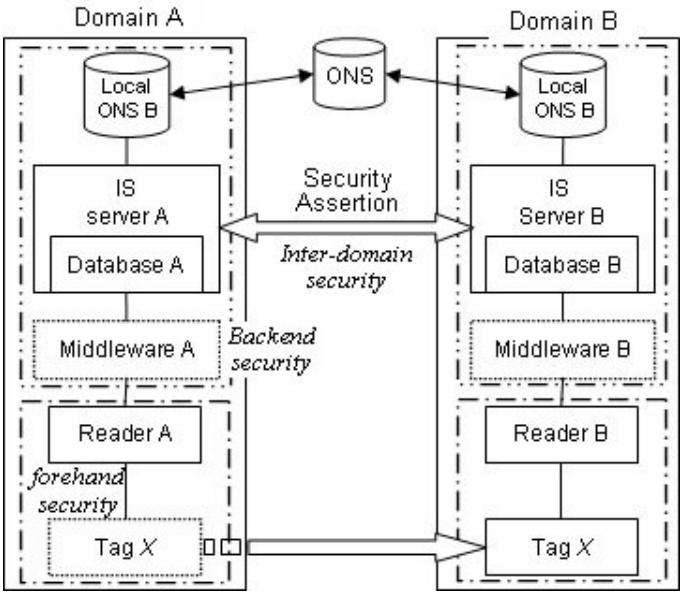


Figure 4 "A RFID multi-domain system" adapted from Kim et al.(2007), Kim et al. included security features in this figure (in italic).

[28] GS1 board of governors includes Auto-ID Labs, Cisco Systems, DHL Supply Chain, Haier, Johnson & Johnson, Kimberly-Clark Corporation, LG Electronics, Lockheed Martin Corporation, Metro AG, Novartis Pharma AG, the United States Office of the Secretary of Defense, Procter & Gamble, Sony Corporation, Dow Chemical Company, and Wal-Mart Stores, Inc. as of May 17, 2018

From the perspective of an RFID Lifecycle, RFIDs are pre-assigned (through an EPC-type standard) prior to all manufacturing and post-consumer SC actions. Prior to manufacturing, RFID can reside in manufacturing machines, in factories that manufacture parts of consumer products and final assemblies, and in their transportation and warehousing locations. Post-consumer acquisition, RFID tags can reside in the product, where disposal of RFID products are in general garbage collection.

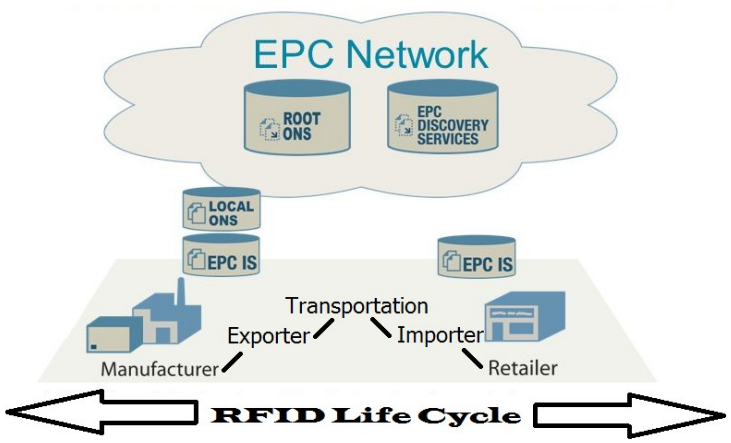


Figure 5 "EPC Network" as proposed by EPCGlobal (2001), original figure focused only with manufacturer and retailer. The concept of RFID Lifecycle is added with inclusion of other typical parties (in black) in the supply chain for demonstration of the use of EPC Network.

This extends tags beyond just spatial domains, to temporal ones based on the flow of the SC. It also adds a dimension to vulnerability opportunities and privacy issues

2.8 Practical Implications of Academic Gaps

Businessmen would prefer to have a single and easy to follow mechanism to solve problems, which is currently lacking from the academic researches. For example, a single flowchart, which leads from identifying RFID vulnerability attack as the problem, through choices boxes as pathways, to practical solutions of the stated problem, would allow businesses for easy adoption to prevent future attacks. Such easy-to-follow flowcharts exist in other business management decisions from minor operational issues like employee termination (Veyrat, 2017) to major systematic decisions like continuous improvement (Veyrat, 2016). Such flowcharts-like decision making model would benefit businesses for making decisions in the fast paced business world.

2.9 Analysis Tools

Data analysis tools allow researchers to sort through data in order to identify patterns, trends, relationships, correlations, and anomalies (Vassallo et al., 2018). Literature explanations of the tools are reviewed in this section, with the application of the tools discussed in Chapter 4.

2.9.1 Fishbone Diagrams

A simple tool used in this study to tackle a complex multi-domain problem would be the fishbone diagram. Fishbone diagram is also known as Ishikawa diagram. It was formed for the aim of recognizing and grouping the causes which create a quality issue. This method has been applied steadily to categorize the causes of other types of problems which an organization would face with. Hence, Fishbone diagram developed as a very handy tool in identifying risk of an event with various related causes (Ilie and Ciocoiu, 2010, Hekmatpanah, 2011, Abraham, Dereje, & Lim, 2001). The application of Fishbone diagram achieved the determination of the risk of key and subordinate causes, and the structure of treatment measures on vulnerability areas, specifically focused on the causes which determine high risk values. It is a simple analysis of cause sequence which mentions numerous causes and their sequence also can be finished with other illustration and hierarchy components for risks treatment. It is used to imitate the dynamic of the process analyzed (Ilie and Ciocoiu, 2010).

Ishikawa diagram was named after Kaoru Ishikawa, a Japanese who was the first quality control statistician using this diagram in the 1960's (Juran, 1999 & Wong, 2011 & Hekmatpanah, 2011 & Bose, 2012 & Doshi, Kamdar, Jani & Chaudhary, 2012 & Abraham, Dereje, & Lim, 2001). The authors used Ishikawa diagram has named it by Ishikawa diagram, cause-and-effect diagram, or Fishbone diagram (through this section these three different names used by authors were kept in originally format, and they are interchangeable). Typical use of this diagram is in the field of quality management in manufacturing industries (Wong, 2011 & Hekmatpanah, 2011). This instrument could be used for groups in problem-based learning or in self-directed learning situations. The number of 'fish bones' in the diagram could be vary, every single 'fish bone' could be split into smaller 'bones' to show the correlation of all probable causes to the presenting problem if necessary (Wong, 2011).

Fishbone diagram is an analysis instrument which provides a methodical way to observe the effects and the causes which make or contribute to those effects. The function of Fishbone diagram can also be used to indicate multiple cause-and-effect relationships (Watson, 2004 & Hekmatpanah, 2011 & Bose, 2012). The configuration of the diagram aids researches to think in a very methodical way. Some of the advantages of creating a Fishbone diagram are that it helps to define the root causes of a problem or quality features using a structured methodology, encourages group participation and make use of group knowledge of the process to identify areas where data should be gathered for further study (Balanced Scorecard Institute, 2009 & Hekmatpanah, 2011).

The design of the diagram looks like a skeleton of a fish. The indication could be simple, bevel line subdivisions which lean on a horizontal axis, signifying the distribution of the multiple causes and sub-causes. It could also be finished with qualitative and quantitative appreciations

(section 2.9.2 further explains the qualitative approach and 2.9.3 for quantitative), with names and coding of the risks which describe the causes and sub-causes, with elements which show their sequence and with other diverse means for risk treatment (Ciocoiu, 2008 & Bose, 2012 & Hekmatpanah, 2011 & Doshi, Kamdar, Jani & Chaudhary, 2012). Fishbone diagram can be applied to determine the risks of the causes and sub-causes of the effect, also of its global risk (Ciocoiu, 2008 & Hekmatpanah, 2011). The analysis usually comes along with other indication and establishing treatment priorities methods after Fishbone diagram (Ciocoiu, 2008).

Fishbone diagram can also be a visualization tool to identify the root causes of quality problems and summarize hidden causes for an effect or issue by classifying possible causes into categories (Chang, 2015 & Tague, 2005). According to American Society for Quality (2005), fishbone diagram and analysis usually assesses the causes and sub-causes of one specific problem and hence assists to find out all the indications of any business issue. Therefore, fishbone diagram would be an overall assessment of the causes of the focal problems as well as the revelation of the root causes (Balanced Scorecard Institute, 2007 & Bose, 2012).

Fishbone diagram is drawn by first identifying a main problem to be fixed and has been put on the head of the diagram while the causes are put as the bones and smaller bones are made as the similarity of the sub-causes (Bose, 2012).

Applications of Fishbone Diagrams

The vast application of fishbone diagram leads to no doubt that fishbone analysis is a very effective tool to sort out the causes of problems but there are some disadvantages stated in few literature. Bose (2012) claimed that fishbone analysis does not make clear the sequence of the causes. Ruhm (2004) said that fishbone analysis cannot fix the problem in reality because a problem might happen owing to some reasons but the extent or extremity of each reason cannot be the same. Watson (2004) thought fishbone analysis just a substance of consequences which unable to signifies details of the relevant cases. Ruhm & Watson (2004) both defined that the fishbone analysis detects causes under pre-defined categories only but not relate to causes to each other and to each category.

There are many procedures have been developed for diagramming problematical business circumstances through systematic conventions. Hennessey (1978) suggested using fishbone diagram to signify observable symptoms attributable to a few causes to be decided upon by the problem framing session participants. The fishbone structure is the tool of helping what is becoming known as the back step analysis of a problem. It is a practical aid to problem formulation in which one proceeds from a problem backward to its assumed causes. The search process of back step analysis involves writing down the observed problem. Back step analysis

is connected to the indication that it takes some variables to create an effect. Back step analysis is very responsive to group problem formulation; benefit could be added though making use of teamwork for brainstorming. Advantages can accompany any problem-framing means which entails a casual diagramming procedure. The fact is that most problem-framing methods try something of the kind is not purely coincidental. Lack of sufficient methodological control can be one of the disadvantages of back step analysis (Madu, 2012).

Ishikawa (1986) suggested that fishbone diagram helps people to think through problem causes (Hekmatpanah, 2011). This method combines brainstorming and a concept map. Identifying the problem; working out the main causes involved; identifying potential causes and analyzing the cause and effect diagram are the four major process steps, which are used to tackle many problems containing risk management in production and services (Dey, 2004 & Hekmatpanah, 2011). This instrument has been used to obstetrics, gynecology, emergency department and healthcare management (White et al., 2004 & Hekmatpanah, 2011).

Fishbone diagram is almost the infinite application in research, manufacturing, marketing, office operations and so on (Hekmatpanah, 2011 & Doshi, Kamdar, Jani & Chaudhary, 2012). The participation and contribution of everybody involved in the brainstorming process is one of its strongest effects. Solutions are established to correct the causes and improve the process as well as criteria for judging the likely solutions may contain cost, feasibility, resistance to change, consequences, training and so forth (Hekmatpanah, 2011). Testing and implementation could be continued upon the agreement of solutions from the team (Madu, 2012 & Hekmatpanah, 2011). Fishbone diagram are beneficial to analyze actual situations for the purpose of product or service quality improvement which is more efficient use of resources and costs can be reduced. Elimination of circumstances causing abnormal product or service and customer complaints and standardization of existing and planned operations are the advantages as well (Hekmatpanah, 2011).

Doshi, Kamdar, Jani & Chaudhary (2012) believe that Ishikawa diagram is very famous and generally used to improve quality and reduce rejection among many methods. It is very useful for identifying the possible causes of error or problem from altered prospective so it would be a proper management tool for making right decision to resolve problem.

Ishikawa diagram shows the causes of defect formation and assists calculating defect weights. It is an instrument for observing and detecting the processes of design, manufacturing, control, assembly and any other actions that take place in the product life cycle. It applied in graphically characterized a cause and effect relation which aids to separate the effects from causes of a problem and to recognize the complication of the problem. Ishikawa established the cause and effect diagram in which the analysis starts from the identified effect (e.g. defect, failure or another undesired situation) and leads towards the identification of all conceivable causes of

that effect. The cause-and-effect diagram is a graphical analysis of the effect of several factors and their interrelations affecting a definite quality problem and the analysis of the consequences (effects) initiated by these interrelations. This instrument was formed in order to diagnose the relations between customer requirements and the quality of the final product, helping the identification of the product attributes (Gawdzińska, 2011).

Fishbone diagram was applied in many divisions in order to structure, identify and look the big picture of the problem. Dhandapani (2004) used fishbone diagram and Pareto principles for software industries as well as Behnam and Alvelos (2011) applied for the tire industries in order to find the root causes that exist during retreading process (Abraham, Dereje, & Lim, 2001). Chang and Lin (2006) used the fishbone diagram for the analysis of the root cause in tanker storage accident. Abraham, Dereje, & Lim (2001) wrote that this instrument uses graphical way to relate the causes of a problem to the problem itself. The diagram focuses on the causes rather than the effect since there might be various causes for a specific issue and hence this tool helps to identify the root cause of the problem in a structured and simple way.

2.9.2 Multi Criteria Decision Making

Multi Criteria Decision Making (MCDM) is involved in many different research areas, including operations research, information systems, healthcare, manufacturing and SC, and other uses. A set of multiple criteria in decision making are typical in evaluating options. A complex problem has to be well structured to make best decisions. Magnitudes of scholars provide solutions that solve MCDM problems. Yu (1973) and Zeleny (1973) suggest the idea of using compromised solutions on different units to solve MCDM, Duckstein and Opricovic (1980) agreed to Yu and Zeleny and formalized the VIKOR method to solve MCDM. Hwang and Yoon (1981) proposed Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) is another method to solve MCDM. Yoon (1987) was able to use TOPSIS to reconciliation discrete compromise situations, and Hwang et. al (1993) illustrated the use of TOPSIS algorithm to solve a numerical nutrition problem. The above solutions require data collection that is beyond the scope of this study, while multi-domain data are either not easy to retrieve or not available to domain operators.

2.9.3 Analytical Hierarchy Processing

Analytical Hierarchy Process (AHP) is a quantitative model to incorporate qualitative data and quantitative analysis (Meade and Sarkis, 1998). AHP is a moderately general instrument for modelling strategic decisions; however its basic associations are prohibited for an integrated dynamic modelling of the environment would be the fundamental limitation. It also assumes that the system elements are not correlated and are affected by a unidirectional hierarchical relationship. The highest element of the hierarchy is the overall objective for the decision

model. The hierarchy breaks down from the general to particular attribute till a level of manageable decision criteria is fulfilled (Meade and Sarkis, 1998).

AHP is a decision-making instrument to define the general decision operation by decomposing a complicated problem into a multi-level hierarchical structure of criteria (Saaty, 1990; Wang, Huang & Dismukes, 2004). It is realized that AHP is an essential generic means and widely applied in different fields, especially for manufacturing areas. It is also believed that AHP could be an operative tool to assist human decision making because the hierarchic structure of AHP could reveal the natural tendency of human mind effectively (Wang et al., 2004).

AHP also is an extensively implemented decision support technique in management research, for instance, the applications of AHP could be found in evaluating risk factors in enterprise resource planning execution. AHP is a dominant tool in solving complex decision problems which was developed by Saaty. It helps analysts to consolidate the critical aspects of a problem into a hierarchical structure which similar to a family tree. Analysts could make the best decision with a clear rationale through decreasing difficult decisions to a series of simple comparisons and rankings, synthesizing the results then (Sevkli, Lenny Koh, Zaim, Demirbag & Tatoglu, 2008).

Using the AHP methodology, the decision problem is structured hierarchically at different levels with each level contains a fixed number of decision elements. The higher level of the hierarchy symbolizes the overall goal, while the lower level comprises of all possible choices (Partovi, 1994).

AHP is a theory of measurement aimed at dealing with measurable and intangible criteria which have been applied to several areas like decision theory and conflict resolution (Vargas, 1990). It is also a problem solving framework and a logical process for indicating the elements of any problem (Saaty, 1983). It involves three steps, starting with decomposing multifaceted problem into a hierarchy which contains some manageable elements. The next step is to use a measurement approach to set priorities among the elements. The final step synthesises the priorities of the elements to form the overall priorities for the decision alternatives. AHP is more objective than traditional decision analysis as it does not acquiring decision maker to make subjective judgements. A SC development project is a group effort and hence it is vital that a decision support tool intends to integrate group decision (Korpela, Lehmusvaara & Tuominen, 2001).

Analytical Hierarchy Processing in MCDM with Fishbone Diagram

Zhao et. al (2012) explained fishbone diagram does not determine causes importance, and the solution Zhao used was analytic hierarchy process (AHP). Zhao performed in his study safety risks of a subject and found priorities of the causes of such safety risk by using what he

described as “a combination of qualitative and quantitative, systematic, and hierarchical analysis method”. He used AHP because he referred fishbone diagram as decomposition of complex problems and AHP as a more comprehensive process which included decomposition, judgment, and integration which solves problem in a systematic way.

Zhao has identified the basic steps of AHP as follows:

(1) Build hierarchy model
(2) Perform pairwise comparison matrix
(3) Weight vector calculations
(4) Combine weight vectors

In addition to Zhao, many authors have used the AHP as supplementary tools to perform researches. Pourghasemi et. al (2012), for instance, discussed the application of fuzzy logic and analytical hierarchy process; Komac (2006) used multivariate statistics with analytical hierarchy process method. Logistics applications applying AHP is also uncommon, Min (1994) applied AHP in an international consolidation terminals study (Min, 1994) and Thompson (1994) applied AHP in the analysis of contract incentives distribution.

AHP starts with pairwise comparsion on a set of alternatives to a solution. Fechner (1860) introduced the pairwise comparison idea, and Thurstone (1927) agrees to Fechner and formally developed pairwise comparison as an analysis tool. Pairwise comparison study has not relate to MCDM until Saaty (2008) studied decision making with the analytic hierarchy process. Pairwise comparison is easy to perform and fit our study objective while SC practitioners, as noted in the semi-structured interview, usually have no control in the cause and source from uncontrolled domains in the SC, a comparison of impacts on the cause and source from the uncontrolled areas is easy to analyze, as the impacts are usually affect the domain with the said SC practitioner reside in.

Alonso et al. (2006) suggests AHP the use of pairwise comparisons to solve Multi Criteria Decision Making problems involving alternatives and criteria. He suggests the use of AHP, which uses a reciprocal decision matrix obtained by pairwise comparisons. AHP breaks down a general question into a hierarchy of sub-problems, which are easier to evaluate. Saaty (1990) suggests the most common evaluation of AHP involves mathematical normalization procedure which the study will follow this approach.

As AHP is based on study target answers, it has a qualitative tools to emphasize the consistency of the pairwise comparison answers given from the survey input. Generally, most authors consider consistency test of the pairwise comparison table is important. Karapetrovic and Rosenbloom (1999) announced various approaches to control consistency are AHP studies.

Kwiesielewicz (2004) discusses the how to spot inconsistent and contradictory judgments in pairwise comparison method in the AHP.

2.9.4 Interpreting AHP Solutions to MCDM Problems

MCDM problems and solutions are complex in nature, and the use of AHP will prioritize a solution for such problem. However, how to interpret the solution and setup policies requires experienced SC practitioners, and focus group studies would be a valid choice. Gill et al. (2008) considers interviews and focus groups are the most common methods of data collection used in qualitative research, while interviews can be used to explore the views, experiences, beliefs and motivations of individual participants, focus group generates qualitative data by use of group dynamics. They further explains that focus groups are used for generating information on collective views, the meanings that lie behind those views, and rich understanding of participants' experiences and beliefs. Agreeing to Gill et al., Stewart and Shamdasani (2014) explained that there are three ingredients in a focus group study. (1) The Purpose, (2) The knowledge of focus group members, and (3) the budget that influences the degree of specification. Focus group study performed is further documented in section 8.4.1.

2.10 The Literature and its Connection to this Study

Literatures have tight connection to most study methods, such as design science approach (discussed in section 4.3), as the basis of design methodology. The literature review not only provides background information relevant to the study, to provide the reader with information and a lens through which to view the rest of the study, but also treats the literature review itself as a research artefact to address a specific research questions (see section 3.3).

Various authors have commented on the use of the literature review. Gall et al. (1996) suggested that literature review plays six major roles in a research paper. Hart (1998) agrees with Gall, Borg, and Gall (1996), but also adds eleven additional reasons for reviewing the literature. The literature review, in addition to providing background for the reader, serves as the first artefact delivered by the design science methodology (discussed in depth in Chapter 3). Application of the framework by (Gall, Borg, and Gall, 1996; Hart, 1998) are linked up with the goals of the literature review, and are shown in Table 12.

Reasons for Reviewing Literature for General Research Papers Shortlisted for this Study	Major Reason for Literature Review Adapted
Gall, Borg, and Gall (1996)	
delimiting the research problem	Security Breaches in RIFD Life Cycle
seeking new lines of inquiry	
avoiding fruitless approaches	
gaining methodological insights	Design Science / Case Study Approach
identifying recommendations for further research	
seeking support for grounded theory	
Hart (1998)	
distinguishing what has been done from what needs to be done	Technical / User Management / Forecasting Approaches done, general integrated approach missing
discovering important variables relevant to the topic	Security Breaches can be measured in various domains
synthesizing and gaining a new perspective	
identifying relationships between ideas and practices	
establishing the context of the topic or problem	
rationalizing the significance of the problem	Significance of RFID Breaches in financial and non-financial means
enhancing and acquiring the subject vocabulary	Various such as privacy, RFID, SC.
understanding the structure of the subject	Yes
relating ideas and theory to applications	
identifying the main methodologies and research techniques that have been used	Kim et al.'s Multi-domain RFID Vulnerability model and list of security breaches by various scholars
placing the research in a historical context to show familiarity with state-of-the-art developments	

Table 12 Reasons for Reviewing Literature Mapped to this Study.

Adapted from Gall, Borg, and Gall (1996) and Hart (1998) and mapped to this study

Through the literature review, it emerges that there is no existing security policy and standards in worldwide practices. This study will supplement the literature by analysing the security breaches, SC members' attitudes to them and approaches to address them. Because of its central and important role as the source of many global SCs, PPRDLH provides a significant focus for research.

Extant research suggests the potential for developing a framework that can bring together wide-ranging directions of study. Such a framework can serve as a means to identify potential research gaps, and also to help build practical policy and standards that extend the academic to the practical realm.

In addition, it is evident that many authors have considered SC RFID security breaches in the context of single domains, even while SCs by definition are connected across several domains. A framework that considers the complexity of multi-domain SCs is needed but missing, this is especially true for companies in the SC buyer's domains, as they have to indirectly pay for all systems in the SC even for RFID systems owned by other domains, say the suppliers, who cannot guarantee system security.

3 Research Objectives

The research aims to reducing supply chain security breaches in a multi-domain RFID system by establishing an easy to use and robust policy framework covering leading-edge to trailing-edge industries. This is a complex question as requirements of first defining security breaches in RFID systems are needed but missing, and different supply chains could have multiple causes and sources of RFID security breaches. Three RQs are used to focus the study in order meet this overall objective. This Chapter considers the rationale and context of the objective and RQs.

3.1 Introduction

Research objectives specify what is to be achieved in a research project. They are set before the project beings and provide a framework to provide direction and set the scope of the project. They typically contain a hypothesis and/or a statement of purpose. Lyons (2017) defined six important characteristics in good research objectives; that they should be (1) brief and concise, (2) in logical sequence, (3) realistic, (4) described in operational terms (5) contain specific action verbs, (6) be static once research begins. The six characteristics were considered in establishing the objectives for this study.

Overall research objectives are supported by Research Questions (RQs). These provide scaffolding for the objective; by asking these RQs the objectives are achieved. Bordage and Dawson (2003) suggest RQs are the most important success factor of a study and a successfully written research question is the basis of the entire project. Extending the suggestions of Bordage and Dawson, Bryman (2006) notes that unclear research questions lead to unfocused research.

Deficiencies in RQs leads to problems in the research. Oki (2016) defines three types of failure in research due to RQ deficiencies. They may remain wholly or partially *unlearned* through the course of the study. They may be *unanswerable* due to their nature or lack of researcher's capability and resources. They may be *unfit*, lacking validity or reliability due to such factors as unsuitable data collected or invalid analyses.

Any of these three RQ deficiencies lead to unsuccessful (compromised) research, and might require a rewrite as the research reveals information and findings, where adjustments will be

required to further direct the research to the correct path. In practice, defining RQs in a research project is an iterative process, where RQs help provide the focus on where the research should start and based on the answers to these, whether the objectives will be achievable, and whether they must be revisited.

RQs may also play a role in approval, funding and resource allocation. For example, ethical approvals, time requirements, and resource allocations in this study were sought before this study started (Bell, 2014). This study has three RQs that represent questions to be asked to achieve the research objectives.

3.2 Research Objective

As evidenced from the literature reviewed and discussed in section 2.5, RFID systems are valuable for SC in a wide range of areas including areas of inventory management, tracking, payment, and transportation (tabulated in Table 5 and discussed in section 2.5.2) as it provides benefits (discussed in section 2.5.5), along with its high utility such systems carry commensurate vulnerability (discussed in section 2.7.8) and prone to security threats (discussed in 2.6). This situation is more complex in multi-domain SC RFID systems that serve modern global SCs (discussed in 2.7.7), where vulnerabilities in one domain could be difficult to tackle solely from other domains. Vulnerabilities and responses to reduce them have predominantly been addressed by means of technical research focusing on the hardware and software. There has been less work on policy frameworks that operate across the SC in its entirety.

This suggests a valuable research gap that can reduce the overall vulnerabilities associated with RFID use, and therefore increase the net benefits of using this technology. Based on these factors the Research Objective for the study is:
Development of a Multi-Domain RFID Security Model for Global Supply Chains

In order to test the model, a framework will also be provided as a byproduct of this thesis. This framework will enable logistics practitioners to adopt the framework easily. Therefore, in addition to the research objective, this thesis will perform: ***Development of a Multi-Domain RFID Security Model for Global Supply Chains, and a Practical Framework for Model Adoption***

This objective is met by answering the following 3 RQs:

RQ1: What are the types and sources of multi-domain RFID security breaches across the SC?

RQ2: In what way can current multi-domain security models be extended to address RFID security breaches across the SC?

RQ3: What policy framework will reduce multi-domain vulnerability?

3.3 Justification of RQs

Research Question 1 (RQ1):

What are the types and sources of multi-domain RFID security breaches across the SC?

Section 2.6 discussed the list of RFID vulnerability as summarized by Rotter (2008) and his list can be used as a starting point of types/sources of multi-domain security breaches apart from the vulnerability human tracking (discussed in section 2.6.6). RFID security vulnerability in SC therefore consists of eavesdropping (2.6.1), relay attacks (2.6.3), unauthorized tag reading (2.6.4), tag cloning (2.6.5), replay attack (2.6.2), tag content changes (2.6.7), malware (2.6.8), RFID system breakdown (2.6.9), tag destruction (2.6.10), blocking (2.6.11), jamming (2.6.12), back-end attacks (2.6.13).

However, are all of these attacks are applicable to RFID systems in SC? It is clear that the list needs to be updated to fit specially for SC, which none of such list exist, which is the research gap for RQ1. This is a prerequisite for studying the phenomenon as otherwise RFID security breaches count cannot be accumulated and analysed. The study shortlists and adds newer security breaches to the existing work of various scholars in order to provide a comprehensive list of security breaches. It should be noted that RQ1 considers breach incidents and vulnerability together, since they are related. It incorporates aspects of Kim et al.'s multi-domain SC model in order to categorise RFID security breaches across the SC.

The outcome list would provide a new model, given by the name Multi-Domain SC RFID Vulnerability (MDSCRV). The new model might not fit all SCs, and therefore a further study of MDSCRV in different SCs are needed. The study of LEI and TEI can provide a wide spectrum of SC with RFID applied has to be chosen. In terms of RFID usage in SC, leading use of RFID applies RFID from end-to-end SC, and has a longer RFID lifecycle. On the other hand, trailing edge uses of RFID could be just applying RFID in one single domain. For example, a retail shop applies RFID to their products for tracking and tracing purposes. The two industries chosen are the pharmaceutical and jewellery industries. The value of goods in both industry are important (non-financial) and high (financial), and the SCs are complex (as discussed in section 1.11). The two industries will be used to benchmark RFID security breaches against the MDSCRV model. As the two industries have high significance in global trade, in terms of financial and non-financial implications (discussed in 1.11), a check list of all of these vulnerabilities would be useful for SC practitioners to implement security measures in protecting their SC. There is a gap in current literature where RFID security breaches study are only based on one single industry but never compare multiple SCs.

As per chapter 2 suggests the financial importance of PPRDLH of Mainland China is a world's factory and has high significance, the jewellery industry and pharmaceutical industry are the two selected industries because both are important SCs, have financial and non-financial implications; however, in terms of technology, one is leading and the other one is trailing. Pharmaceutical SCs, on one hand, have applied RFID end to end since raw material and production to end consumer, but jewellery SCs have only applied RFID recently and most of them only have applications in the retailing areas. In addition, as discussed from chapter 2, the financial and non-financial implications of SC can be well demonstrated by the two types of goods. While jewellery has higher impact on financial implications, pharmaceutical products have higher impact on non-financial implications.

Different SCs have different characteristics as discussed by authors over the past twenty years as discussed in section 1.11.4. However, why would RFID applications in SCs be different even for same cargo values? Is there categorization of SC that leads to RFID applications? Would RFID security breaches be different in different SCs?

Research Question 2 (RQ2):

In what way can current multi-domain security models be extended to address RFID security breaches across the SC?

While the preliminary model could advise solutions to RFID security breaches, more complex industries with multiple security breaches cannot be solely explained from the preliminary model. Security vulnerability from any domains can cause RFID security breach in other domains. Considering solely the vulnerabilities without which domains the vulnerability arose cannot tackle the RFID security breach problem entirely.

Therefore, the preliminary model needs to be extended in order to capture the problem entirely. Current academic papers only consist of study for single domain RFID systems, or for studies that have considered the multi-domain property of the SC, only some RFID systems (for example only EPC tags have been researched by Kim et al., as discussed in section 1.8). A framework that can cover both long and short RFID lifecycle for all RFID systems are required but missing.

In particular, jewellery industry has a relatively higher financial implication and the pharmaceutical one inclines more on non-financial implication, hence the security breaches of these two industries could be different. It will make it easier for future studies on RFID security breaches of a SC to be based on the results presented in this study by determining whether the SC has higher financial or non-financial implication. Furthermore, if a relationship of RFID security breaches to SC and various types of financial implications categorization can be drawn,

those RFID security breaches of other categorization of SC can also be determined, resulting in the RFID security breaches being directly identified according to its specific categorization of SCs. For example, for high financial implication SCs, RFID security breaches of this SC tend to be higher as well.

Research Question 3 (RQ3):

What policy framework will reduce multi-domain vulnerability?

Causes and sources of the RFID security breaches are also important for dealing with RFID security breaches. A set of RFID security breaches could come from the same RFID security cause or source. Once this has been studied in future scenario, dealing with multiple cases of RFID security breaches identified in this study could be done by just resolving one or two cause or source of RFID security breaches, which will be easier than dealing with multiple RFID security breaches themselves.

While the nature of SCs can be categorized, the RFID security breaches in SCs can also be identified and categorized. If such categorization is possible then in the best scenario future RFID security breaches can be directly identified by the category of SC. Say for example, RFID signal jamming is likely to occur as a possible RFID security breach for SCs that has products directly interacting with end consumers.

For LEI, the situation is more complex, and multiple domains vulnerabilities should be considered. For example, vulnerability issues in domain A could lead to security breaches in domain Z in a SC with solutions found by SC practitioners in domain Z, however such solutions cannot be applied due to the domains are not directly associated. Therefore, solutions to multiple RFID security vulnerabilities need to be prioritized, and is missing from any literature. To the best understanding this is the first study ever tried to tackle such problems.

3.4 Discussion

Like all the above-mentioned academics, the aim of the research is to solve the vulnerability problem of RFID. RFID has the advantage of being fully automatic and works without line of sight. However, these would also expose the weakest areas in security. If RFID security breaches are eliminated from the SC, the potential of RFID in reducing human errors and performing automated tasks are unlimited. A good research methodology (discussed in section 4.3) is able to solve the vulnerability problem.

3.5 Academic Studies

These researchers come closest to recognizing SC complexity with respect to RFID security, but have not addressed the real world complexity of global SCs for a product and its associated packaging and transportation time during its existence throughout that SC.

As evident from these issues, backed up by the literature being reviewed, the existing models of SC RFID vulnerability are far from sufficient. Lehtonen (2008) for instance, only focused on a system that is based on a limited part of the SC, where connections to non-predefined SC partners were not considered. Ideally, a study should focus on the RFID from planned product manufacturing to the ultimate destruction of the RFID tag downstream in the SC after product consumption; that is a multi-domain system (Kim et al., 2007). Kim et al.'s multi-domain model attempts to deal with the situation, but it is too convinced that RFID tags only appear in the EPCGlobal format and therefore missing out a generalized study considering all different types of RFIDs.

What has been omitted from the current research is a model that explains RFID security with the SC partners with whom a business deals. This leads to questions of RFID security implementation guidelines and checklists, and the addition of "timeframe" as a conceptual structure on which RFID security enforcement can be focused.

Some researchers have tried to tackle only this problem with a purely technical approach (discussed in 2.7.1); however, as a product moves along the SC, from the time before the factory manufactures the goods to after the ultimate consumption by the consumer, there is little research on what kind of security requirements is needed. Point-in-time approaches based only on technical issues, hence it certainly cannot address the security issues in this multi-domain environment. Goods can travel in the SC in two directions (e.g. reverse logistics) and can skip certain parties (e.g. online shop and direct selling). Unnecessary information broadcasted in the SC could cause data "leakage" or flood systems with invalid and irrelevant data. These serious "RFID information pollution" questions have to be well addressed before RFID tags are distributed in consumer products in a worldwide scale.

These questions cannot be addressed easily by any of those models; even that of Lehtonen (2008) or Kim et al. (2007). Development of a model that addresses these complex real world issues could be used to effectively identify security concerns of SC partners, focusing on the attack vectors of RFIDs used through its lifespan, and be used to develop a practical security framework that can be shared by members across the SC.

The significance of this research is highlighted by the increasing amounts of sensitive data stored in the RFID systems as the use of RFID is forecasted to grow exponentially at 33% per

year at least until 2018 (Gartner, 2003). Major security issues including item track and trace (Swedberg, 2003), inventory monitoring and control (Lewis, 2005), asset monitoring and management (Hsiao et al., 2018), electronic payment (Kourouthanassis, Koukara, Lazaris, and Thiveos, n.d.), access control (McCullagh, 2003), anti-theft (Colvey, 2003), anti-tampering (Ward, 2006), and anti-counterfeit (Handfield and Nichols, 2002) are all sources of, and impacted by, whole-of-SC security concerns. These issues will contribute to major financial and other negative impacts if security vulnerability is not addressed.

As Lehtonen (2008) shows, due to decreased controls between SC domains, the problem is further magnified, and this is likely to increase as SCs become more complex and the goods are more globally distributed. Academic theorists have tried to provide model-based or technology-based solutions but in practice an operating and policy framework is needed to provide accepted rules that ensure security principles are followed.

The limited pool of current literature can be adopted to examine the possible vulnerability of RFIDs and build this operating and policy framework. This model will be constructed and used to highlight the points and types of security vulnerability and estimate the percentage coverage of such points against overall security breaches. The results from the model will be beneficial to companies (especially PPRDLH factories that export to world market) who wish to implement security measures.

The significance of this result would be its crucial contribution to a safer production environment in factories in China. Buyers from overseas including US and EU will enjoy and be rest assured of all items produced are tagged with secure RFIDs along with a secured operation framework, reducing direct and indirect financial impact of data and products, including the above mentioned example RFID sealed containerized products and terrorist attack weapons.

3.6 Summary

Review of the literature justifies the objective as it reveals gaps that this research addresses. The research questions have been drafted to align with and completely consider the research objective. The process of aligning the RQs with the objective, and the research methods used in addressing them are arguably *learned* questions, they are *answerable* because scope and terms are well defined. Finally, the RQs are *fit* questions, as data collected according to the methodology chosen was able to answer the RQs. The methodology is explained in the next chapter; and data collected in chapter after next.

4 Research Approach

Research methodology guides the researcher to collect samples, data and subsequently find a solution to a problem. Research methods are not chosen arbitrarily but require justification based on paradigms and methods suggested by various philosophers. Research design, including plans for data collection, measurement, and analysis provides a structure and overall strategic plan for the overall research project

4.1 Introduction

Research Methodology is important to a research study. Merriam-Webster Dictionary (n.d.) defines the term "methodology" as "a body of methods, rules, and postulates employed by a discipline", and "the analysis of the principles or procedures of inquiry in a particular field". Maxwell (2012) considers research methodology to be the approach to discover the result of the RQs. Researcher uses different criteria for solving the RQ (Voss, 2002) and different methodologies have been considered when choosing the research methodology for this study, and the justification will be provided.

4.2 Research Paradigms and Methodologies

The worldviews that researchers subscribe to, and their beliefs about the nature of 'truth' and how it is established are the backbone of modern research philosophy (Saunders, Lewis, and Thornhill 2009). Many different scholars have tried to describe research philosophy, and two key primary types are summarized by Chua (1986), Hussey and Hussey (1997), and Mingers (2002) as "Positivism" and "Interpretivism" philosophies. There are also four different types of assumption, operating in research form an important basis of the research and might affect research hypothesis, data gathering, and certainly results as well.

4.2.1 Characteristics of Paradigms

Candy (1989) suggests paradigms can be grouped by their characteristics into three main taxonomies, namely Positivist, Interpretivist, or other paradigms (including critical paradigm, discussed in 4.2.2). Positivist and Interpretivist philosophies differ in the perceptions of reality. Positivists perceive reality and the existence of the physical world as objective phenomena.

Interpretivists believe that reality is a subjective phenomenon formed in the minds of individuals and generates meaning within the physical and social environments.

Many authors agree with Candy, Chua, Hussey and Hussey, and Mingers, and further suggest other research philosophies. Examples include *Realism research* (Saunders, Lewis, and Thornhill, 2012 and Novikov and Novikov, 2013), *argumentation* (Van Eemeren, Grootendorst, and Eemeren, 2004), *Critical Theory* (Stahl and Brooke, 2008) and *Design Science* (Venable, 2010).

Positivist Research

Positivists believe reality is stable and can be described from an objective viewpoint (Levin, 1988) and therefore their philosophy of research pre-assumes the existence of an objective world without the perceptions of its social actors. In positivism there exists an objective reality that has measurable and tangible properties, and is measured and described using methods independent of the researcher (Myers, 1997). Positivist research usually starts by making assumptions and then evidence is sought for propositions, conducting measurement on quantifiable variables, testing hypotheses, and drawing statistical results from representative samples to the research subject. Positivist philosophy research consists of studies that can be measured, quantified and determined based on reliable data.

There is a limitation to positivism, as all knowledge is based on transitional conjectures and can be changed as new information emerges that contradicts established beliefs (Lynch and Jarvis 2008). Therefore, positivist research accepts that all findings based on empirical evidence are imperfect and subject to errors and changes (Phillips and Burbules 2000). In addition, positivists believe existing knowledge can be improved by examining smaller parts of subjects which form additively, into a bigger reality. Such examination can be done typically by means of quantitative instruments, such as structured survey questionnaires, scientific apparatuses, measuring devices. Repeated experiments and surveys of smaller parts of subjects forming arguments of larger reality are very common in positivists' data collection in the field of social science.

Interpretivist Research

Interpretivist researchers argue that all individuals continually seek to make sense of the world in which they live and therefore assert that reality is a perception from social constructions such as language, shared meanings, documents, tools, artefacts and consciousness. As such social context, meanings and experiences of individuals evolve due to ongoing social negotiations, therefore reality is not a static phenomenon. Thus interpretivist researches gather data by listening to participants in a study in the context of social settings, since dynamic reality exists

in the minds of individuals with the impact of cultural influence on the experiences of reality in research.

Interpretivist research does not emphasize predefined dependent and independent variables and is focused on context and process. Qualitative instead of quantitative data is more likely to be used to analyse perceptions and build theories, rather than just test them. This approach is very common in business research topics since business is fundamentally a human construct with interactions.

When dealing with the study of management information systems in the context of organisations, one cannot omit organizations, their culture, management and the actions of individuals (Pather & Remenyi, 2004). Olson (1995) explains that information system researches features both social science and a view of the world from the viewpoint of the actors within it (Olson, 1995).

Balancing points of philosophical view are emphasized in many studies. This includes Trauth (2001) who suggested that researchers must define the studied areas that are being treated as important, balancing those getting the most attention and also those getting less. Moreover, while research is taking place, researchers will develop knowledge of the subject and also a viewpoint (Janesick, 2000).

The researcher's philosophical perspective affects the process of enquiry, so it is not possible to obtain value-free data (Fielden, 2003; Krieger, 1991; Walsham, 1995). Researchers could be resultant bias (Krieger, 1991) and it is important to highlight the interaction between the researcher and the subject studied (Amaratunga et al., 2002; Myers, 1997), and to understand the philosophical approach taken in order to interpret the answers research provides.

Other Research Philosophies: Realism, Argumentation, and Critical Theories

Realism research suggested development of knowledge is a scientific approach independent from the human mind. Saunders, Lewis, and Thornhill (2012) coined this "direct realism", suggesting that the world is portrayed through personal human senses. On the other hand, Novikov and Novikov (2013) argue with Saunders, Lewis, and Thornhill (2012) that the real world is experiences by humans through sensations, and therefore the world portrayed could be deceptive. Such studies are named as "critical realism". Critical realists recognise the importance of human constructs (for examples organisations) as themselves influencing reality.

Toulmin (1958) recognized argumentation as a study that builds knowledge based on a process of Claim, Data, Warrant, Backing, Rebuttal, and Qualifier. *Claim* is the conclusion with facts proving it as the *data*. *Warrant* is the bridge that gives the connection of data with the claim,

and such warrant has credentials named as *backing*. *Rebuttal* is the exceptions to the claims and *qualifier* is the level of certainty. Some studies use these arguments, for example, a rebuttal is used to oppose thesis statements showing that opposing side's viewpoint has been considered and find it to be weak or invalid.

Instead of focusing on human sense and constructs as critical realism scholars believe, critical theory scholars assess by social sciences and the humanities knowledge. Horkheimer (1937) defines *Critical Theory* as a philosophy in which understanding the society directly contributes to outcomes. It should always be improved by considering major social science studies, including geography, economics, freedom, power, social control, values, sociology, history, political science, anthropology, and psychology. Stahl and Brooke (2008) regards critical theory as a tool of discharging studies in social and ethical responsibilities, Orlikowski and Baroudi (1991) agree with Stahl and Brooke and further exclaim that studies are ever changing in nature and such changes cannot be neglected.

4.2.2 The Four Dimensions of Assumptions

Creswell (2009) agrees to these scholars with respect to positivist, interpretivist, and other researches, and further suggests four dimensions in which they may differ: Ontological, Epistemological, Axiological and Methodological.

The Ontological Dimension

Ontology is about the nature of reality and assumptions made by researchers in regards to how the world operates. Objectivist ontology is the argument put forward by positivists. In this, reality is an objective phenomenon, which exists independent of human perceptions and social constructs and can be measured, studied and investigated. Subjectivist ontology on the other hand, represents the interpretivisit argument, and suggests that reality is a social phenomenon and can only be studied by examining the individuals in the situation by listening to participants in the context of social settings.

The Epistemological Dimension

Epistemology relates to how appropriate knowledge about reality should be established. From the descriptions of positivist and interpretivist given above, a positivist would establish knowledge based on a measurement, examination, or analysis on objective data, while an interpretivist would build knowledge from a perceived, interpreted and inferred points of view from minds of individuals. In the epistemological dimension, a positivist would invalidate an interpretivist's knowledge and similarly the interpretivist would invalidate the positivist's knowledge, on the grounds that these were built on inappropriate knowledge from their respective point of view.

The Axiological Dimension

Axiology examines the correlation between the subject of the research and the biased values of the researcher. “Value-laden” indicates that an investigation being prejudiced by the beliefs of the researcher with high potential for bias, while “value-free” means the investigation is independent of the predispositions of the researcher, with lower potential for bias. Heron (1996) argues that values guide reason of all human action. For example, an interpretivist study with data collected through semi-structured interview suggests that researches value personal interaction highly than anonymous survey data.

The Methodological Dimension

Methodology is the actual process of the research, and is guided by ontology and epistemology. It is important for methodology to be clearly detailed and is therefore discussed in full in chapter 4.3. Research methodology is determined by many criteria, such as whether the research object exists, types of data needed to be collected, interpretivist or positivists research. Large scale surveys, structured or semi-structured interviews, disguise or non-disguised interview are all concerns of research methodology.

4.2.3 Research Methodologies

Research Methodology is the backbone of a research study. Galliers (1991) suggests fourteen different common research methodologies, and Pervan (1994) reported that Alavi and Carlson (1992) uses a hierarchical taxonomy to describe eighteen research methodologies, indicating their suitability for positivist and interpretivist research. With the variety of research strategies, researchers need to carefully study them before engaging one type of research strategy over the others. The research strategies have been studied and the findings are shown below, explaining and confirming the research strategy being used in this study.

Laboratory Experiments

A researcher adopts laboratory experiments to locate particular relationships between a small numbers of variables, which will be studied intensively through a planned laboratory condition by quantitative analytical techniques, in order to make general statements that can be used in real-life situations; but this method’s weakness is "limited extent to which identified relationships exist in the real world due to oversimplification of the experimental situation and the isolation of such situations from most of the variables that are found in the real world" (Galliers, 1991).

Subjective/argumentative research, for instance, hermeneutics and phenomenology entail researchers to set an innovative or theoretical stance instead of being a spectator. It is a worthwhile practice which new theories can be created, different ideas generated and then

tested. Nonetheless, a high possibility of researcher bias would exist in an unstructured and subjective form of research.

Field Experiments

Field experiments prolong laboratory experiments into reality of organizations and hence accomplish larger realism and lessen the extent to which circumstances that can be critiqued being affected (Gerber and Green, 2000). Actually, it is challenging to recognize organizations that are ready to be trialed and even to attain enough control to make reproduction feasible.

Surveys

Fink (2003) expressed that a researcher utilizes surveys to acquire data about practices, circumstances or opinions within a particular time from questionnaires or interviews. Implications could be made from this data regarding current relationships by using quantitative analytical technique. Researchers may study more variables at one time via surveys when compared with laboratory or field experiments, while data could be collected about real world environments. Weakness of surveys is that it is actually hard to realize interpretations concerning the reasons or processes involved in the occurrences surveyed. Also, bias might come from the possibly self-selecting nature of respondents, the time slot when the survey is conducted and the researcher him/herself via the design of the survey.

Action research is a form of applied research where the researcher endeavours to develop outcomes or a solution which is beneficial to researchers and evolves theoretical knowledge simultaneously. Researchers intend to make practical and emancipatory outcomes, re-inform existing theory in the field studied by intervening problems directly. Action research is the same as case studies, which are tough to generalize findings because it is generally constrained to a single organization. Also, different researchers might explain actions contrarily. The personal beliefs of the researcher are important because the researcher always intervene directly.

Case Studies

Case studies usually try to describe relationships which occur in a single actual organization (Walsham, 1995). Positivist and interpretivist are different nature in case studies; it depends on the methodology of the researcher, who could gain more features of reality through observation. More variables would be analysed when comparing case studies to experimental and survey research. Weakness of case studies is that it is difficult to generalize findings which is usually limited to an organization. It is also hard to search similar cases with similar data to analyse in a statistically meaningful way. Besides, different researchers might have different explanations of the same data which will increase bias of the research analysis.

Theorem Proof

Rosenbaum and Rubin (1984) used theorem proof to reduce bias in observational studies using statement that has been proven, in a recessive manner, based on previously established statements and theorems. The proofing of additional theorems, or justifying the truth of previous theorem statements, widens the human knowledge. This is the study by theorem proof. Usage of theorem proves include mathematical conditional statements by building hypotheses or premises. It is worth to note that scientific theory cannot be proved because it makes predictions and is tested by experiments.

Forecasting and Future Research

Makridakis et al. (2008) believes forecasting research can predict possible future events using regression, where time series analytical techniques is the fundamental concepts of forecasting research. It is a valuable research method which intends to deal with the prompt changes taking place in IT and forecasts the effects of these changes on individuals, organizations or society. However, this method is full of troubles connecting to the complication of reality events, the random nature of prospect variations and the absence of information about the future. Researchers are unable to shape factual visions but can create scenarios of likely expectations and influences under these probable conditions.

Simulation and Role / Game Playing

Dormann et al. (2013) defines the study of simulation as "copying the behaviour of a system". It is used when problems are hard to solve analytically, and where it often contains the introduction of random variables. It is the same as experimental forms of research that is challenging to make a simulation appropriately truthful, which is similar to reality events.

4.2.4 Research Instruments

Variety of research instruments include *questionnaire*, where set of written questions on a sheet with empty spaces provided for respondents to openly reply to the questions, and are most useful when a small amount of clearly defined facts from a large number of people are needed. Interviews, on the other hand, can be structured, semi-structured, or unstructured. A *structured interview* has questions wording and sequences are same on all interviews. *Semi-structured interviews* allow interviewer to alter the sequence of the questions to obtain more information after important questions are asked initially. *Unstructured interviews* are list of topics only and respondents can freely express ideas. *Focus groups* can explore a new issue in monitoring and evaluation studies and participants can talk to each other, under the control of a facilitator. *Observation* method involves watching and record of research target, and

finally *document analysis* base research on reliable information without interacting with the research target (Cooper et al., 2006).

4.2.5 Addressing Research Bias and Validity

Research bias is a process where the researcher has influenced results of his/her research with or without knowledge or awareness to it. Examples of research bias are gained from experimental error or calculation without taking into account of all possible variables. Some other biases are resulted from subjects being studied are selected without representation of the entire population concerned. As bias exists in the researching process, qualitative research results are more dependent on experience and judgment compared to quantitative research, therefore, the bias problem must be identified and avoided in qualitative researches.

Identifying and Avoiding Bias in Research

Dictionary.com (n.d) defines bias as "any tendency which prevents unprejudiced consideration of a question". Merriam-Webster.com (n.d) further explains bias in the research concept, and emphasizes that research bias occurs when "systematic error [is] introduced into sampling or testing by selecting or encouraging one outcome or answer over others". In general, research bias must be carefully considered since it applies to all the steps in design science research. For example, study design, data collection, data analysis and building new artefacts from each of the above steps. Pannucci and Wilkins (2010) had the idea that bias is not a dichotomous variable and addressing bias cannot be simply limited to simple question of whether bias is present or not. Instead, any degree of bias has to be prevented by proper study design and implementation.

Bias During Study Design

Yin (2002) alerted bias in the study design should be minimized. It relates to research paradigms (discussed 4.2.1), assumptions (discussed 4.2.2), methodology (discussed 4.2.3) and instruments (discussed 4.2.4), and must be well considered and chosen for an unbiased study. Apart from the study design, bias is also introduced during the study performed. For instance, Sarniak (2017) further defined three different types of bias, namely the Selection bias, Research bias, and Respondent bias.

Selection Bias

Selection bias occurs while the study population is being identified. Common issues include study population not clearly defined, accessibility, reliability, and interests in developing specific (often biased) outcome.

Respondent Bias

Respondent bias includes four major biases resulted from respondents, including the acquiescence, social, habituation, and sponsor biases. Acquiescence bias is the act of "yea-saying" or the friendliness bias. Some respondents have tendencies to agree with the moderator.

Social desirability bias refers to respondents trying to answer questions they think will be best accepted and liked (Dodou and de Winter, 2014). Respondents will report inaccurately on questions that they fell too sensitive or personal to themselves.

Habituation bias happens when respondents tried to provide the same answers but worded in different ways. Vaney et al. (2008) explained this phenomenon as a biological response, where respondents' brains habituate or go on autopilot to save energy when responding to studies. In this case, respondents often show signs of fatigue and complain questions seem repetitive.

Sponsor bias happens when respondents is suspicious of the sponsor of the research and biasing their answers to reflect their opinions to the sponsors. There is no favor or unfavor answers relative to the sponsors for the bias, as views are on respondents' core beliefs to the sponsor.

Researcher Bias

Confirmation bias occurs when a researcher uses respondents' information to confirm hypothesis or belief (Nickerson, 1998; Rabin and Schrag, 1999). In this bias, the researcher would weigh responses higher for those that confirm their hypotheses and neglect reponses that disprove them. Some researchers remember better supporting responses and forget other points, without awareness.

Leading questions and wording bias is similar to confirmation bias with the same objective: to have the respondents confirming the researcher's hypothesis. This is achieved by putting words in respondent's mouth by questions leading to such words.

Culture bias is the assumptions about motivations of respondents based on the researcher's cultural lens. The act of judging another culture that are different from culture values of the researcher is coined by the term Ethnocentrism (Pirkey, 2015).

Question-order bias is the bias introduced from the sequence of the questions. For example, asking the respondents to name top three RFID security breaches and then to rate their severity

in Likert scale[29] could have the first RFID security breaches level affect the latter two; the respondent could rate the first one, and the latter two were responded by comparing the first responded severity.

The halo effect is described as respondent's tendency to response in an influenced opinion due to responses in another area. This is a common bias and a wide magnitude of studies have been performed by academics for halo effect due to many areas such as social desirability (Krosnick 1999; Mick 1996), extreme response style (Greenleaf 1992; O'Donovan 1965), positive and negative affectivity (Baumgartner & Steenkamp 2001), and leniency (Podsakoff et al. 2003). When halo effect happens, respondents may respond to a certain topic positively overall compare to other topics.

4.3 Research Design of this Study

With the consideration of the various research paradigms and methodologies in section 4.2, design science methodology is chosen to be the research methodology for this study, because the design science research paradigm is the backbone of this study. Design science methodology focuses the central role of the creation of the innovative artefact (Weber 1987; Orlikowski and Iacono 2001; Benbasat and Zmud 2003), the RFID security framework, to solve problems in real-world, Multi-domain RFID security breaches. The problem shares characteristics of "wicked problem" as defined by scholars Rittel and Webber (1984) and Brooks (1987), which can be solved by design science methodology. Wicked problem has the characteristics of:

- unstable requirements in environmental contexts which are ambigiously defined,
- complicated relationships within problem subcomponents,
- design artifacts and design processes can be amended,
- human creativity and teamwork for solutions are needed

4.3.1 Research Paradigm of this Study

Venable (2010) believes most researches are paradigms that can be categorized as positivist, interpretivist, theoretical-argumentative, critical and design science. This research uses a design science approach, as Simon (1981) refers natural science as explanation of how and why

[29] A 5 or 7 point ordinal scale developed in 1932 by Rensis Likert. Respondents' attitudes are measured with regards to the degree which a statement is being agreed or disagreed

things are, where design science is concerned with developing artefacts to achieve results. Agreeing with Simon, March (1995) mentioned that human goals can be achieved by design science, offering prescriptions and then creates artefacts that represent those prescriptions. Natural science, on the one hand, tends to be basic research, while design science, on the other, has a higher tendency to be applied research. This research will build an RFID security framework and in turn evaluate its performance, while application of the model is not in the scope of this research, hence the research is design science oriented.

Design science attempts to create things that serve human purposes and can be categorized into four types: constructs, models, methods, and implementations (March, 1995), of which the two basic activities are "build" and "evaluate". Building constructs an artefact and evaluation determines the performance of the artefact. Hevner (2004) further explains that IT artefact can be evaluated quantitatively by optimization proofs, analytical simulation, and quantitative comparisons with alternative designs, should be done using design science research. In the evaluation process, one should ask the basic question "How well does it work?" (March, 1995) and metrics should define what the artefact tries to accomplish. In this research the deliverables match the design science actions by March (1995) with details listed in Table 13. The rating obtained from the model will be compared against the RFID security breached incidents that would draw analysis to the RFID security model.

March (1995) design science research actions	**Deliverables in the research corresponding to the actions**
Build	RFID Security framework with elements drawn by investigating case studies
Evaluate	Evaluate with security flaw by following life cycle of RFID

Table 13 Deliverable of the research corresponding to March (1995) design science research actions

4.3.2 Research Methodology of this Study

Research methodology helps this study to describe, explain and predict phenomena of their research. The research design will be based on design science, by iteratively building artefacts the RQs will be answered through the research process. Design science is the best fitting methodology as artefacts are iteratively built on SC environment, which is a "wicked problem". SC environments are ever changing due to business changes. For example, United States President Trump started trade war with Mainland China dramatically changed the SC landscape[30]. SC problems are complex and involves teamwork as it is full of dependent and interdependent companies. Solutions are always critical, flexible, and adapt to changes, as fast

[30] Reported by Fortune Magazine, on April 2nd, 2018.
http://fortune.com/2018/04/02/china-tariffs-128-us-products/, last accessed June 2nd, 2018.

response SC systems are well preferred (Cheng and Choi, 2010). Along with design science, case study approach is the most appropriate research methodology due to question asked and the environment of study.

Benbasat et al.'s (1987) comprehensively defined the conduct of case research and identified a study is made possible by case study research.

- natural setting of phenomenon must be studied;
- "How" and "why" questions should be studied by the researcher to understand the nature and complexity of the processes;
- Research should be performed in areas where only few previous studies exists.

There is no standard way to define a case study. Scholars (Benbasat et al., 1987; Yin, 1984; Bonoma, 1985 and Kaplan and Duchon, 1985) have tried to define case study as "a phenomenon in its natural setting, employing multiple methods of data collection to gather information from one or a few entities (people, groups or organizations). The boundaries of the phenomenon are not clearly evident at the outset of the research and no experimental control or manipulation is used."

Yin (2002) further explained that a case study based approach seems to be more appropriate to address the above research objectives at each domain of SC. Yin (2002) has referred case study to empirical inquiry that tries to understand contemporary phenomenon, in cases where boundaries between phenomenon and context are not established. Case study research method is selected because (1) the research environment is not controllable – relevant behaviors in the multi-domain SC practitioners cannot be manipulated, and (2) the research environment is a contemporary business situation – where relevant persons are alive to report. Benbasat et al. (1987) also supports the use of case study approach in studies whenever there is a need to focus on contemporary events or phenomena in a natural setting, particularly if there is no strong theoretical base for the research.

Mini case studies are also increasingly used in business studies (IBS, 2018). Kralsson et al. (2016) described mini cases have advantages of providing comparison among mini cases and critical analyses can be performed by utilizing various mini-cases scenarios, especially when there is no definite answer to a specific problem. Agreeing to Merriam (1998), Kralsson et al. further concludes "that reality is not an objective entity; rather, there are multiple interpretations of reality" (1998, p. 22). This original idea was developed by Stake (1995, p.108), that "there are multiple perspectives or views of the case that need to be represented, but there is no way to establish, beyond contention, the best view" (Stake, 1995, p. 108). Mini-cases gives a comprehensive view to the research question.

A key issue in designing case study research is the number of cases included. Lee (1999) advises more valid and generalizable multiple cases contribute to a better study, though there are times where only instructive single case exists where there is no previous theory in the study.

Design Science Action 1 - Build

The process of building the RFID Security framework will include elements drawn by investigating case studies. The role of theory in design science research is at the centre of the research process (Venable, 2006), and models can facilitate problem and solution understanding (Hevner, 1994). In this research, the theory from Kim et al. (2007) is expanded in the build action to a general RFID security model that does not just focus on EPCGlobal tags.

Action 1: Build	Step 1: Review Literature and Analyze Requirements	Step 1 Deliverables: Secondary Data Available from Literature Review
	Step 2: Create List of Elements in RFID Security Framework	Step 2 Deliverables: List of Elements in Existing RFID Security Frameworks
	Step 3: Design the RFID Security Framework	Step 3 Deliverables: Comprehensive RFID Security Framework
Action 2: Evaluate	Step 4: Evaluate the Framework over the RFID Lifecycle	Step 4 Deliverables: Descriptive and Inferential Statistics Analysis
	Step 5: Final Report and Thesis	Step 5 Deliverables: Evaluation Report Documented

Figure 6 Breaking down design science research actions (March, 1995) into step by step operations

Apart from Kim's theory and literature that relate to existing policies and standards, this study will also examine how other approaches could reduce security breach. For example, RFID Journal (2007) has performed a survey to SC groups and results have shown that most consumers have no knowledge of consumer products they acquired carry RFID tags, or without a way to permanently destroying the tag. The results of this study will draw conclusions on policies and standard to literature (discussed in Chapter 7).

Building the artefact involves primary research and survey, where two selected SCs – one with a long and the other one with a short RFID lifecycle will be chosen. The difference in RFID characteristic can give a good comparison of how a LEI and TEI RFID security breaches are differed (described in section 7.4.5). Goods that are shipped in both SCs must be high impact, in terms of financial and non-financial means. The two SCs will be used for the study to build and evaluate artefacts in a step by step manner as illustrated in Figure 6.

A range of companies in the selected SCs has been identified (described in section 5.2) and approval in analysing their SC sought from these mini case studies. These companies were required to report their RFID security incidents to this research. Their RFID security breaches were recorded and rated in terms of severity in each domain in the RFID lifecycle model. Rating procedures aim to (1) build up a list of concerned vulnerabilities in each domain, and (2) devise a subjective rating by security breach count or value impacted. Semi-structured interview with the knowledge of multi-domain in the particular SC will be performed for identifying vulnerability in all the domains, and assigning these vulnerabilities into direct / associated / uncontrolled domains (documented in section 7.4.13). The coverage of the evaluation will include an initially proposed RFID lifecycle, defining a definite start and end for the evaluation scope.

Throughout the SC, an RFID can be considered as having a "lifecycle". There were previously no scholar writings to describe this idea. The closest is the "EPC Network" defined by EPCGlobal as discussed in 2.7.8. The "Lifecycle" concept was introduced in this step, and with this concept, attack vectors of RFID through the SC from production of an RFID tag to its ultimate disposal can be pinpointed. The vulnerabilities across the SC, developed by Rotter (2008), focus on products manufactured in PPRDLH, can be expanded into other systems in additional to "EPC Network" which was the sole system considered by Lehtonen (2008). Because of its global significance, the RFID originating at PPRDLH area has been chosen as the research ground of this study to provide a comprehensive report. In addition, by finding out the actual elements of vulnerabilities and contrast to various security frameworks utilized in the world, this study will attempt to illustrate a security framework for goods exported from PPRDLH, China. Then, by ranking financial impacts of the above products with different security breach impacts, the study addressed and divided all these security issues by

referencing to the SCOR model, thereby giving a common language for the SC members to communicate on the issue of security in an RFID Lifecycle.

The study will then attempt to develop a security framework of RFIDs, and the framework will add to literature a way to describe RFID vulnerability in multi-domain SCs, and identify ways to tackle such vulnerability. The study will be the first literature to introduce the concept of "RFID lifecycle" (discussed in Chapter 6). An RFID should be introduced when the product is produced; a raw material is procured, instead of tagging the tag in the retailer's shop which some SCs do nowadays. The definition of such lifecycle is missing from literature today. Generally, the longer the RFID lifecycle is, the more benefit it brings to SC. However, for an RFID that is being used by various parties in the SC could introduce multi-domain attack vectors, and this will be examined in the study.

Design Science Action 2 - Evaluate

The evaluation of security flaws by following life cycle of RFID will be performed. Hevner et al. (2004, p.81) expresses that the goal of design science is utility, and the researcher should also clearly identify its contribution to the archival knowledge base of foundations and methodologies. For example, a textual description of "best practice" approaches can be such a contribution. In this research the knowledge gained by evaluating RFID will serve as the foundations for further studies.

4.4 Steps to Perform the Actions

Venable (2006) has identified a framework for designing science research actions, consisting of Problem Diagnosis, Theory Building, Technology Invention/Design, and Technology Evaluation, and this research will follow this framework (Figure 7). This research will follow the five steps closely with details summarized in the below Table 14.

Activity in Venable's (2006) framework	**Steps in the research proposal corresponding to the framework**
1. Problem Diagnosis	1. Review Literature and Analyze Requirements
2. Theory Building	2. Create List of Elements in RFID Security Framework
3. Technology Design Invention	3. Design the RFID Security Framework
4. Technology Evaluation	4. Evaluate the Framework over The RFID Lifecycle
5. Theory Building	5. Final Report and Thesis

Table 14 Steps in the research proposal corresponding to design science framework (Venable, 2006)

This research uses the design science approach adapted from Venable (2006) to generate a product lifespan-based, multi-domain conceptual model. As Simon (1996) explained, natural science explains how and why things are, while design science devise artefacts. Agreeing with Simon, March and Smith (1995) consider design science to be aimed at developing ways to achieve human goals and purposes, offering prescriptions and creating "artefacts" that embody those prescriptions. Natural science can be basic research and design science are applied. There

are four possible outcomes in design science (March and Smith, 1995): constructs, models, methods and implementations. Agreeing with these outcomes, Hevner (2004) explained that quantitative evaluations of design science artefacts, including optimization proofs, analytical simulation, and quantitative comparisons with alternative designs should be done in design science research. In the evaluation process, one should ask the basic question "How well does it work?" (March and Smith, 1995) and a metrics should be formed to define what the artefact tries to accomplish. Design science proceeds iteratively until the artefact "works well".

Design science building and evaluation steps (explained in 4.3.1) are used in this research, to the primary artefact, a multi-domain conceptual model of RFID security during a product's SC life cycle. Rotter's (2008) list of RFID vulnerability, Lehtonen's (2008) single domain system, and Kim et al.'s (2007) multi-domain system will provide initial models on which artefacts can be built and further refined. This is also used to build a security policy framework artefact. Evaluation is the process of determining how well the artefact performs and in this study it will be determined by identifying and analysing RFID security in manufactured goods, down to the component level, and including elements of packaging and transport, from the PPRDLH. This vibrant manufacturing region will be used as the starting point of the RFID lifecycle, an initial source of information, and the testing ground for iterative process of building and evaluating the model and its associated framework.

4.4.1 Design Science Building Phase

The design science approach is used and a conceptual model is the deliverable of this research. This research will follow a plan, going through steps, sometimes iteratively, to produce the conceptual model and associated framework. The purpose of this framework will solve the research question 1. These initial findings will then inform the next step, which in turn further focuses elements from the previous step. The gradual building of the theory is one of the most important aspects of the methodology.

In the building phase, Google scholar search has been used to determine the validity of Rotter's (2008) list of RFID vulnerability in the SC context, and semi-structured interviews was used to establish essential elements of security vulnerabilities, domains in which these organisations operate, and other factors pertinent to existing models (RQ1).

The form of this artefact will be in itself a useful practical outcome of the research, which in turn will be used for theory building to improve both the conceptual model artefact and the framework. The approach is iterative with theory building as the nucleus of the model, but not in a circular loop or a waterfall approach which other design science researchers have proposed.

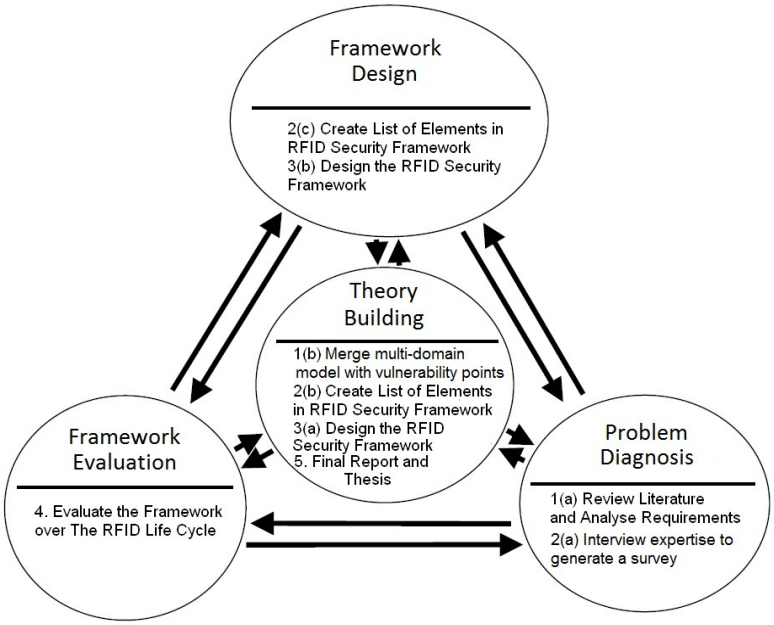


Figure 7 Research design aligned to design science elements (after Venable, 2006)

The following discrete steps are planned:

Step 1: Review Literature and Analyse Requirements

(Iterative loop in between: Theory Building -> Problem Diagnosis -> Theory Building)

Particularly in design science, existing models aid problem and solution understanding and frequently represent the connection between problem and solutions components (Hevner et al., 2004). In this research, the theory of Kim et al. (2007) was expanded in the build action to a general RFID security model that does not solely focus on EPCGlobal tags. Rotter (2008) suggests RFID attack vectors that can be layered over Kim et al.'s (2007) model. Together these theories represent a starting point for the iterative design of this research, as they will establish an initial model to be evolved in subsequent steps.

Step 2: Determine a Comprehensive List of Elements that constitutes an RFID Security Framework based on the conceptual model

(Iterative loop between: Problem Diagnosis -> Theory Building -> Framework Design -> Theory Building)

This step will require data collection in the form of Google scholar searches in order to adapt and contrast Rotter's (2008) vulnerability elements, as the initial bases of RFID security threats in SC. A range of companies that provided the selected products will be identified, where their RFID security incidents and according impact will be collated through semi-structured interview, on companies involved in the SC of a limited set of significant products sourced in the manufacturing region of the PPRDLH. In addition, these companies will be identified and

categorized into their respective positions in the multi-domain environment. Two different products, an LEI and TEI with highest representation in the region in terms of values of goods have been chosen. The relative SCs should also have RFID well applied but with different characteristics, for example long and short RFID lifecycle, security breach incidents, and other criteria to be chosen. The surveys will capture information from subject domain experts and RFID users. Secondary data, including reported security incidents and cases of breaches, will augment the primary data. Where secondary data is used, its reliability, suitability, and adequacy will be considered, as recommended by Camp (1989).

Camp (1989) described that primary and secondary data should be used in a research – primary data was defined to be collected afresh and for the first time, while secondary data are data collected by other researchers. In this research, secondary data analysis involves expanding Kim et al.'s (2007) multi-domain RFID security framework and generalizing to all RFID tags, covering all RFID security breaches collected. Camp (1989) also mentioned that the use of secondary data should be evaluated based on reliability, suitability, and adequacy. In the research, data is not adequately available and so primary data has been collected in additional to the use of secondary data. In order to further obtain a comprehensive list of requirements, opinions of the subject domain experts and RFID users will be collected in addition to data on existing models.

Four major methods have been defined to collect primary data, namely observation, interview, through questionnaires, and through schedules (Camp, 1989). Data collection and analysis methods proposed is tabulated in Table 4. Camp (1989) defined surveys to be describing, recording, analysing, and interpreting conditions that exist or existed, and surveys are further categorized based on their structure and disguise characteristics. Structured surveys are formal list of questions framed to get the facts, and disguised surveys do not reveal its objective to the respondent.

With the first research question in Table 4, semi-structured interview has been performed to determine a list of perceived elements within the scope of RFID security issues in order to perform mini-case study research. Mini-case studies in TEI and LEI industries have been selected and top security breaches are identified and the incidents of security breaches before and after RFID application are recorded. This list has been analysed by descriptive statistics to outline a list of perceived elements.

Research question	Data needed to answer the research question	Collect data from	Data collection methods	Analysis that carried out on data to answer the research question	Documented in Chapter
1. What are the types and sources of multi-domain RFID security breaches across the SC?	List of security breaches Kim et al.'s multi-domain model	Literature review	Observation Secondary data	Descriptive statistics analysis to outline perceived elements mapped to Kim et al.'s Multi-domain model	7
2. In what way can current multi-domain security models be extended to address RFID security breaches across the SC?	Security breaches incidents (RFID and non-RFID), SC policies and standards	Cargo owners Logistics service providers (Focus in various domains in Supply Chain)	Semi-Structured Interview	Inferential statistics analysis to shortlist missing or over-focused security elements	8
3. What policy framework will reduce multi-domain vulnerability?	Detailed information of actual security breach incidents	Cargo owners Logistics service providers (Focus in causes of RFID security breaches)	Focus Group Discussion	Descriptive statistics analysis to determine the vulnerability decrement	9

Table 15 Research questions answered in order to build and evaluate the artefact.

Step 3: Design the Conceptual model for RFID Security

(Iterative loop in between: Theory Building -> Framework Design -> Theory Building)

Step 3 actions analysed the data gathered in step 2 to refine the conceptual model, and to align the security policy framework to it. Finally, it would involve the creation of a security framework. The list of elements in the security framework was used to categorize the attack vectors that exist in the domains of the RFID lifecycle. A conceptual diagram (Figure 9 in Chapter 6) illustrates some of the elements found in the literature. The design will encapsulate three levels as suggested by Kim et al. (2007), where controlled and uncontrolled domains exist in the RFID Lifecycle. Furthermore, an attempt to categorize these top security breaches is then performed in order to propose a framework for further study. This step will allow the developed model and asserted framework to be evaluated.

This study then used this information with the MDSCRV model to form an extended model of RFID security breaches, and the study once again went back to literatures to review how policies suggested by various scholars can be used to tackle this extended model. By building a framework, the study aims to explain the security breaches of RFID in both LEI and TEI cases and draw policies that would give precaution to avoid these breaches.

To understand different RFID vulnerabilities scenarios in different SCs, a framework can be drawn from the preliminary model by accessing the common features in the two industries. The similar SC RFID breaches can be drawn as a framework which most SC will possess such RFID security breach.

The policy framework can be used to prevent RFID security breaches before they actually take place. For example, if "RFID signals being jammed by civilian telecommunication devices" is found to exist in drug stores but such jamming does not exist in hospitals, a possible policy framework can be obtained by revisiting literatures based on operating equipment security breaches. Such policy framework might involve banning the use of cellular phones in the cash counter in the point of sale systems would prevent similar issue of RFID signal jamming from ever happening in hospitals.

Next, the differences between the two industries have been assessed, along with the different SC RFID breaches. This framework specified the uniqueness of RFID security breaches that feature only in one SC, be it the LEI or TEI.

Fishbone diagrams (explained in section 2.9) will be used to form the basis of the framework, to find similar vulnerability to RFID security breaches. If a common framework in these two distinct industries can be drawn, this framework could also be useful when one study other industries within similar simply chain contexts. For example, if human mistake is the root cause of multiple common breaches in both SCs, then human mistake could be a major cause for SC industrial practitioners to tackle in priorities. However, it has been found that there are certain difference in the LEI and TEI SCs (documented in Chapter 7) and a common framework cannot be formed. Therefore MCDM (explained in section 2.9.2) has been used as a model to make decision based on multi criteria vulnerability in multi-domains SC RFID systems. Focus group members have been recruited to generalize the MCDM by answering pairwise comparison questions (documented in section 2.9.2), and AHP (explained in section 2.9.3) has been used to suggest prioritized solutions based on the MCDM model (documented in Chapter 8).

4.4.2 Design Science Evaluating Phase

Designed artefact evaluation is an important activity in Venable's (2006) design science framework. Researchers have proposed frameworks to evaluate artefacts, including conceptual models (Pfeiffer and Niehaves 2005), system analysis and design methods (Siau and Rossi 2008), and reference models (Fettke and Loos 2003). No researcher has provided a general evaluation model for all design science artefacts but several have used expert opinion and mini-case study based on the criteria of completeness, extensibility, usability, functionality, reliability, interoperability, scalability, and efficacy (Cleven et al., 2009; Pries-Heje et al., 2008;

Pfeiffer and Niehaves, 2005). Hevner et al. (2004, p.81) outlined the goal of design science as utility and it should also clearly identify its contribution to the archival knowledge base of foundations and methodologies.

In this research the evaluating phase will commence after the conceptual model and associated practical framework have been built. The iterative nature of the Design Science approach to this project allows fall back to the building phase to further enhance the model.

Step 4: Evaluate the Framework across the SC
(Iterative loop in between: Theory Building -> Framework Design -> Framework evaluation)

The RFID security framework has been evaluated, as the designed artefact evaluation is an important activity in Venable's (2006) design science framework. Hevner et al. (2004) agreeing to March and Smith (1995) mentions evaluation is important and there are no particular methods or techniques suggested for evaluation. The above mentioned eight criteria (completeness, extensibility, usability, functionality, reliability, interoperability, scalability, and efficacy) will be evaluated on the RFID security framework instead of its construction process, and the evaluation will be performed ex-post (after the framework has been created). This evaluation will be an objectivist evaluation based on the outcome (decrement of RFID security breaches) after the application of the practical framework by quantitative and qualitative approaches in an interpretivist evaluation. The evaluation of the artefact is summarized in Table 16.

Artefact	RFID Security Framework
Artefact Type	Model
Evaluation Criteria	Completeness – Does the framework cover the entire scope of study, i.e. the proposed RFID Lifecycle? Extensibility – Can the framework be extended to cover SC that is out of the location that is being studied, i.e. Pearl River Delta? Usability – Can the framework be used to analyze SC? Functionality – Can the framework address security vulnerability? Reliability – Can the framework reduce security vulnerability? Interoperability – Does the framework work with other SC operation reference models like SCOR? Scalability – Can the framework apply to the extreme case studies selected? Efficacy – Does the framework reduce security vulnerability solely based on the evaluation taken place?
Object	Artefact instead of its construction process is the object of evaluation
Time	Ex-post
Ontology	Objectivist
Evaluation Type	Outcome
Epistemology	Interpretivism
Approach	Quantitative and qualitative
Evaluation method	Evaluate the framework by change in security vulnerability with case studies from Pearl River Delta

Table 16 Evaluation framework for the research based on the frameworks.

Proposed by Cleven et al. (2009), Pries-Heje et al. (2008), and Pfeiffer and Niehaves (2005)

The evaluation was taken place with companies in various domains of the SC, in a focus group discussion to discuss on how the prioritized solutions can translate to policies to tackle SC vulnerability. The security policies and standards were recorded and performed by the focus group members. By the use of inferential statistics analysis on observations on the focus group members who used the prioritized solutions, quantitative evaluation of the use of the artefact and the possible decrement of vulnerability in the particular SC will be used as one of the main performance index. To elucidate this, focus groups consisting of members with RFID security breach in the same category discussed the conceptual model and framework developed to this point.

Qualitative analysis of data from these focus groups validated the framework elements and the conceptual model developed. The use of focus groups with representatives from all domains of the SC grounded the model and framework to practical use in a complex environment. To simplify the analysis steps to the focus group member, pairwise comparison allowed focus group members to consider a complicated scenario and answer in a much focused manner (discussed in 2.9.3). An analogy can be a doctor's clinic visit by a patient with a fever; a doctor would ask the patient to focus on just one single symptom, and ask questions like "compare the

severe level of headache verses fatigue", or "if coughing is experienced once, how many times does running nose experienced". By repeating few times of these questions, pairwise comparison can be performed, and would lead a doctor to understand which priority medication should be given. Of course in such simple analogy one would argue that all related medications can be taken as long as they do not have side effects or overdosing issue, however in SC business scenario applying several solutions to solve a single problem could be costly and violate risk management theories, where a solution should always be cheaper than the expected lost.

After the pairwise comparison are performed, they must be checked for consistency (discussed in 2.9.3) to ensure answers provided by focus group members are consistent. The way to check the consistency is:
1.Calculate the consistency measure.
2.Calculate the consistency index (CI), by the formula of CI = (l max – n)/(n - 1)
3.Calculate the consistency ratio (CI/RI where RI is a random index).
CR = CI / RI

These consistency checks were calculated and documented in 8.6.1.

Step 5: Final Report and Thesis
(Theory Building)

A finalised "design theory" of design science researchers should always be documented (Walls et al. 1992). A further update on research contribution, method, and limitation should also be included as a theory for design and action (Gregor and Jones, 2007). The results will be basis for development of future RFID security models by further researchers and will be finalised during the thesis writing process.

4.5 Data Analysis for this Study

Data analysis is a process of discovering conclusions from data researched (Weir, 1990). The actions of data analysis include inspection of data, cleansing incorrect retrieved data, transforming data to usable information, and deriving data models. Analysing data is important for a research study. There are two methods of data analysis, namely the quantitative and qualitative research. This study features both methods of data analysis, first by qualitative analysis follow by quantitative.

4.5.1 Qualitative – Semi-Structured Interview

The number of cases included in the mini-case study is important for a qualitative research as the nature of qualitative research is inductive and describes a problem by in-depth interviews as

discussed in chapter 3. There is no magic number for choosing the number of cases included in a mini-case study. Distinguished scholars have studied this issue and there are some common understandings. To start with, Yin (1994) recommended at least 6 sources of evidence. Creswell (2009) lowered to this minimum number and recommended 4 or 5 cases to start with.

Glaser and Strauss (1967) suggest researches to stop continuing when the data starts to repeats itself or they used the term *diminishing return* has taken place. Morse (1995) agreed to Glaser and Strauss, and advised the idea of *significance of saturation* is *to collect data until saturation occurs*. Cresswell (2008) suggested a number in between 5 to 25, Baker & Edwards (n.d) suggested 12 to 60 to be the range, and 30 being the mean.

Marshall et al. (2013) had a study of number of interviewees and suggested there will be a degrade of study quality a particular study with more than 30 interviewees. This echoed Glaser and Strauss' idea of diminishing returns, as illustrated in Figure 8. On average, Mason (2010) identified and calculated 560 research studies and found the mean of number of interviewees are 31.

4.5.2 Quantitative – Focus Group Meeting

As explained in section 2.9.4, there are three ingredients in a focus group study. (1) The Purpose, (2) The knowledge of focus group members, and (3) the budget that influences the degree of specification. These three ingredients are carefully considered to allow verification to the model, the purpose is examined in section 8.2, and knowledge and budget are reviewed in section 8.3.

4.5.3 Qualitative Research

Exploratory research is the basis of qualitative research, to help gain understanding of reasons, motivations, and opinions (Merriam, 1998). Miles and Huberman (1994) explained qualitative researches are inductive and formulate theory or hypotheses and efforts are mostly spent in the analysis phase to analyse unstructured data. These data can be obtained by unstructured and semi-structured interviews, or focus groups in a carefully selected small sample respondents' size. Dey (2003) suggested that as a researcher experiences the research process in a text based manner instead of numerical data, it can be subjective and depends on researcher's skill sets. Qualitative researches are useful to take place before studying in depth into a problem, which are performed to understand a trend of thoughts. Such thoughts can give insights or develop ideas for a given problem where quantitative research might be performed afterwards.

4.5.4 Quantitative Research

While qualitative researches are focused on text, a problem can be quantified by statistics study of numerical data; they are the quantitative researches. For example, attitudes and behaviours of a larger sample population can be formatted into variables which are then measured by quantitative researches. Bryman and Cramer (1990) suggested structured data collection methods are used in quantitative researches including methods of surveys, structured interviews, and systematic observations. Life (1994) agreed to Bryman and Cramer (1990) and further acknowledged that qualitative researches are deductive in nature with pre-specified concepts, constructs, and hypotheses for testing, and therefore the planning phase in qualitative researches are more focused instead of the analyses phase. The researcher interpret observed effects, usually in numerical format, with minimal interpretation from the researcher, therefore, the reliability of the study depends on the measurement device or instrument instead of the researcher's experience. As quantitative researches are carefully designed, robust, and highly repeatable, usually a large number of cases are studied with quantitative researches. Characteristics of qualitative and quantitative researches are summarized in Table 17.

	Qualitative Researches	**Quantitative Researches**
Methods	Focus groups, in-depth interviews	Surveys, structured interviews & observations,
Process	Inductive, formulate theory or hypotheses	Deductive, test pre-specified concepts, constructs, and hypotheses
Focuses	Analysis phase	Planning phase
Point of View	Subjective: describes a problem by researcher experience	Objective: observed effects interpreted by researchers
Data	Text	Numbers
Case Count	In-depth study on a few cases	Breadth of information from large number of cases
Method	Unstructured or semi-structured	Structured with fixed response
Generalizability	Less	More
Reliability	Depends on researcher's skillsets	Depends on the measurement device or instrument

Table 17 Characteristics of Qualitative and Quantitative Research

Compiled from various researchers' studies including Weir, B. S. (1990), Merriam, S. B. (1998), Miles, M. B., & Huberman, A. M. (1994), Dey, I. (2003), Bryman, A., & Cramer, D. (1990), and Life, R. S. (1994).

4.5.5 Qualitative Research in this Study – Semi-Structured Interview

In the beginning of the study, qualitative analysis has been performed. Semi-structure interview is used to gain knowledge about the RQ and identify key thoughts to the subject. Questions including pre-set answer choices or open ended questions that lead to discussions helped to categorize security breaches. Top security breaches and average lost values of pre and post RFID application were analysed to identify causes and sources of RFID security breaches (discussed in section 7.3.1). With the causes and sources categorized, a revisit to

literature to seek for solutions is performed (literature discussed in section 2.7.6, analysed in section 7.4.11). However, the above solution only fit TEI SCs with short RFID lifecycles, where limited vulnerability exists in associated if not direct domain in the SC (found and discussed in section 7.5). Therefore, a new model needs to map these vulnerability in the multi-domain SC, which is the MCDM (discussed in section 2.9.2, documented in section 7.5.3).

4.5.6 Quantitative Research in this Study – Analysis on Focus Group Meeting

Next, quantitative methods are used to find prioritized solutions in the MCDM models. Hierarchy models were built on MCDM models (documented in section 2.9.2) for use of AHP (discussed in 2.9.3, illustrated in Figure 16). Pairwise comparison has been performed in focus group by pre-set answer options in scales (illustrated by Table 18), and the answers were recorded in matrix formats (discussed in section 8.6). AHP were performed (discussed in section 8.6, documented in section 8.4.1) and consistency test was used to ensure correctness of analysis (documented in section 8.6.1).

To establish practical policies a focus group was chosen. This is because multiple evaluation studies with participants communicate and help each other under the control of a facilitator is best to be done in a focus group (discussed 4.2.4). The purpose of the focus group interview is to verify the usefulness of the elements of EMDSCRV Model. Focus groups can further enhance the study and benefits has been discussed in section 2.9.4. In Chapter 7, semi-structured interviews were done to explore the views and needs to build the MDSCRV Extended model, and in this chapter the focus group should be used to verify the model. While semi-structured interview provides information in an individual basis, focus group studies allow collective understanding of the study topic (discussed in 2.9.4). Therefore, the focus group study is useful in the study to generate detail approaches to the solutions of the causes and sources of the RFID security breaches, as compared to just a direction evidenced from the revisit of literature.

The focus group members are industry practitioners in the SC, whom could be best qualified to judge the results in the pairwise comparison method (discussed in 5.4). In each study, criteria and alternatives are presented in pairs, where focus group members are required to evaluate individual alternatives and deriving weights for each of the criteria. After that, each member can construct an overall rating of their particular RFID security breach in the SC, including the alternatives, and identifying the highest weighting one.

The focus group study setting is in a round table discussion with an overhead projector in one side of the room. Printings of materials were also provided. The members first discussed the particular cause and source of the RFID security breach in an open discussion mode. Emphasis

have been made that even in a multi-domain SC security breach could have other causes or sources, the other causes and sources should not be considered.

A size of 4-6 participants for each security breach causes and sources is used for mini-focus group study. The reason of choosing this focus group size is discussed in section 2.9.4, where major benefits are ease of manage while provides wealth of experience sharing, especially in the case where participants have intense or lengthy experience.

This study has taken the best of a large focus group and mini-focus groups, it first started with a large focus group for general discussion and then broken down into four mini-focus groups for the four causes and sources of RFID SC breaches. By doing so, the wealth of experience of the focus group members can be well captured while the mini-focus group gave a chance for group members to explain their thoughts in details. After discussion, the causes and sources obtained from the semi-structured interview will be used to form a pairwise comparison matrix (discussed in 2.9.3)

Pairwise Comparison Matrix used in Focus Group Meeting

Pairwise comparison matrixes were built by asking the focus groups members to compare the solutions with respect to only the causes and sources of RFID SC breaches. A survey form was distributed to the focus group members prior to assigning them to the most relevant focus group. Focus group members with several RFID security breach incidents and were assigned to both focus groups in answering the survey form as two different cases. The survey form focused on answers to the pairwise comparison, and the actual figures of pairwise comparison were carefully calculated during the focus group meeting. The results were calculated based on an average rounded to nearest integer 1/3/5/7/9 for AHP analysis as shown in Table 18.

Scale	**Degree of Preference**	**Mean Value**
1	Equal importance	mean of x>2
3	Moderate importance of one factor over another	2>=mean of x>4
5	Strong or essential importance	4>=mean of x>6
7	Very strong importance	6>=mean of x>8
9	Extreme importance	x>=8
2,4,6,8	Values for inverse comparison	

Table 18 Modified Example Scale for Comparison

Adapted from Saaty & Vargas (1991), modified by Adding Mean Value Column for Implementation in This Study.

Identifying Main Causes and Sources in Focus Group Meeting

After the cause and source comments are finished, each individual, the group members were asked to perform pairwise comparison of the solutions to the causes and sources. The online

tool PoolEV[31] was used for instantaneous pool, and members have to choose the comparison answers of the pairwise comparison by their mobile phones at the same time, to avoid respondent bias as discussed in section 4.2.5. Since different group members have provided input to PoolEV, consistency check is extremely important and was immediately performed to make sure the pairwise comparison delivers consistency results. For contradicting results spotted, a discussion session was held to correct the issue. An mean of the scores were taken with conversion entries in Table 18 were used for the study. After such scores are retrieved, analysis will be performed on the results (documented in 8.6)

4.5.7 Avoid Study Design Bias in this Study

Bias in qualitative researches are common and bias in the qualitative part of this study is minimized in the semi-structured interview by the principles discussed in 4.2.5. Carefully written semi-structured question scripts also lead to the focus groups study where the same principles have been adopted. Only quality questions at the right moment is being asked in order to achieve high standards of results. Table 19 lists ways of avoid bias in study design, and data selection bias is further discussed in section 5.5.

[31] Poll Everywhere, https://pollev.com/, allows the use of mobile phones to perform polling. In this application pairwise comparison was performed in a poll, in a confident and simultaneous environment.

Bias Category	Bias Prevention Mechanism
Study Design Bias (Discussed 4.2.5)	Following design science approach and artefacts are being built by mini-case study and focus group discussion
Selection Bias (Discussed 4.2.5)	Minimized by having different sizes of companies with different SCs in different continents of the world during the selection process. Furthermore, companies participated in semi-structured interviews will not be reinvited in the focus group discussion to avoid any selection bias
Respondent bias - Acquiescence bias (Discussed 4.2.5)	Replacing closed end yes/no questions to open end natural questions which focus on the respondent's true point of view in their answers.
Respondent bias - Social desirability bias (Discussed 4.2.5)	Included non-personal questions so as not to entice respondents from picking socially desirable answers, for example, instead of asking what the respondent feels, the semi-structured interview asked about how the public or SC practitioners would feel in general. This allows more honest and representative answers to be retrieved.
Respondent bias - Habituation bias (Discussed 4.2.5)	Engaged the respondents by keeping up the interview conversational and varied question wordings to minimize habituation.
Respondent bias - Sponsor bias (Discussed 4.2.5)	No sponsorship taken in this study, and interviewer has repeatedly reminded interviewee before commencement of interview.
Confirmation bias (Discussed 4.2.5)	The semi-structure interview had a different findings compared to the MDSCRV model, which has disproved certain RFID security breaches in multi-domain SC. As the results disproved the model, shortlisted the breaches and improved the model, the confirmation bias does not exist.
Leading questions and wording bias (Discussed 4.2.5)	Similar to confirmation bias, since the study did not lead to a confirmation to the MDSCRV model but rather disprove some of the items, there is no answer-leading questions and wording bias.
Culture bias (Discussed 4.2.5)	The researcher is a logistics practitioner with multi-domain SC operations background, so as the respondents
Question-order bias (Discussed 4.2.5)	Interview has performed by asking general questions before specific questions to avoid question-order bias.
The halo effect (Discussed 4.2.5)	Minimized by asking all questions about one solution before asking for feedback on another, because when respondents are required to rate two RFID breaches solutions, there is a tendency that the opinion of one is projected to the other solutions as well.

Table 19 Mechanism to Minimize Bias in Study Design

4.6 Concluding Remarks

Design science was used in this study and qualitative methods helped to understand the motivation and reasons for the study. By using the results, a quantitative research that built on

this study from TEI to LEI SCs can be formed. The study will capture different perspectives, agendas, and assumptions of the study target. Further analysis in different levels to capture more complex behaviours can be then performed in order to conceptualize results of this study. By the research approach, an attempt was made to solve the RFID SC vulnerability problem by using mini-case study and focus group, via the design science methodology, with details documented in the next chapter.

5 Data for this study

The data was collected from 50 business operating in two representative types of SCs are used as the basis for this study. Qualitative data was gathered using semi-structured interview and focus group, and was augmented with a quantitative phase to address RQ1. The target group selection, sample size and bias minimization are considered in this chapter. In the second phase of the study, 25 focus group members adopted and evaluated the usefulness of the model, these companies were not repeated in order to ensure an unbiased study being performed. Supply chains can be very different from one another and therefore there is a need to select case studies from a wider spectrum, and the numbers and rationale of selection is explained in this chapter.

5.1 Introduction

In research the choice of mini-case study targets can affect the quality of the research outcomes (Flyvbjerg, 2006; Stake, 2013). SCs member companies are very diverse in how they conduct business and use the SCs. This is driven by factors such as financial implication, long or short SCs as differentiated by Schipmann and Qaim (2011).

In this study it is not possible or necessary to consider all these variations. However, two styles of SC operation are defined and chosen to represent two diverse approaches. These are referred to as leading-edge industries (LEI) and trailing-edge industries (TEI). 25 cases are considered in each of these groups. Discussions and conclusions are also based on these groups and used where possible to be extended to other SC groups.

The results from the mini-case study should be evaluated, and a focus group meeting with 25 participants, not overlapping the mini-case study group members was used. The evaluation with non-overlapping members ensure the study is not *selection biased*.

5.2 The Mini-case Study Group

The pharmaceutical SC applies RFID in an end-to-end manner with a longer RFID lifecycle (discussed in section 1.11.4). This is a more integrated and arguably sophisticated system. In this study it is treated as a LEI since the RFID systems are more complex and spans across the

multi-domains SC. On the other hand, some SCs require RFIDs operating in a single domain. The jewellery SC is representative of this and in this study is treated as a TEI.

The distinction between LEIs and TEIs is important because RFID systems that can be controlled by a system owner is easier to manage, from tagging, usage, to dispose. Whereas a longer RFID lifecycle system can have RFID manipulated by more domains in the SC, giving a system with more attack vectors and therefore higher chance of being security breached.

The study uses the properties of LEI and TEI in terms of levels of RFID technology application as examples to illustrate SC breaches in daily operation. In LEI and TEI industries, levels of application of technologies to SC are very different from one SC to another. Therefore, in order to solve the research questions, two groups are selected to provide comparative analysis. For example, TEI companies have a lower concern of product SC aspects such as security, delivery time, and lead time. These TEI companies have a shorter RFID lifecycle and the main application is limited to item tracking. On the contrary, LEI SCs, even though they consist of members who are smaller or independent companies, focus on end-to-end SCM since a mistake made in SCM, even in a simple logistics delivery or storage transaction, could have huge impact.

5.2.1 LEI and TEI SCs Needs

In the SCs selection process, the first group of company selected is the jewellery industry. The jewellery industry has strong SC requirements as the goods value is high. Between the two selected industry, the jewellery industry is old and application of RFID is not high (discussed in section 1.11.4). The second group of company selected is the pharmaceutical industry. The pharmaceutical industry has been selected as the goods value are not high, but the SC is equivalently important as the jewellery SC as the impact of the goods are high, non-financially speaking; failure to deliver the right product at the right time to the right place in the right quantity and goods behaviour can cause human lives. The two industries have a completely different view on SC. For pharmaceutical, being in LEI, considers a delay in product delivery causes life, while in TEI, a jewellery retailer considers a delay in product delivery causes only business issues. Similarly, a LEI company would consider delivery chain of product including storage must be well maintained in secured and well controlled environment (for example, temperature and humidity), while TEI has only concern about security, and would transfer such risk to insurance company as lost values can be monetarised.

An equal number of logistics practitioners are drawn from each of the LEI and TEI industries. RFID applications of each of the practitioners are considered across all the domains in the respective SC.

5.3 Semi-Structured Interview Data and Selection of Participants

The importance of avoiding research bias and selecting valid samples are well justified (Section 4.2.5). The study carefully followed the justification to select valid sample cases. The sample selection process started by determining a sample size for study, after that the number of cases selected went through a rigorous process of check list (Illustrated in Section 4.2.5) to eliminate samples with possibility of research bias.

The study was performed to work up from the retailers to their chain towards the upstream side of logistics. The companies were selected by visiting local telephone book of active pharmaceutical and jewellery retailers in Perth, Australia and Hong Kong, China, working back the way towards their parties in SC such as importer, distributor, logistics service providers, and manufacturer and raw material providers. Letters of invitation for study has been sent from a research institute in Perth, Australia and a logistics association in Hong Kong, and then follow up calls made by the researcher for semi-structured interview opportunities either face to face preferred or over the phone with the questionnaire sent to the interviewee before the interview. This operation is repeated until twenty-five qualified interviewees have been carefully selected and interviewed in each of pharmaceutical and jewellery SC, making a total of 50 semi-structured interview cases (25 in each of TEL and LEI industries) in this study.

This study size used is 25, with started from the scholars recommendation of minimum of 12 (discussed in 4.5.1), and reached 25 then there were no new ideas reported by the interviewees. As the number of 25 falls in the range as suggested from the scholars (explained in 4.5.1), it was accepted as a good range for a comprehensive study.

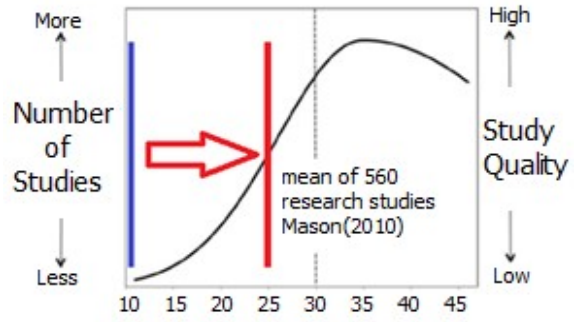


Figure 8 Starting and ending point of number of interviewees used. Blue line is the minimum starting point (as suggests by Yin (1994), 6 cases to be minimum. Creswell (2009) suggests 5-25, indicated by the red line, also is the mean of 560 research studies case number recapped by Mason (2010). Dotted line indicating the point of *diminishing return* as suggested by Glaswer and Strauss (1967). Diagram adapted from Marshall et al. (2013) with additional lines indicating interview count for this particular study.

Initial few companies who agreed to participate in this study expanded their SC for the researcher to research. Given the retailers who agreed to participate in research and they are the customer in the SC, the interview to the upper stream are easier with the contacts provided by the retailers. The choice of upstream are broader and the interviewee selection for the mini-case study data collection is based on the following three criteria: SC characteristics, domain in SC, and accessibility.

The semi-structure interview has given an understanding to the security breaches of RFIDs, which added list of security breaches to compare the security breaches evidenced from the literature review, formed the MDSCRV model. After this comparison study has been completed, an extended model has been built, namely Extended MDSCRV, or EMDSCRV. The EMDSCRV model incorporated the results of the semi-structured interview. A revisit to the literature enabled the study to find causes and sources of the security breaches to form the EMDSCRV model, and then a focus group study performed to evaluate the model, by the use of a practical framework. The detailed model, practical framework, and focus group study is explained in Chapter 9.

Revenue (US$)	**Number of companies**
< 1.99 million	8 companies
2 – 3.99 million	19 companies
4 – 5.99 million	11 companies
> 6 million	12 companies
Local market (%) vs. Worldwide markets or exports (%)	
20% vs. 80%	28 companies
40% vs. 60%	11 companies
60% vs. 40%	8 companies
80% vs. 20%	3 companies

Table 20 Focal Company Characteristics

First, the focal companies are chosen based upon their market share in the industry. One large and one small SC is being chosen. Second, the focal companies as data collection targets are required to be in a multi-domain SC that has manufacturing domain performed in the PPRDLH, as the biggest supply base in the world. The diversity of supply destination can hence provide better comparison between the jewellery and pharmaceutical SC. Finally, focal companies' accessibility is a criterion as well. The study started with the focal companies and then followed the SC to both directions of upstream and downstream.

5.4 Focus Group Data and Selection of Participants

In order to have an unbiased study, the focus group mini-case study contains a new set of companies but not any from the semi-structured interview. These companies are members of a logistics association in Hong Kong that are in the pharmaceutical and jewellery SCs. Instead of

dividing the focus group targets by the two SCs they below, they are divided into the four causes and sources of SC RFID security breaches, namely the Unethical Usage, Hacker Attack, Operating Environment, and Human Error groups (four causes and sources determined in section 7.4.11 and explained in 2.7.6).

Stewart and Shamdasani (2014) believe the ideal size of a focus group study should be 10 to 12 people for commercial topics, while for non-commercial topics 5 to 8 participants, as focus group with over 10 members will decrease sharing of insights and observations from participants. Furthermore, small or mini focus groups with 3 to 6 participants are getting popularity due to ease of manage. However, the mini-focus group also has a disadvantage, where total experiences range are being limited due to smaller group. Stewart and Shamdasani (2014) further comment that smaller groups are best to gain understanding of people's experiences and in-depth insights. Smaller groups are generally preferable when deep experience participants are willing to share and discuss.

Factors to consider recruit a small focus group	**Properties**
The purpose of the study	Understand an issue or behaviour
The complexity of the topic	More complex of topic
Level of experience of participants	More experience
Level of topic passion of participants	More passionate
Number of questions studied	More questions

Table 21 Factors to Consider to recruit small focus group, tabulated from Stewart and Shamdasani (2014)

Focus groups between 3 to 8 participant in each of the causes and sources of SC RFID security breaches was selected to serve as the second of the three ingredients of a focus group study as discussed in 2.9.4 and further highlighted in section 8.3. The participants and their background, is important for a focus group study. The focus groups study started in Hong Kong to evaluate the study finding when facing practical problems. The group has been selected to observe RFID security breaches in their logistics RFID applications, they were chosen by mail survey to all members of a logistics association in Hong Kong that are in the jewellery or pharmaceutical SC. Volunteering individuals were selected based on the criteria that they must have existing RFID security breaches within one year. In total, twenty-five focus group participants were selected based on company size, SC characteristics, and more importantly, the previous RFID security breach incidents. The individuals were then asked to apply one or more proposed policies from the policy framework (developed in 7.4.14) and document changes of RFID security breaches before and after the solution application. Finally, a survey was distributed to the focus group members for evaluate the usefulness of the model (results documented in 8.6.6).

The budget of the focus group study is minimal as they were chosen from the logistics association in Hong Kong, and an additional 3 hours were needed for members to stay behind after association function. The focus group members to be well related to the purpose of study.

Every single focus group member is not only screened by the researcher, but also the backgrounds of these members are experienced SC practitioners from their involvements in such logistics association. The fifty semi-structure interviewees were not invited to join the focus group to ensure unbiased study results. The group discussed various policies that were applied based on the suggested list of policies from the extended framework, and the results after such policies were applied. The process of the focus group discussion and results are discussed in Chapter 9.

5.5 Data Selection Bias in this Study

In section 4.2.5 ways of avoiding bias was well discussed. Following on section 4.5.7 where study design bias were avoided, data selection bias were also avoided. Section 4.2.5 further discussed about *selection bias* with the issues of *definition*, *accessible*, *reliable*, and *interests*. The *definition* of mini-case study selection involves two distinct industries where selection bias is minimised. There were no *accessibility* issues and all mini-case study and focus group members joined the study from start to the end. *Reliable* study results were ensured by the use of focus group member to evaluate a model that is drawn by mini-case study group members, verifying study results. Finally, there were no common *interests* spotted in the study cases, they were drawn by industry association members where knowledge is built up instead of trade associations where members are more likely to be business oriented.

5.6 Concluding Remarks

The mini-case study members allow this study to explain and analyse the research problem and the cause behind the answers. Semi-structured interview based on the mini-case study members allow primary data to be obtained, and further analysis of such data allowed the model to be drawn. Finally, focus group members allow the model to be evaluated. These artefacts formed enabled the building of the answers to the research questions.

6 Categorization of sources of RFID Security Breaches

Research Question 1: What are the types/sources of multi-domain security breaches?

6.1 Introduction

This chapter addresses RQ1, i.e. "What are the types/sources of multi-domain security breaches?" This question is important as it provides confirmation of the list of vulnerabilities established in the literature review (various authors including Rotter (2008) suggested a comprehensive list of generally RFID vulnerability – discussed in 2.6). It also extends criteria and frameworks, and assesses their importance in a SC context.

An important extension of the extant literature on vulnerabilities is to apply them in a multi-domain aspect. This extension concept requires extra consideration because SC practitioners only have complete control over their domains, but not all domains along the SC. Hence vulnerability in the other domains is not easily detected or addressed by the focus operators implementing solutions in the domains they control.

RQ1 therefore recognizes that different RFID security breaches exists in multi-domain SC. Logically, various causes or sources of security breaches exist in such multi-domain SC, however there is no comprehensive list particular to SC given by any scholar. In order to address to these various causes or sources of security breaches, a thorough and critical literature review of all security breaches on RFIDs have been performed.

In the design science framework, the first step 1(a) is represented by the literature review in Chapter 2, which was used to build the artefact used in later steps. In this chapter steps 1(b), 2(a), and 2(b) continue to build another artefact through semi-structured interviews to create a list of RFID security breaches in a multi-domain SC.

6.2 Method

The method includes Design Science Methodology 1(a) Review Literature and Analyze Requirements and 1(b) Merge Multi-Domain Model with Attack Vectors. 1(a) is in Problem Diagnosis and 1(b) is in Theory Building. These two methods provide background information in the form of artefacts. The methodology is described in full in Ch 4, starting by shortlisting

existing literature into a list of attack vectors relevant to SC operations. The list is compiled by revisiting to the wealth of literature that cover both SC RFID and the vulnerability suggested by Rotter (2008). The number of qualified literature will be recorded.

Data used in this RQ is based solely on literature, in an attempt to provide a list of RFID SC attack vectors based on the researches of various scholars. Not only journal papers but also textbooks and other references including patents, trade publications and both government and institutional reports were reviewed.

The review of literature and analysing requirements are considered as building new artefacts in design science studies as discussed in section 4.4. Google Scholar, as the world's most comprehensive database of quality literature and scholar's writing, was used as a starting point of the review.

6.3 Results

The result is listed below in Table 22. The result counts are relevant as it shows the vulnerability studies by researchers, which formulates the initial RFID vulnerability list. All the abstracts of these papers have been reviewed and selected journals related to this study are reviewed in full, as presented in Chapter 2.

Google Scholar Search Keyword	**Result Counts**
"Eavesdropping" RFID "Supply Chain"	2230
"Relay" RFID "Supply Chain"	5020
"Unauthorized Reading" RFID "Supply Chain"	1008
"Cloning" RFID "Supply Chain"	2130
"People Tracking" RFID "Supply Chain"	261
"Replay" RFID "Supply Chain"	2110
"Data Content" RFID "Supply Chain"	1390
"Malware" RFID "Supply Chain"	1250
"Breakdown" RFID "Supply Chain"	5050
"Destruction" RFID "Supply Chain"	3570
"Blocking" RFID "Supply Chain"	4000
"Jamming" RFID "Supply Chain"	1300
"Back-end" RFID "Supply Chain"	5310

Table 22 Google Scholar Result Counts of RFID Vulnerability as Suggested by Rotter (2008)

As reviewed in section 2.6, Rotter (2008) was the first author to suggest a list of RFID vulnerability, however, this list was not categorized into specific industries (in the case relevant to this study, the SC) and did not consider the areas where the vulnerability existed, unlike Kim's model which is tailored for multi-domain SC studies (discussed 2.7.7). This study first starts to revamp this list from Rotter (summarised in Section 2.6) and map it to the multi-domain idea as suggested by Kim et al.

There are additional RFID vulnerability issues that are identified from the literature (discussed from 2.6.14 to 2.6.17). The new list, combining Rotter's (2008) list (discussed 2.6.1 to 2.6.13), where vulnerability identified by literature is added, is the starting point of the list building. There are also attack vectors omitted. It can be seen easily that *People Tracking* should be omitted as the RFID SC vulnerability is the only vulnerability item from Rotter's list with less than 500 results. Reviewing all the 261 scholar writings from the results, people tracking referred to cases where the RFID is not tagged in goods that track human being, but rather in cases were human being is being tagged and tracked, for example, in a hospital where patients could be tagged by an RFID hand band in order to be tracked. Some authors (in the 261 writings) have studied the use of product with RFID to track human being, however, this is not in the original scope of people tracking according to Rotter, who stressed on vulnerability issues in implanting RFID in human body. This study will ignore this item, People Tracking, for RFID SC vulnerability. This vulnerability list from Rotter without People Tracking is named as SC RFID Vulnerability (SCRV) in this study.

6.4 Analysis

The list of attack vectors should then be mapped into the multi-domain SC environment in order to show where in the SC the attack vectors are more likely to exist. This is the step 1(b) as suggested in section 4.4 and illustrated in Figure 7. A review of literature relating to PPRDLH OEM and ODMs reveals that SC practitioners in the region are mostly manufacturing for buyers located in the world (OEM and ODM discussed in section 1.9.1). They are not brand owners and they do not have control over the selling side of the products. For example, a garment manufacturer might produce clothing for worldwide fashion shops but they do not have control over the RFID systems that the fashion shop uses. They also do not deal with raw materials neither. For example, the yarn used in the textiles is not made in the PPRDLH area (Thompson, 2002), and when these factories received the raw materials, they were already processed. These factories would be the first domain in the SC that gets finished, if not semi-finished goods. Therefore, for such goods these companies would be the first domain to *directly* tag the RFID to an item.

In such case, the most comprehensive RFID lifecycle would start from there and until the product is being sold, where the RFID is being disposed. In the middle of the process RFID tag reading can be done at any point in the logistics flow in the SC, and data will be updated. For example, when an end product is put into a transport device, say a plane, it will have status update. Another example would be the product being put into a warehouse. This could also generate a status update. Retagging is the last resort to fill particular business needs if an update to the data represented by the RFID cannot serve that purpose. These logistics service providers have connections to the PPRDLH factories, and are considered as the *associated* domain. This

domain is responsible for the movement of finished goods from the factory to the point of sale, most likely in Europe or USA (Top ten listed in Table 4, discussed in section 1.9.3).

These points of sale are considered as the *uncontrolled* domain. Some of these companies are not even connected to the factory, as the PPRDLH factories sometimes go through trading houses or buying offices in the SC in the trade. Even if the seller domain directly receive purchase orders from the buyers, they are still likely have no influence to the buyer's use of RFID as the buyers are customers of the sellers. Such usage could include tag reading for tracking and selling purposes, or the final RFID tag disposal by the consumers who have bought it. Consumers who dispose the tags are in the uncontrolled domain from the perspective of the PPRDLH factories.

6.4.1 Mapping Attack Vectors to Multi-Domain Supply Chain Environment

The mapping of the RFID security attack vectors to the Kim et al.'s model highlights areas where vulnerability exists. An attempt has been made and discussed in section 1.9.3, based on a typical SC in the PPRDLH. The result of this attempt should allow PPRDLH SC practitioners to examine the possible solutions to tackle such attack vectors.

This literature puts the concept of "lifecycle" to the study of RFID (discussed in 2.5.3). The uni-directional property of SC[32] suggests there is a start and end of all data flow. Likewise, there should be a "life" in RFIDs too. Currently there is no lifecycle of RFID model, in particular to consumer products. Similar to the SCOR model, which has provided a common language for SC partners to communicate; this study suggested how a lifecycle model of RFID will operate. This RFID lifecycle can be mapped to SCOR model as suggested in Figure 2 and "The EPCGlobal Network" in Figure 5. This is the model combining scholars' ideas as described in the SCRV list, and will form the basis for this chapter, which will further be modified.

The RFID Lifecycle has definite starting and ending points, the starting point could be the time that the identification of the RFID is being planned, and the ending point could be the detachment and disposal of the RFID by the consumer. The RFID Lifecycle is the scope of RFID attack vectors being studied.

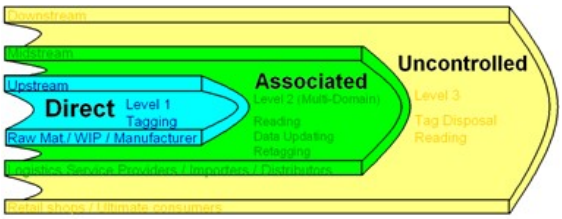
---

[32] Reverse supply chain (or reverse logistics in the operational sense) is the supply chain process for the purpose of recovering value or proper disposal. Typical examples of reverse supply chain include product returns and management of their wastes. Reverse supply chain is not in the scope of this study.

6.4.2 The MDSCRV Model: A Proposal from the Literature

Instead of defining RFID Lifecycle by drawing a simple line such as many SC literature did (as discussed in section 1.9.2), this study uses the idea of the multi-domain from Kim et al., and considers it necessary to insert the multi-domain idea of "Direct", "Associated" and "Uncontrolled" in to the RFID Lifecycle. A *tube* is used to demonstrate the relationship between the three areas in the RFID Lifecycle. A tube can easily show the "inner" and "outer" relationship of OEM factories in PPRDLH, where one factory manufacturer produces for many different retailers in the world. As the study covers RFID lifecycle starting when the RFID are being planned and tagged, the number of different companies adopting the RFID is tend to be more than the companies which tag the RFID, or "wrapping" the factories.

The inner part is the "Direct" area, which the focal company using the model has direct control of the RFID system used. The middle part is the "Associated", where the RFID systems are running by the companies associated with the focal company. Finally, the outer part is the "Uncontrolled" area, which the RFID system running details are not controllable by the focal company.



Security Vulnerability
Eavesdropping
Relay Attacks
Unauthorized Tag Reading
Tag Cloning
Replay Attacks
Tag Content Changes
Malware
RFID System Breakdown
Tag Destruction
Blocking
Jamming
Back-end Attacks

Figure 9 Security breach in RFID Lifecycle, from PPRDLH factories perspective

Three levels are defined in the RFID Lifecycle, namely "Direct", "Associated", and "Uncontrolled". A focal company can apply the MDSCRV Model to analyse their SC RFID security breaches. From the focal company's point of view, a SC could have areas where the company has absolute power to control, and can be considered as a "Direct" control over the RFID system. There could also be parties that are "Associated" with the focal company. For example, logistics service providers that the company uses, which are under outsourced logistics contract from the point of view of the focal company. The focal company has control over these companies in the sense that shall the outsourced logistics companies perform below certain satisfaction level, their contracts can be renegotiated. As a result, the focal company has

an “associated” control over these outsourced logistics service providers. The last type of parties on the SC are the “uncontrolled” parties, such as retailers that have no direct connection to the focal company. For example, a manufacturer uses a distributor in a certain country, and then the manufacturer, as from their point of view as the focal company, has no control to the retail shops. Another example could be the consumer, who has purchased the goods from the retailer, regardless of whether the retailer being in the associated or direct area; the focal company has no power to control how the consumer treat the RFID tag. In this case, the consumer is a party in the “uncontrolled” area in the multi-domain SC.

Previous authors have many solutions to RFID security threats as discussed in section 2.7. However, these authors did not consider the threats in a SC environment. If a solution has to be applied in an “uncontrolled” area of the SC in order to solve a possible security breach that is happening in the “direct” area, most likely such a solution cannot be applied at all as SC companies have no connection to or influence over companies in the “uncontrolled” area. In the previous example it would be that the manufacturer has no power to request retailers to kill the RFID tag (or erase the data) after the items being sold, even if it finds out customers are using the RFID data of their purchased goods in an unwanted way. This issue will be tackled in Chapter 8, where the multi-domain SC problem is further studied.

These security breaches can be mapped into the RFID Lifecycle, and then different security breaches can be “wrapping” the tube. For instance, shall a security breach happened, a company can highlight that part in the tube to emphasize that the breach happened in the “Direct”, “Associated”, or “Uncontrolled” manner, as the management and solutions of these security breaches are not the same.

MDSCRV Model for Pharmaceutical Supply Chain

For example, if a manufacturer in a SC tags RFID in the products it makes, every single RFID goes through “Direct” stage where the RFID tag owner manipulates the RFID tag, and the security breach therefore could include a) cloning, b) removal and c) reapplying of the tag. For discussion purpose, it can be denoted as *Da*, *Db*, and *Dc* for the three types of security breaches taking place in the “Direct” area.

The second stage “Associated” follows the multi-domain idea illustrated by Kim et al. (2007), where a single-domain model (“Direct” Level in RFID Lifecycle) was extended to a multi-domain model (“Associated" Level in RFID Lifecycle). Kim et al. focused only on EPC tag while this study will take a general approach and identify security breaches other than EPC tags. For example, shall a manufacturer tags RFID in the products it produces, its associated level could be its contracted logistics service provider and security breach could include j) tag

cloning, m) back-end attacks, and r) eavesdropping. In this case, the security breaches can be denoted as *Aj, Am* and *Ar*.

This RFID lifecycle model further extends security breaches to a third level, which is in an area that is uncontrolled and therefore security breaches could be difficult to control. For example, for the manufacturer with difficulties to control the retail shops selling their items. The security breaches identified in this level could include f) Disposal of RFID tag, which can be denoted by *Uf*, for RFID disposal breaches happened in uncontrolled areas.

MDSCRV Model for Jewellery Supply Chain

On the other hand, there could be cases where the retailer is the SC party which tags products with RFID for retailing automation purposes, and the tags are removed after the products are sold. This is very common in the jewellery SC. In this case, there will only be one stage, the "Direct" stage, as the RFID system owner uses the RFID only in the retailing domain of the SC, without any other domains in the supply chain involving the RFID tag.

6.5 Discussion

The purpose of this model is to enable a discussion of the security breach list that are originally discussed by scholars but in the context of a multi-domain SC, since the security breaches in direct, associated, and uncontrolled domains should be tackled differently. For example, eavesdropping in the manufacturing stage and for tags that are being disposed would have different security solutions, as a tag being disposed will allow more time for hackers to perform eavesdropping reading to the tag. Different solutions should be given to the same security breach in different domains on the SC.

The model, incorporating Kim et al.'s multi-domain model and the list of categorized security breaches by various scholars (as discussed in 6.3), should be given a new name that well represent both the work of Kim et al. and other scholars. It is hence named as MDSCRV Multi-domain RFID security model for discussion in this study.

6.6 Concluding Remarks

Based on the theoretical background, the multi-domain idea from Kim et al. and the comprehensive list of RFID security breaches from other scholars, a new model can be made to describe RFID security breaches in a systematic and hierarchal manner.

The comprehensive list of RFID security breaches retrieved from the scholar literature is results of individual observation from various scholars. Not any one of them has attempted to use a systematic way to analyse the various RFID security breaches. For example, which breach has a higher tendency to happen? Or which breach happens in which part of SC? By

combining the Kim et al.'s multi-domain idea, and the comprehensive list of RFID security breaches, one should be able to identify areas which a particular breach has a higher tendency to happen. This model should also be able to encapsulate the entire RFID Lifecycle, where Kim et al.'s model alone only focused in multi-domain but did not emphasize that the entire RFID Lifecycle has to be covered.

While the model can explain the different attack vectors of different RFID systems in different areas, discussion on the RFID security breaches is the main purpose of this model. A focal company should assign various security breaches to the three areas of the *tube.* Every different company could have different RFID security breaches, in different "Direct", "Associated" and "Uncontrolled" areas of the RFID Lifecycle.

This model, combining the literature from various scholars with a comprehensive list of RFID security breaches, the Kim et al. multi-domain model, and the idea of RFID Lifecycle where RFID has a definite start and end points in a particular SC, is created as the MDSCRV model. The next chapter will validate the vulnerability in this model retrieved from literatures by real world business mini cases studies.

7 RFID Breaches in Multi-domain Supply Chain

Research Question 2: In what way can current multi-domain security models be extended to address RFID security breaches across the supply chain?

7.1 Introduction

In chapter 6, a list of RFID security breaches from various scholars was identified and applied to a multi-domain environment that is suggested by Kim et al., which was given the name MDSCRV (discussed in 6.4.2). Although the MDSCRV Model has already been established considering literatures from various scholars, does that fit in to the real world business cases? Can the model be applied to all SC? A further understanding of RFID list of vulnerability in the SC industries is required to validate the MDSCRV model. This chapter aims at extending this model to one that can explain RFID security breaches in the longer RFID lifecycle LEI and shorter TEI environments. As detailed in Section 4.5.7 , the study of both LEIs and TEIs will ensure the result is free from "*sample biased*", and would not target on a way too simple or too complex SC environment.

The two chosen SCs have their own characteristics, as illustrated in section 1.11, both industries have key significance in the global trade, both financially and non-financially. Section 4.2.5 further suggested the study of a leading-edge industry (LEI) and trailing-edge industry (TEI) could give an unbiased understanding on the topic, as the wide spectrum of RFID usage allows the study of both long and short RFID lifecycle security breaches. For example, The jewellery industry, a TEI, uses RFIDs only for tracking and point of sales automation, while pharmaceutical industry, a LEI, uses RFIDs with far more sophisticated requirements in patient associations, drug, dosage, and cold chain verification. Later in the chapter, common and different features of LEI and TEI will also be examined and the differences in RFID breaches can be explained by an extended model.

This study corresponds to the design science step 3(a) Theory Building and 3(b) Framework Design. The RFID security framework has been built from the list of elements in Chapter 5 and the study performed semi-structured interview in reviewing whether all the RFID security breaches on the list are valid for SC. The validated security breaches form a shortened list that allows the framework to be more precise. The figure below shows the steps described in this chapter.

The steps described in this chapter follow the study design as shown in Figure 11; 3(a) Theory Building and 3(b) Framework Design. Factors of the MDSCRV Model were extended by incorporating the list of RFID security threats and shortlisted to the RFID security breaches in multi-domain SC. However, there is no solution provided for those security breaches. This chapter extends 3(a) Theory building to categorize causes and sources of these breaches. In addition, the causes and sources with their respective solutions will expand the MDSCRV model into an extended framework in step 3(b).

7.2 Method

Addressing RQ2 requires performing semi-structured interviews with 50 mini-case study targets, 25 for pharmaceutical and 25 for jewellery industry, as listed in Chapter 5. An interview script with 15 open ended questions have been drafted to allow discussions.

The questions are divided into four sections: Background section relates to general information about the company; IT and RFID systems section identifies the RFID systems being used in the mini-case study; Past experience of SC security breach, and more importantly, the RFID breaches percentage inside these breaches are studied by RFID Security Breaches section's questions; and finally security risks and operation framework that are not related to RFID systems are studied to understand whether the company has risk management and framework or performance benchmarking experience in the last section.

Background Related Questions		
No.	Questions	Rationale
1	What is the role of your company in the SC [example: trading firm, retailer, etc.]?	Determine suitability, and the controlling power of the mini-case in the SC.
2	If this "role" identified is recognized as a "domain" [parties along the SC – domain examples: raw material -> manufacturer -> logistics service providers -> importers -> retailers -> consumers]. Are there other companies in the same domain that you are aware of?	Determine involvement, allow benchmarking of other members in the same domain of results being studied to ensure results are bias-free
3	Who are the members you are aware of in the next "domain"? [these members will be followed up by semi-structured interview as well]	Determine relationships between the mini-case study targets, and controlled and uncontrolled areas, identify study targets on the same SC.
4	Approximately, how many employees do have access to the goods [and discuss any perceived implications about risk management]?	Determine human labor in the SC operations level.

IT and RFID Systems Related Questions		
No.	Questions	
5.	Approximately, how many IT systems do store information related to the goods [and discuss any perceived implications about risk management]?	Understand possible targets of security threats, as kinds of data (e.g. product and customer) residing in servers pose a security threats for hackers to attack.
6.	Identify the RFID systems in the goods [frequency level / writable tags / power source]?	Type of physical RFID tag (e.g. re-writable tags carry more data can be stored in the tag for intruders to overwrite the RFID; read only tags can cause intruder to hack server or clone tag)
7.	Identify the tagging location of the RFID [item / carton / pallet level]	Tagging position changes the difficulties in RFID re-applying. For example, bottom of reusable pallets to be read by forklift trucks are physically difficult to re-apply.
8.	Which of the following can best identify the goods [high value / fast moving / made to stock / made to order], [further discuss the value / product life cycle of your goods]?	Generally speaking, the higher the value, the higher the probability of the goods tempered; Fast moving consumer goods (FMCG) can be resold easier than tailor-made / made-to-order goods
9.	Discussion of who determine the use RFID security system [Buyer / Supplier / Other] and other factors	Study the controlled / uncontrolled area in a multi-domain SC. Solution found by uncontrolled domain might have business difficulties to deploy even if found.

RFID Security Breaches Related Questions		
No.	Question	
10.	Have your RFID system experience any security breach?	Previously involved with RFID security breach could mean a highly vulnerable system.
11.	Can you select the top 3 likelihood of damange and top 3 damaged level caused by the following issues? [select top 3 on Eavesdropping/Relay Attacks/Unauthorized Tag Reading/Tag Cloning/People Tracking/Replay Attack/Tag Content Changes/Malware/RFID System Breakdown/Tag Destruction/Blocking/Jamming/Back-end Attacks]	Likelihood of damange level from the findings of most likely and highest damage level RFID security vulnerability in general RFID systems. The items for choice are adopted from SCRV categories of RFID vulnerability (Table 11)
12.	Would you classify your financial implications respective to goods value in case of RFID security breaches [Likert Scale]	Higher financial implication goods have higher potential of breach, and multiple smaller valued breaches or a single higher valued breach could have different incentive study target to deal with such breach[33]
13.	Is there a security systems in place	if a security system is already in place, it could have targeted wrong source of security vulnerability due to wrong understanding of causes of breaches

Other Security Breaches Related Questions		
No.	Question	
14.	How does your company approach security risks not particularly related to RFID?	Further understanding of how security risk is being managed by the mini-case study target, e.g. does mini-case study acknowledge, retain, or transfer risks, say to insurance companies
15.	Not particularly related to RFID systems, does your company use any operation framework or performance measurement mechanism such as ISO, Benchmarking or Six Sigma	Operation framework or performance measurement systems in means performance measurement mechanisms in place for further study.

Table 23 Semi-structured interview questions and rationale

[33] Aven and Zio (2018) summarized risk assessment and management by many authors and suggested risk transfer as a way to manage risk.

7.3 Results

Twenty five results from each of the two study groups were obtained (details discussed in 5.3), and studies were performed for identifying RFID security breaches and incidents before and after RFID application to the SC. The inclusion of RFID security breaches study before the application of RFID framework can single out effects of the framework on RFID security breaches.

There are security breaches mentioned in the semi-structured interview but not in the MDSCRV model. The differences shall first be noted by performing a comparison study, and then this list of differences should be mapped back to the MDSCRV model in order to fully capture the security breaches in the multi-domain arena. For security breaches that are controllable, the SC practitioner (in the direct domain) should have the ability to control the problem in their own business operations. On the other hand, if the security breaches are in the uncontrolled domain, the SC practitioner should be able to convey the breaches to the SC partner who can control them.

7.3.1 Use of RFID by the Mini-case Study

The twenty-five companies were asked whether they have applied RFID in their domain, and the results are tabulated in Table 24.

	Domain (Interviewed)	RFID Applied in Domain
Jewellery	Component(5)	No
	Assembler(5)	No
	LSP(5)	No
	Distributors(5)	No
	Retailers(5)	Yes
Pharmaceutical[#]	Raw material(2)	No
	Manufacturer(6)	Yes
	LSP(3)	Yes
	Importers(9)	Yes
	Retailers(5)	Yes

Table 24 Number of companies interviewed, with RFID applied in respective domain

#80% of retailers are not equipped with RFID readers. 60% of pharmaceutical manufacturers are not using RFID in item level.

The pharmaceutical industry has broadly adopted RFIDs whereas the jewelry industry has not, although retailers have embraced this technology due to the need for point of sale (POS) systems and antitheft purposes rather than to deliver SC management benefits. The use of RFIDs in jewelry industry simply involves scanning the tag when the jewelry is sold, in order to record the sales and charge the customer with correct charges only. Antitheft purpose is also accomplished by installing Electronic Article Surveillance (EAS) systems in jewelry display cabinets and shop entrances to trigger alarms when there is any jewelry leaving shop without being paid for.

7.3.2 RFID Implementation and Security Breach Incidents

The companies were also asked on the SC security breaches in terms of value involved and number of incidents, both before and after RFID implementations (if it has been applied). Its difference on value loss is shown in Table 25.

	Domain	Value Lost % (Incidence)*	
		Before	**After****
Jewellery	Component	2.3%(1.2)	
	Assembler	1.5%(0.5)	
	LSP	0.4%(0.2)	
	Distributors	1.8%(0.1)	
	Retailers	1.8%(86)	2.3%(70)
Pharmaceutical	Raw material	0.3%(1.2)	
	Manufacturer	0.2%(0.5)	0.2%(0.5)
	LSP	0.1%(3.2)	0.1%(2)
	Importers	2.1%(5)***	2.0%(3.3)
	Retailers***	3.1%(112)	3%(103)

* Lost percentage is approximated based on product value traded.

** Security breach occurrence is averaged regardless of the size of the company for over a one year period, companies with less than one year RFID application has incident calculated pro-rata. Some companies apply RFID systems together with computer inventory management system over previously manual inventory management and accounting.

*** For pharmaceutical products, retailers can call for exchange product from importers shall product shelf life is over, and such importer's lost is not accounted as these are not security breaches.

Table 25 Incidents of Supply Chain Security Breaches Before and After RFID Implementation

It can be observed from Table 25 that the security breaches have not been reduced significantly even after implementing RFID. This observation is reflective of the need to address the security breaches in RFID based SCs, as this shows that although there are benefits using RFIDs, its advantage will be offset by the vulnerability of RFID while this is introduced to the SC. Therefore, the urge to study security breaches related to RFID is obviously necessary so that practitioners could identify the causes and sources of these breaches.

7.4 Analysis

The primary data collected from semi-structured interview echoed the literature and industrial journals reviewed on the background of the two SCs. They have different usage of RFID and new findings were observed.

7.4.1 Findings from Jewellery Supply Chain Semi-Structured Interviews

The jewellery industry has a complex and fragmented SC process, as discussed in section 1.11.1, that starts from raw materials to the retailers. The raw material of jewellery is sourced from different countries; in which along the jewellery SC there are many small artesian jewellers and corporate retailers, from mines to smelters to end customers. As a result, it is difficult to trace from the mine of origin. Although the use of RFID is supposed to able to be traced to its origin, real world RFID applications in raw material domain were not found, and

the applications of RFID are owned by brand name owners. Such application is illustrated in the diagram on the right of Figure 10.

Indeed, there are reasons to apply RFID in the early stage of a SC. For example, the Kimberley Process Certification Scheme requires certified members to claim diamonds they sourced are legally obtained and the production process is free from human rights abuses. In addition, Responsible Jewellery Council (RSJ)[34] requires members to use audited facilities and it is necessary for products to be certified by Chain-of-custody certification system through their SC. That means most of the stages in jewellery SC are clearly stated and raw materials are traceable throughout the production process till the checkout of products in stores, but without the adoption of RFID technology.

Using RFID in the jewellery industry eliminates error-prone tasks such as manual counting and item-level scans. This benefit has increased adoption of RFID systems and compliance, also resulted in a variety of business management efficiencies. Using RFID can reduce process steps, optimize labour resources, avoid errors, and enhance data collection. However, it is observed that RFID in jewellery industry has a short lifecycle and is just used by the retailers instead of end-to-end throughout the SC, which consist of domains categorized as component, assemblers, logistics services providers (LSP), distributor and retailers. Table 24 illustrates the Jewellery SC which does not adopt RFID until the shop level by individual retailers. The retailers' systems are implemented as a single domain system.

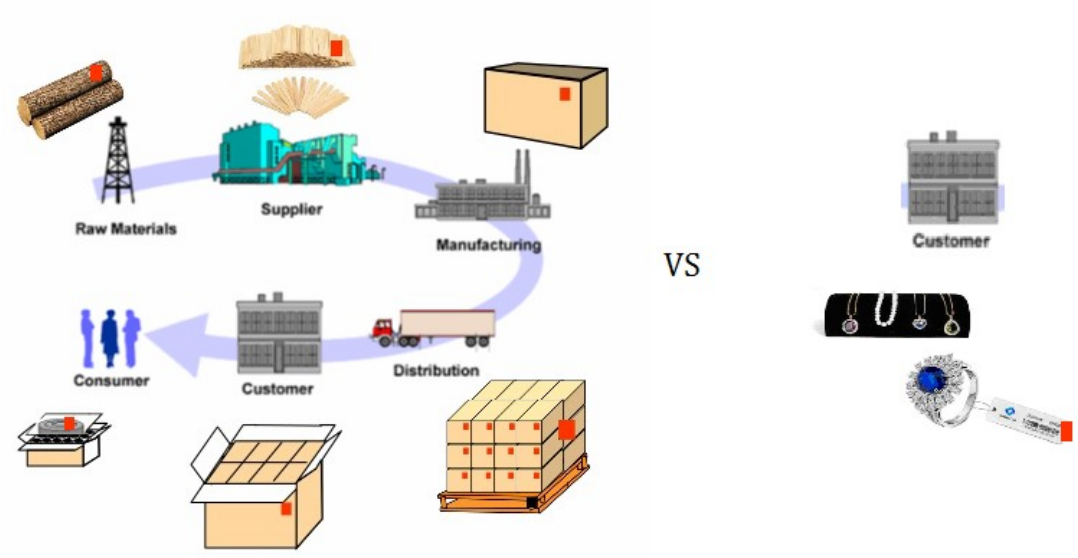


Figure 10 LEI and TEI Supply chain with RFID application illustrated in a diagram side by side. A long RFID lifecycle for LEI in the left and short RFID lifecycle in the right for TEI. Diagram updated from Figure 2 originally adapted from The Progress Group (2001) http://www.theprogressgroup.com/publications/wp_images/fite1.gif.

[34] Responsible Jewllery Council (RSJ), which comprises of over 850 organizations globally (RSJ, 2016).

7.4.2 Findings from Pharmaceutical Supply Chain Semi-Structured Interviews

On the other hand, the pharmaceutical sector tends to implement RFID in an end-to-end manner. A typical pharmaceutical SC consists of domains categorized as raw material, manufacturer, LSP, importers and retailers. As discussed in section 1.11.2, the pharmaceutical SC has a huge impact on health-related goods and therefore can result in human being life-and-death consequences. Even though the products (i.e. drugs) might be less expensive compared to an average SC, it's more important than an average SC in the sense that if anything goes wrong, the results could be devastating. RFID systems should naturally be used in important SCs like this one, for e.g. verification of drugs all along the supply chain can be done through RFID, like verifying a drug before patient's intake in a hospital. Because almost every person in the world use pharmaceutical drugs, so logically its influences are global too. Even for late adopters of RFID in the industry, practitioners have a common consensuses to implement RFID systems as soon as possible.

The industry's general perception to invest in new technology is different from that of the jewellery industry, given the profitability of the industry, there is no doubt that everyone in the pharmaceutical SC is willing to pay a lot of effort to improve business management, taking into account the cost of any product recall and the degree of damage. As section 1.11.2 suggested and reflected in the 12 case studies from semi-structured interviews (reported in 7.3.2) and 15 cases from focus group members (reported in section 8.4.1, and summarized in Table 34), poor quality control of pharmaceutical SC could lead to serious consequences, include counterfeiting, efficacy of drugs, to name a few.

Technology certainly is one of the solutions to maintain the pharmaceutical SC performance. "Smart packaging" is one of the drivers to meet such needs, which is a convenient anti-counterfeit solution with the vision to improve SC efficiency and safety in pharmaceutical packaging by increasing product availability and ensuring product quality. This driver alone increased the RFID tag market in the pharmaceutical sector from US$100 million in 2008 to US$2.1 billion in 2016[35].

Most pharmaceutical SCs adopted RFID right from the start at manufacturing stage, until it reaches the final consumer's hand, as illustrated in diagram on the left of Figure 10. The importer, for and on behalf of themselves or the manufacturer (or the brand owner), typically hires sales representatives to visit the retailers. A pharmaceutical representative will generally be assigned to visit clinic physicians, hospitals, drug stores once every few weeks. Representatives often have to deal with 200 physicians, 3 hospitals, or 300 drug stores. For

---

[35] "The Potential for RFID in Pharmaceuticals", http://www.rfidupdate.com/articles/index.php?id=1195, last accessed July 25, 2018

each visit, samples are often delivered by hand or through logistics service providers. Once orders have been placed, the products are delivered by logistics service providers on a different visit. The retailers (hospitals, clinics, and drug stores) would then need to verify by manual count.

It is worthwhile to note that pharmaceutical products are sold in bonus terms or in short "terms". For example, drug A might be sold in quantities of 50 with bonus 40, which are always denoted as 50+40, with a standard unit price. This means the unit price are unchanged no matter if the retailer is a hospital or a small medical clinic, and the pricing is controlled by the "terms". This incurs difficulties in stock receiving as the quantity could be different every time and might not match the ordering quantity, while in other businesses such quantity can be easily traced. To deal with this situation, RFID system has been implemented by some pharmaceutical companies, and this system is being utilized in the entire pharmaceutical SC including hospitals and drug stores. The use of RFID could be a precaution of such errors.

For hospitals, the use of RFID usually emphasizes more on patients' safety, employee efficiency and inventory cost control. There is a high incentive for hospitals to adopt the RFID being tagged by pharmaceutical manufacturers. RFID automation in the pharmaceutical SC can save thousands of dollars through optimizing labour, reducing supply waste and commitment costs while providing data-driven insight to optimize revenue.

A typical pharmaceutical product manufacturer would apply RFID by placing small RFID tags on drug packs. An RFID tag consists of an antenna and a chip that serves as a unique identifier. By the use of a handheld scanner or card reader, product information and data such as manufacturer, drug name, lot number, and expiration date can be displayed. This information is retrieved by the handheld scanner wirelessly linked to a database server, via its associated unique identifier in the relational database.

Once the product information is placed in the relational database, one can use the data throughout the entire RFID lifecycle. The pharmacy is equipped with automated hardware, including kit and pallet management workstations and inventory management control temperature cabinets. These hardware systems can automatically read RFID tags for all inventories which aid human operation. For example, a typical stock take by RFID in a hospital for a particular subset of drugs would take 3-7 seconds instead of manually counting that takes 15 minutes.

RFID systems identify any lost, expired or expiring drugs, so replenishment can be done quickly and accurately, saving human lives by eliminating medication errors. Alerts are programmed to support optimized workflows and alert medical practitioners in case of

inappropriate use of drug for patients, say weight and dosage mismatch or inappropriate use of drug due to medical history.

Computer systems can utilize RFID to control the temperature in the SC, say in warehouses, and link these data up to online and high visibility inventory management systems. These systems update the inventory status whenever the cabinet door or station drawer opens or closes, maintain a permanent stock quantity by enabling auto- notifications to be sent to appropriate medical practitioners to replenish drugs that are going to run out of stock.

All in all, pharmaceutical SC has been taking advantage in the entire RFID lifecycle from the RFID that is tagged by the pharmaceutical product manufacturer. Last but not least, in all RFID solutions, data is provided through a powerful reporting suite to improve medical practitioners' self-confidence and enable informed decision making.

7.4.3 Proposed Conceptual Model

Some breaches are common in mini-case study results, and some of them are in the same category; Some of these breaches are with the same root cause or from the same source, and some have similar solutions to close vulnerability loophole. Therefore, a proposed conceptual security framework can explain these results, and this framework can identify and categorize major causes and sources of the studied RFID security breaches. These causes and sources are then analysed by literature review on various scholars based on the identified causes and sources of the RFID security breaches.

This conceptual framework is a three step model that can be adapted to explain causes and sources of RFID security breaches. It contains three steps as shown below and illustrated in Figure 11. The funnel illustration is adopted because the causes and sources in the policy framework can be deduced from the security breaches in the process of going through the model.

(1) Identify and categorize the RFID security breaches in SC (Blue to Green)

(2) Identify the causes and sources of RFID security breaches (Green to Cyan)

(3) Categorize the causes and sources in the policy framework (Cyan to Yellow)

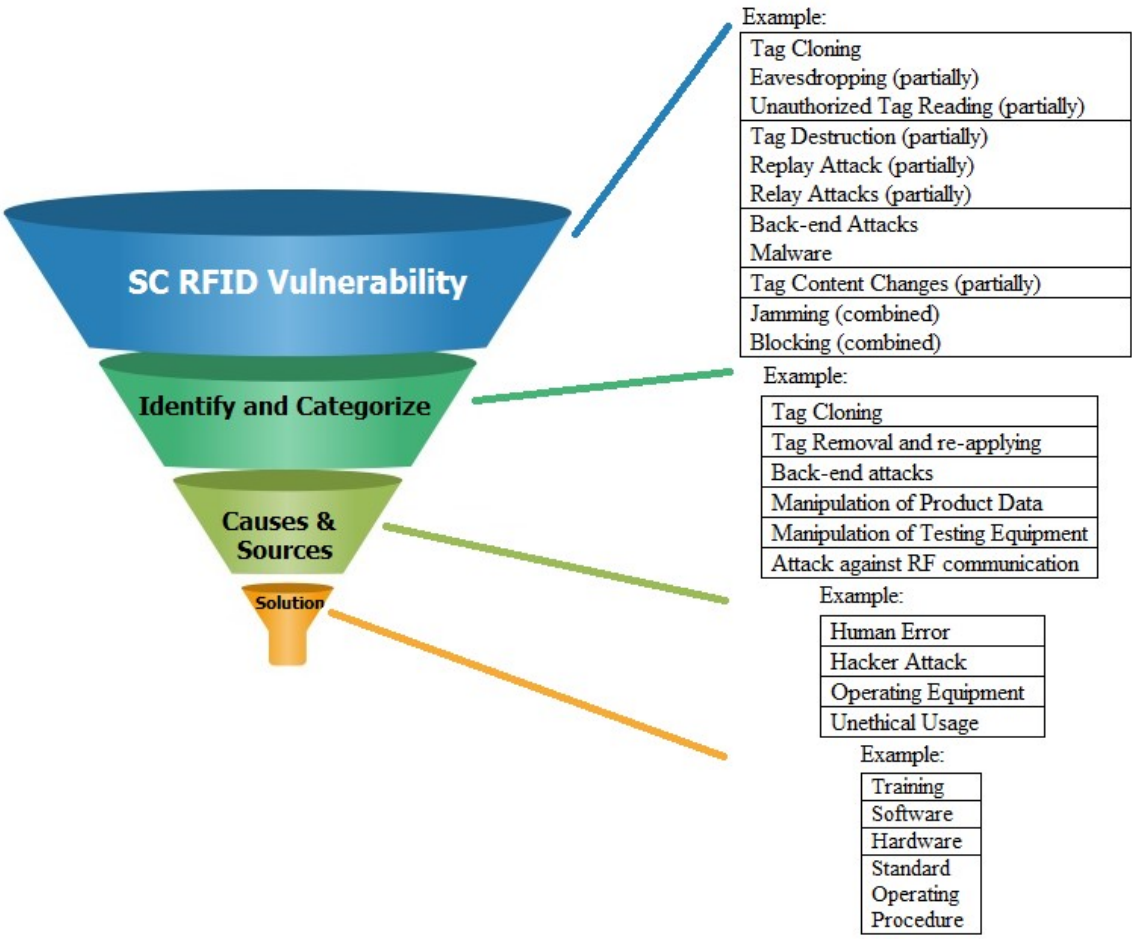


Figure 11 Proposed conceptual model to explore RFID Vulnerabilities in multi-domain supply chain (Left). Examples provided are reflected from results from section 7.4.4 and 7.4.11 (Right).

7.4.4 Top Security Vulnerabilities

The list of security breaches should be revisited, to update the list of RFID vulnerability in the MDSCRV model which originally categorized by Rotter (2008) (discussed in section 2.6) and shortlisted to SCRV (discussed in section 6.3). The semi-structured interview consists of 50 company mini-case study targets, spanning across various company sizes and in several of domains in SC, should be a better representation of RFID security breaches in SC. There are items in MDSCRV that are not found in the semi-structured interview, or vice versa. Hence there is a need to trim down the MDSCRV model in order to allow SC practitioners to tackle RFID security breaches in a more targeted way. A list of six security breaches can further be categorized to give a meaningful analysis for RFID security breaches that are specific to the SC, and they have been categorized by introducing new categories combining old categories with similar causes, and ignoring categorizes that do not exist.

Some of MDSCRV model's items are combined, such as back-end attacks is combined with malware and back-end attacks as both happens at the same time in all semi-structured interviews. Some items are covered in other categories, such as RFID system breakdown. The proposed new categories are discussed in the below sections and summarized in Table 26.

Tag Cloning

Tag cloning (discussed section 2.6.5) was featured in both the MDSCRV list and the semi-structured interview, and since it requires the same frequency of tag to be cloned, and most likely in a large batch of read only tags, for the cases with read only tags, the RFID security breach is relatively well-planned and in bigger scale .

Tag Removal and Reapplying

A tag removal RFID security breach is simply removing the tag to make RFID reading impossible (section 2.6.15). When a tag is simply removed, SC operators will spot that the reading of the RFID is unsuccessful, while a good one moves through a reading point. In case of the tags being removed and reapplied, the goods' identity is replaced by the original tagged goods (section 2.6.16). The MDSCRV model did not address both breaches, while the closest one is tag destruction (section 2.6.10). Tag destruction is the act to destruct a tag that is applied on an RFID. Without a tag a product's existence in the SC may be undetectable. For example, in a warehouse loading dock where pallets are tagged with RFIDs, missing a tag could mean an entire pallet missing as there is no tag to be scanned, or in a supermarket a missing tag might result in product lost due to tag missing in checkout counters. In some logistics operating environment, goods' existence is being detected by another mechanism, and therefore a missing tag might trigger the exist of an unknown object . For example, the Hong Kong Asia Airfreight Terminals Limited has installed RFID systems in identifying trucks to pick up airfreight goods with RFID tags hanged on the reverse mirror in the driving cabin, and for trucks without such tags parking in the loading bay, coil loops are installed in the ground of the parking bay in order to detect the existence of any trucks even without the RFID tag. However, this additional detection is for detecting tag removal in general but whether the tag is being destructed as suggested by MDSCRV is not a major concern.

There is no tag destruction reported from the semi-structured interview while MDSCRV model identified tag destruction being a major RFID security breach. In addition, the case of tag removal is not the same as tag destruction, in particular when a tag can be reapplied. Since the semi-structured interview mini-case study has RFID security breach of tag removal and reapplying happening simultaneously, they are considered as one single breach and being studied together.

Back-end Attacks

While attacks against servers exist in both MDSCRV and the mini case studies, and malwares are common ways of attacking information systems, MDSCRV model explicitly distinguished back-end attacks from servers and malwares which commonly attack client machines. In the mini-case study targets, backend consists of repository of everything for the information systems, including all data in the Enterprise Resource Planning (ERP) software. ERP software contains SC information from one domains to another, including upstream SC to downstream. Examples of such information include product planning, manufacturing, inventory management, marketing, shipping, and payment. Though, purposely installed of malware to breach RFID systems were not reported from our semi-structured interview. As the attacks are not specific to any systems, the extended framework should not categorize such attacks particularly to database servers or backend attacks, but generalizes these attacks as attacks against servers.

Manipulation of Product Data

Manipulation of product history is a combination of security breaches including tag content change and manually changing database records. Some SC RFID systems are able to retrieve product information from the tag without the need to interpret tag information from database, and a hacker can solely perform a tag content change (Section 2.6.7) to manipulate product history. Other systems require an update to database records of product's data stored. However, this should not be considered as a backend attack by a hacker as the user who update database records are practitioners in the SC. Since both breaches achieve the goal of manipulation of product history, they can be considered as one single category in SC RFID systems.

Manipulation of Testing Equipment

The issue of manipulation of testing equipment does not exist in the MDSCRV model. However, in the study it was reported that some logistics operators manipulate testing equipment to satisfy their own needs. Two cases were reported in this study, where testing equipment was manipulated by manually changing the data in offline handheld RFID reader, and manually amending the reading angle of RFID reading devices that are mounted in a logistics environment. Study of this behavior is important as systematic enhancement, for example, use of online reading equipment which sends data to servers immediately after read, or the act of prohibiting users to change data in an offline scanner, could make such manipulation impossible. For mounted RFID reading devices, cages can be used to protect such equipment to ensure 100% RFID scanning.

Attack against RF Communication

The security breach "attack against RF communication" is a combined result of RFID vulnerabilities in MDSCRV. Jamming and blocking of signals are both causes of this

vulnerability, and they did not exist alone. Most RFID security breaches targeting low frequency RFID tags have higher immunity to EMI, as discussed in the chapter 2 literature review section. Civilian uses of RFID devices do jam the signal, and sometimes the signals are blocked by such devices as they are made by metal. However, in the case of semi-structured interview, higher frequencies of RFID tags are being used. Blocking is not reported from the semi-structured interview apart from operational equipment jamming of radio frequency signals. In discussion of blocking, one cannot omit the incidents of tempering RFID antenna, which can be discussed in a dichotomy. The first way is destruction of the physical antenna. RFID readers have external antennas and the destruction can be performed easily. The second way is to block the RFID antenna in the RFID tag, which is also a way of blocking. There is no RFID security breach on antennas in the semi-structured interview but MDSCRV model has recorded antenna as vulnerability in RFID systems.

Categorized SCRV	**Mapping to MDSCRV RFID Vulnerability**
Tag Cloning	Tag Cloning Eavesdropping (partially) Unauthorized Tag Reading (partially)
Tag Removal and re-applying	Tag Destruction (partially) Replay Attack (partially) Relay Attacks (partially)
Back-end attacks	Back-end Attacks Malware
Manipulation of Product Data	Tag Content Changes (partially)
Manipulation of Testing Equipment	
Attack against RF communication	Jamming (combined) Blocking (combined)
Does not exist in semi-structure interview cases	*RFID system breakdown*

Table 26 Comparing list of RFID security Breaches in MDSCRV Model and the extended framework

7.4.5 Top Security Breaches

The semi-structured interviews found that different companies identified different top RFID security breaches, which are listed in Table 27. In evaluating RFID security systems for a particular industry, the first step would be to identify and categorize such RFID security breaches for that industry. For instance, the interviews with case companies of the pharmaceutical industry manufacturers identified tag cloning, tag removal and reapplying, back-end attacks (breach item I / II / III) systems to be the top three RFID security breaches in the SC. Different domains in the SC could identify different top RFID security breaches, for example the logistics service providers had identified back-end attacks, manipulation of testing equipment, and attack against RF communication (breach item III / V / VI) instead.

Category	Security Breaches	Examples
I	Tag cloning	Cloning
II	Tag removal and reapplying	Removal and/or Reapplying
III	Back-end attacks	System software and hardware
IV	Manipulation of product data	Including database manipulation
V	Manipulation of testing equipment	Handheld and gate scanners
VI	Attack against RF communication	RF signal jamming

Table 27 Top Security Breaches and Examples

The top security breaches are calculated by assigning mark 3 / 2 / 1 to the top three choices of breaches the domain subjects replied. 3 marks assigned to the top choice, 2 marks assigned to the second, and 1 mark to the least. By adding up marks in each category, the study extracts the top three marks which would in turn became the top three security breach concerns.

The semi-structured interview paid particular attention to "Rank the top 3 concerns (in terms of likelihood of damaged) caused by the following issues" and "actual security breach incidents happened, before and after RFID application". This research used the same terms and phrases in the semi-structured interviews for jewellery and pharmaceutical operators to facilitate fair comparison and results are summarized in Table 28.

	Domain that applied RFID (Interviewed)	Top Security Breaches					
		I	II	III	IV	V	VI
Jewellery	Retailers		1	2			3
Pharmaceutical	Manufacturer	1	2	3			
	LSP			1		2	3
	Importers			2	1		3
	Retailers				3	2	1

Table 28 Rankings of Security Breaches Identified by Jewellery and Pharmaceutical Industries

A follow-up question was then asked to each response, for details regarding to the RFID security breach. Illustrated below are the cases that are retrieved from the semi-structured interviews. Following notations are used to capture the response of each domain for each breach category for both sectors.

These responses were useful in understanding in detail how a breach is defined and encountered differently by each domain in two types of industries.

7.4.6 Domain Specific Top RFID Security Breaches

There are a total of 15 top security breaches identified, and are best represented by the case studies as below (3 each in JA and PB/PC/PD/OE). It is worthwhile to note that the domain

where the vulnerability came from and the RFID system owner are not always the same. For example, a pharmaceutical RFID system could have security breach that occur in a pharmacy. This leads to a more complex problem (discussed in Chapter 8) with cases summarized in Table 29.

JE1[36] - Tag removal and reapplying

The RFID tags are carried on a piece of small "paper item tag" that attaches on the piece of jewellery. Upon customer purchase of the piece of jewellery, the tag is removed. Multiple incidents happened when the customer finally decided not to purchase multiple pieces of jewellery, and the "paper item tags" requires to be reattached to the pieces of jewellery. This is the case when the tags are mistakenly removed and reapplied.

JE2 - Attack against servers

An incident reported where jewellery companies' IT system were being attacked by a hacker trying to retrieve all properties of all jewelleries. This hacker wanted to build a database containing all image of this jewellery company, for building up an online catalogue. At that point, RFID tag serial numbers were also copied.

JE3 - Attack against RF communication

RF communication has always been jammed as a result of electromagnetic interference. While this are not planned attack, mobile phones, liquid, computer systems, are ranked top three in the jewellery retailing environment

PB1 - Attack against RF communication

---

36 Notations used are as follows:

J: The Jewellery supply chain

P: The Pharmaceutical supply chain

A-E: Different domains of supply chain, with 'A' for the most upstream supply chain domain and 'E' for the most downstream domain of the supply chain that is the retailer. For pharmaceutical supply chain A/B/C/D/E would stand for Raw material/Manufacturer/Logistics Services Providers/Importers/Retailers, and for jewellery supply chain, A/B/C/D/E would stand for Component/Assembler/Logistics Service Provider/Distributors/Retailers respectively.

1-3: The numbers are used to indicate top RFID security breach by each domain

Example: For instance, "JA1" would be the topmost (1) security breach for the first domain, (component, A) in the jewellery (J) industry.

For instance, "PC2" would be the second (2) security breach for the third domain (Logistics Service Providers, E) in the pharmaceutical (P) industry.

Similar to the jewellery retailers, RF communication has always been jammed as a result of electromagnetic interference by mobile device users in the outsourced warehouse of the pharmaceutical company. The outsourced warehouse supposed to perform cargo receive for the pharmaceutical company with the use of RFID as a mean of cargo receipt approval, shall the purchase order number exists in the system. The jammed electromagnetic interference caused manual work in seeking for cargo receipt approval, and the system did not provide improvement in operation automation but instead caused confusion.

PB2 - Manipulation of testing equipment

Handheld scanners were used to test whether a pharmaceutical product is parallel imported or genuine and warning information will be displayed in a screen in a drug store. A drug store receives periodic check from drug importer to ensure only genuine product is being sold, in order to be branded as a genuine goods distributor. An interviewee reported drug store next door was caught selling parallel imported drugs but the periodic testing staff from the drug importer manipulated testing equipment records in testing equipment before returning such equipment to office.

PB3 - Manipulation of product data

Forgery of product data has been reported where sample drugs with RFID tags marked as “samples” are being removed in order to fake product as regular drug, in order to charge patient with “samples - not for sale” products. This case exists in Hong Kong, where the medical clinics can dispense drugs by a medical doctor without need of a pharmacy or pharmacist.

PC1 - Manipulation of product data

Importers are required to reassess the due date of product, and sometimes will extend the best before date after reassessment. Manipulation of product history is being done manually to the database, and human errors were spotted.

PC2 - Back-end attacks

An incident reported where pharmaceutical importer IT system being ran in the pharmaceutical point of sale system in a pharmacy were being attacked by an IT company providing cloud computing software-as-a-service. The IT company is trying to retrieve all properties of drugs imported to build a database containing all drug constituencies, as drugs manufactured by different manufacturers are sold under brand name but could have similar active ingredients. This cloud computing software-as-a-service is targeted for access of individual medical physicians to access, and in the process, RFID tag numbers are also copied in the same database.

PC3 - Attack against RF communication

Similar to the pharmaceutical retailers, RF communication has always been jammed as a result of electromagnetic interference by mobile device users. This happens in the outsourced warehouse of the pharmaceutical importer. The system is used for identifying the earlier expired items when drug is shipped to the pharmacies. The closer in proximity an RFID scanner is from the first expired drug will sound a higher frequency alarm. The signal jamming cause misidentified drugs.

PD1 - Back-end attacks

Cases of attack against IT web server have been reported by logistics service providers. Although there is no evidence and it is not believed that the attack is related to RFID information. The web server containing RFID information has been downed due to Denial of Service (DOS) attack.

PD2 - Manipulation of testing equipment

All shipments going through a logistics service provider has to go through 12 points scanning, and pharmaceutical items get higher priority in an airfreight unit load device unstuffing process. At peak time sorting or flight delay, airfreight logistics ground handling staffs purposely changed the angle of a scanning device in order to have urgency override importance handling of goods to avoid delay.

PD3 - Attack against RF communication

Similar to the pharmaceutical retailers, RF communication has always been jammed as a result of electromagnetic interference by mobile device users.

PE1 - Tag cloning

The pharmaceutical manufacturer has their own proprietary format of RFID number system and is the largest customer of the RFID system provider. In order to cater for needs of smaller clients who could not cater for a single run of RFID tags production, the RFID vendor cloned the tag format to sell to these smaller clients when they are making a production run. It was reported even the tag serial numbers could be completely identical, which could cause issues although there were no lost reported from this incident.

PE2 - Tag removal and reapplying

Automatically tagged RFID on manufacturing item boxes were found mistaken. It required manual removal and reapplying, which could again cause issues although there were no errors reported from this incident.

PE3 - Back-end attacks

Similar to pharmaceutical logistics service providers, IT web server containing RFID information has gone through Denial of Service (DOS) attack with no indication the attack aimed at the RFID information.

	Security Breach	RFID Owner	Vulnerability From	Domain
JE1	Tag removal and reapplying	Jewellery Retailer	Jewellery Retailer	Direct
JE2	Back-end Attacks	Jewellery Retailer	Jewellery Retailer	Direct
JE3	Attack against RF communication	Jewellery Retailer	Jewellery Retailer	Direct
PB1	Attack against RF communication	Pharmaceutical Manufacturer	Outsourced Warehouse	Associated
PB2	Manipulation of testing equipment	Pharmaceutical Manufacturer	Pharmacies	Uncontrolled
PB3	Forgery or manipulation of product history	Pharmaceutical Manufacturer	Medical Clinics	Uncontrolled
PC1	Forgery or manipulation of product history	Pharmaceutical Manufacturer	Drug Importer	Associated
PC2	Back-end Attacks	Drug Importer	Drug Importer	Direct
PC3	Attack against RF communication	Drug Importer	Outsourced Warehouse	Associated
PD1	Back-end Attacks	Logistics Service Provider	Logistics Service Provider	Direct
PD2	Manipulation of testing equipment	Logistics Service Provider	Logistics Service Provider	Direct
PD3	Attack against RF communication	Logistics Service Provider	Logistics Service Provider	Direct
PE1	Tag cloning	Pharmaceutical Manufacturer	RFID System Provider	Direct
PE2	Tag removal and reapplying	Pharmacies	Pharmacies	Direct
PE3	Back-end Attacks	Pharmacies	Pharmacies	Direct

Table 29 Multi-Domain RFID Security Breaches Cases with Vulnerability Originated Domain Highlighted

Through the observation, it is clear that RFID breaches could be very different in different SCs. Some of them have similar causes/sources or effects, but the breaches details could be very different, while others could appear in earlier or later stages in different SCs. Exploration to the causes/sources of these breaches needs to be carefully planned in order to categorize them and address implications. Table 29 summarized the security breaches, RFID system owner, company which the vulnerability came from and the domain relationship to the RFID system owner.

7.4.7 Common Features between LEI and TEI

Both LEI and TEI the study has chosen are SCs with huge implications. Pharmaceutical is an LEI and its SC has high non-financial implications shall the SC is compromised. For example, a drug that has to be shipped under temperature control, or in a cold-chain, could have caused lives if the drug is shipped under unintended temperature. On the other hand, the TEI selected has high financial implication, which is an equally important SC comparable to the LEI counterpart. Jewellery SC is an example that has high financial implications, but would be considered trailing edge in SC technologies. Products shipped could be raw material, including gold, diamonds, and gems. Theft or other security breaches are very common in this industry.

Both LEI and TEI are mission critical SCs. Jewellery SCs are critical as the longer lead time they have, the higher capital cost is being held in the SC, which increases business costs including financing and opportunity costs. Pharmaceutical SCs are equally critical. Drugs have

limited shelve lives: the longer pharmaceutical SCs drag on, the shorter time the drugs will remain consumable. Therefore, good management of both pharmaceutical and jewellery industries have always been discussed by scholars (as reviewed in sections 1.11.1 for LEI and 1.11.2 for TEI).

7.4.8 Differences between LEI and TEI

There are many differences between LEI and TEI RFID usage. The major difference is that application of RFID to the TEI is limited. Most TEI retailers can add RFID as a tool for security and item tracking, and this application is within the controlled environment in the retailing domain. Item numbers can be implemented easily without communication between multi-domain partners, and the destruction of the RFID tag can be done as a paper tag is always used alongside with the jewellery, unlike the pharmaceutical case where the RFID is inside the layers of the paper boxes.

In the upstream SC, RFID applications are simply missing. Most SC practitioners would outsource the security of the goods by risk transfer, or simply purchase insurance to cover any loss if security breaches happen. Some logistics service providers note that when RFIDs are attached in other logistics companies in the SC then it is possible to incorporate RFID with other domains in the SC, such as reusing the number in the RFID tag in the logistics process.

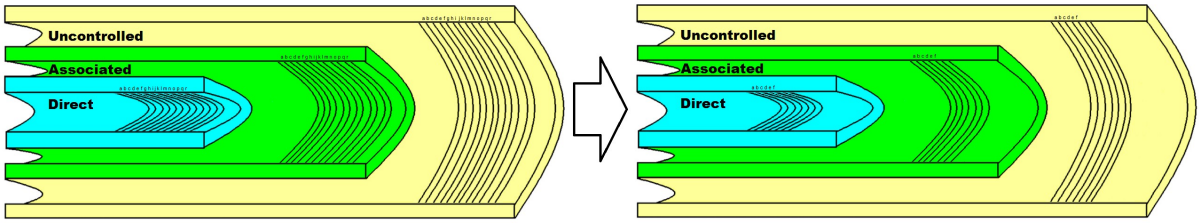
7.4.9 Differences in RFID Security Breaches in LEI and TEI

There are differences in the RFID security breaches in the LEI and TEI. LEIs are in the leading position of RFID applications and the RFID lifecycle is longer than that of the TEI. For example, the pharmaceutical industry has RFID tagged when the pharmaceutical product is being manufactured. However, the jewellery industry, being a TEI, has RFID tagged by the retailers in the final retailing stage of the SC only. Differences in the terms of the RFID Security Breaches can be explained by the Kim et al. multi-domain theory, stating that RFID applied in different domains in a multi-domain SC can have different RFID security breaches. TEI RFID security breaches that are caused by operations of an active human operator, such as tag removal and reapplying, manipulation of product or testing equipment, the human operator is more likely to have awareness of such breaches. While some of them might not have unethical intention, there were reasons behind such breaches (for example, ignoring alerts in peak time logistics sorting). In LEI RFID security breaches, associated or uncontrolled domains could have the same security breach, but the involving companies were not aware of the RFID system at all, as the system is not owned by them. On the other hand, for passive security breaches, such as back end attacks, attacks against RF communications, tag cloning, happen less in terms of count in TEI as the operation is smaller and the domain has full control of the environment. The differences between LEI and TEI RFID security breaches captured by

the semi-structured interview are mapped into the MDSCRV model and categorized by the causes and sources (discussed in 7.4.3, conceptualized in Figure 11).

7.4.10 Mapping RFID Security Breaches to Vulnerability List

The vulnerability list from SCRV, updated from Rotter's (2008) by reviewing various scholars' literature, is the starting point of this update. This is needed because more specific RFID vulnerability to SC should be used for this study. This list is now further refined by the results of this study to concentrate on vulnerability factors of multi-domain RFID systems. There is a need to update the list to contain only SC RFID vulnerability as discussed in Section 7.4.4. Figure 12 is an update of Figure 9 with the results from the semi-structured interview on the mini-case studies and shows a more comprehensive model for SC practitioners.



Security Vulnerabilities (SCRV)
Eavesdropping
Relay Attacks
Unauthorized Tag Reading
Tag Cloning
Replay Attacks
Tag Content Changes
Malware
RFID System Breakdown
Tag Destruction
Blocking
Jamming
Back-end Attacks

Security Vulnerabilities (Semi-Structured Interview)
Tag Cloning
Tag Removal and re-applying
Back-end Attacks
Manipulation of Product Data
Manipulation of Testing Equipment
Attack against RF Communication

Figure 12 MDSCRV Model with RFID vulnerability updated from semi-structured interview results

7.4.11 Causes and Sources in the MDSCRV Model

The semi-structured interview has provided insights into possible security breaches in the multi-domain. However, the pre and post RFID application did not reduce SC security breaches (tabulated in Table 25). Although RFID introduced benefits to the SC, such as the ability to track and trace the product, it also introduced vulnerability from the usage of RFID.

If all the security breaches encountered by domains of SC are observed, one can see that human related issues are the causes of some of these security breaches. For some types of breaches human errors are involved while reapplying the tag (JE1), manipulation of product data (PB3, PC1), tag cloning (PE1), tag removal and reapplying (PE2) or skipping the inspection and scanning by manipulation of testing equipment during rush hours (PD2). Hacker attack has also been spotted, as seen in attacks to internal IT systems in various stages (JE2, PC2, PD1, PE3). At the same time, operating environment can cause electromagnetic interference, for e.g.

the use of mobile devices is also a cause to security breaches (JE3, PB1, PC3, PD3). Furthermore, as there is no line of sight and air is used as the medium of communication for RFID, eavesdropping or illegal reading of tags also exist in an operating environment when radio frequencies usages are not controlled. Finally, some human activities are involved in unethical practices, which are purposely done to break the RFID system (PB2). Based on the observation one can divide the sources of RFID security breaches into four major categories (1) Human Error, (2) Hacker Attack, (3) Operating Environment, and (4) Unethical Usage. The relationship between the RFID security breaches and the causes is illustrated in Figure 13.

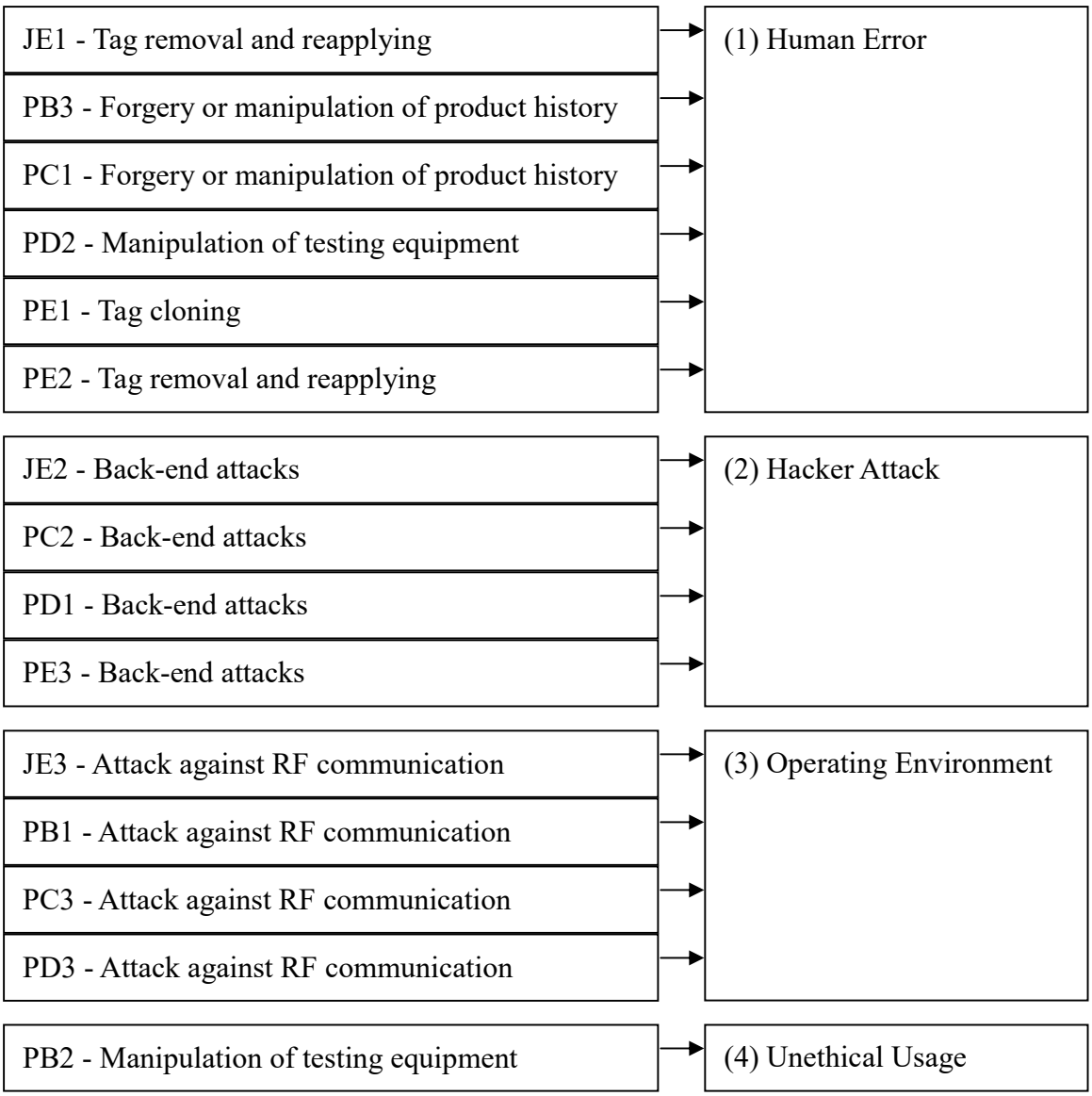


Figure 13 The causes and sources of RFID security breaches

7.4.12 Updated List of Security Breaches

The updated list of security breaches could lead to the discovery of their causes and sources and should be used to provide an EMDSCRV model, which can offer a practical solution to the SC RFID security breaches. In addition, the causes and sources of the SC RFID breaches could also lead to solutions by revisiting the literature.

Figure 14 summarized the literature findings of solutions to the four causes and sources of RFID security breaches. Human error security breaches should be tackled by *training* staff for operating the RFID system (discussed in 2.7.6); Hacker Attack problems should be solved by applying *software* protocols in all data server and storages (discussed in 2.7.6); Operating Environment issues should be attended by introducing *hardware* systems to block unnecessary radio frequency (RF) activities (discussed in 2.7.6); and finally Standard Operating Procedures (SOP) should be used to manage Unethical Usage cases (discussed in 2.7.6).

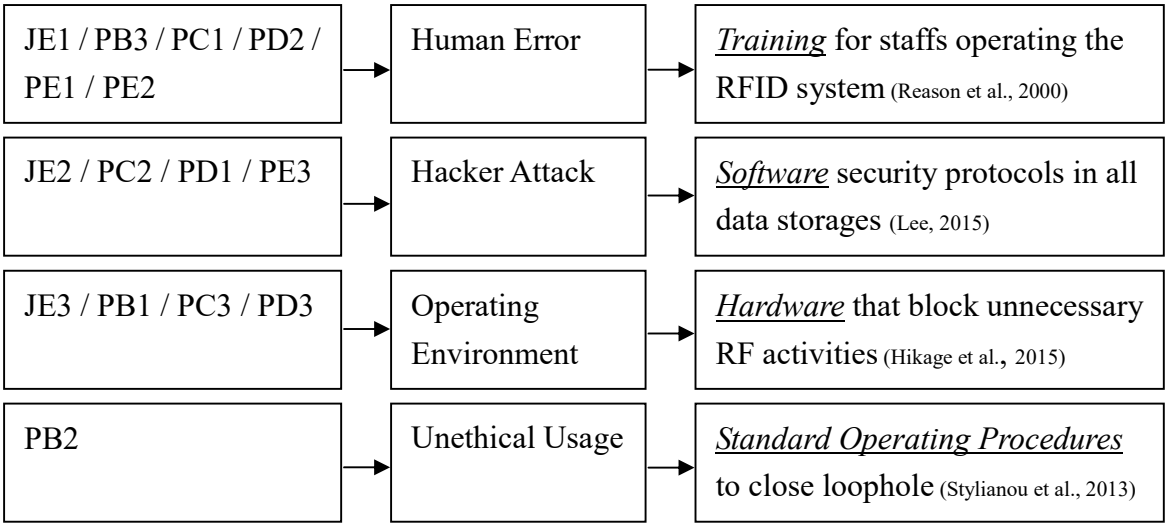


Figure 14 Suggested solutions to the four major causes and sources

7.4.13 Mapping LEI Security Breaches to the MDSCRV Model

In the semi-structured interview, we applied the MDSCRV Model in the pharmaceutical industry with the five identified domains in the SCs being A) Raw Material, B) Manufacturer, C) Logistics Service Provider, D) Importers, and E) Retailers. This is the second domain in the semi-structured interview cases as explained in Chapter 5. For example, focusing in an RFID system owned by the B) Manufacturer, who is considered as the direct domain, the A) Raw Material and C) Logistics Service Provider domains could be the associated domains, while the D) Importers and E) Retailers could be the uncontrolled domains for the said RFID system.

Therefore, PB) Manufacturer is denoted to be *Direct*, while PA) Raw Material, PC) Logistics Service Provider are *Associated*, and PD) Importers and PE) Retailers are considered to be *Uncontrolled*. Of course, each individual company business arrangement could be different. For example, some B) Manufactures can affect business decisions of D) Importers and E) Retailers, then both of these two domains should be considered as *Associated* instead of *Uncontrolled*.

Human Error Semi-Structure Interview Cases

The human error cause was featured in PB3, PC1, PD2, PE1, and PE2. The domain PB is direct, while PC and PD are associated, and PE is uncontrolled. Therefore, the PB3 case can be represented by a tab in the direct, at the C column. The HE cause is demonstrated by the orange colour, and therefore there is an orange tab in the direct section, in the C column. Likewise, another domain, the associated, has reported the PC1 case, therefore the C column in the associated section is also coloured in orange. Likewise, for case PD2, the D column is also coloured to represent this breach. For the uncontrolled domain, PE1 and PE2 were reported, as well as another two HE cases. An arrow is drawn from the human error box to the RFID lifecycle "Tube" with all the direct, associated, and uncontrolled highlighted. Furthermore, there are sub level indexes in the security threats, representing the security threats that are listed as major security threat categories.

Case No.	**Case Details**	**Direct Associated Uncontrolled**	**Sub level Index**
PB3	Manipulation of product data	B) Manufacturer (Direct)	C
PC1	Manipulation of product data	C) Logistics Service Provider (Associated)	C
PD2	Manipulation of testing equipment	D) Importers (Associated)	D
PE1	Tag cloning	E) Retailers (Uncontrolled)	B
PE2	Tag removal and reapplying	E) Retailers (Uncontrolled)	A

Table 30 Semi-Structure Interview Reported Cases with Sources and Causes of Human Error

This mapping demonstrated the three domains have vulnerability that caused the HE security breaches. One can observe the orange colour indicator to find the sources of the security breaches. In total, for HE related security breaches, one can spot the colours to determine whether they came from Direct (C), Associated (C, D), or Uncontrolled (B, C) sections.

There were four categories summarized, namely the hacker attack, operating environment, unethical employees, and human error. They can be connected to the MDSCRV model in order to identify the four causes and sources of the problem. The connected model is addressed as the EMDSCRV model in this study.

The four boxes represent the four categories, and there are arrows that go from the boxes into the MDSCRV model, which represent the causes or sources in different levels of the SC. RED color stands for Hacker Attack, GREEN for Operating Environment, Human Error is denoted by the PURPLE color, and Unethical Usage on BLUE color. In addition to the arrows, there are also the coloured tabs indicators for the security breaches that feature in the particular semi-structured interview.

Hacker Attack Semi-Structure Interview Cases

The human error cause was featured in PC3, PD1, and PE3. The domains PC and PD are associated, and PE is uncontrolled. Therefore, an error is drawn from the hacker attack box to the RFID lifecycle direct, associated, and uncontrolled areas. Table 31 highlights the cases.

Case No.	**Case Details**	**Direct Associated Uncontrolled**	**Sub level Index**
PC2	Back-end attacks	C) Logistics Service Provider (Associated)	E
PD1	Back-end attacks	D) Importers (Associated)	E
PE3	Back-end attacks	E) Retailers (Uncontrolled)	E

Table 31 Semi-Structure Interview Reported Cases with Sources and Causes of Hacker Attack

For example, the pharmaceutical security breach case of PC2, attack to servers reported by C) Logistics Service Provider, in the associated section. Therefore, an orange tab is being placed in the associated section under the sub category index of E. The other cases are completed in the same manner, where tabs are placed for hacker attack, in the section of Direct (E), in the Associated (E), and in Uncontrolled (E).

Operating Environment Semi-Structure Interview Cases

The operating environment cause was featured in PB1, PC3, and PD3. The domain PB is direct, while PB, PC, and PD are associated. Therefore, an error is drawn from the hacker attack box to the RFID Lifecycle direct and associated areas. The below table highlights the cases.

Case No.	Case Details	Direct Associated Uncontrolled	Sub level Index
PB1	Attack against RF Communication	B) Manufacturer (Direct)	F
PC3	Attack against RF Communication	C) Logistics Service Provider (Associated)	F
PD3	Attack against RF Communication	D) Importers (Associated)	F

Table 32 Semi-Structure Interview Reported Cases with Sources and Causes of Operating Envrionment

For example, Pharmaceutical security breach case of PB1, attack against RF communication reported by B) Manufacturer, in the direct section. And another tab is placed in that section under the sub type F. The other cases are completed with the same manner, which tabs will be placed for operating environment, in the section of Direct (F) and the Associated (F).

Unethical Usage Semi-Structure Interview Cases

The unethical usage causes is only reported with a manipulation of testing equipment in case PB2. Therefore, an error is drawn from the unethical usage box to the RFID Lifecycle direct areas. The below table highlights the cases.

Case No.	Case Details	Direct Associated Uncontrolled	Sub level Index
PB3	Manipulation of testing equipment	B) Manufacturer (Direct)	D

Table 33 Semi-Structure Interview Reported Cases with Sources and Causes of Unethical Usage

As PB3 is a security threat due to manipulation of testing equipment as reported by B) Manufacturer, having a sub category code of D. Therefore, a green tab is being placed in the direct section under the sub category index of D. This completed the MDSCRV Extended model, and a final figure is shown in the left of Figure 15.

7.4.14 Mapping TEI Security Breaches to the MDSCRV Model

Similarly, the TEI can also be mapped to the MDSCRV Model. A shorter RFID Lifecycle is featured in the TEI, and the semi-structured jewellery industry can be used as an example to illustrate the case. JE1 is a security threat due to tag removal and reapplying reported by E) Retailers and that tag removal and reapplying is having a sub category index of A. Therefore, a red tab is being placed in the uncontrolled section under the sub category code of the “a” category. JE2 is a security threat due to attack to servers reported by E) Retailer, having a sub category code of E. Finally JE3 is a security threat due to attack against RF Communication

reported by E) Retailer, having a sub category code of F. Therefore, a green tab is being placed in the direct section under the sub category index of F.

All of these causes were in the direct domain, as RFID is only used in the retailing level of the jewellery industry, with breaches and vulnerability only appearing in the retailing domain. Therefore, all JEs are considered to have impacted only from the direct domain. The final mapping of EMDSCRV model to the jewellery industry is show in Figure 15 .

Case No.	Causes	Sources	Domain of Vulnerability (Direct, Associated, Uncontrolled)
JE1	HE	Tag removal and reapplying	E) Retailers, Direct
JE2	HA	Back-end attacks	E) Retailers, Direct
JE3	OE	Attack against RF Communication	E) Retailers, Direct

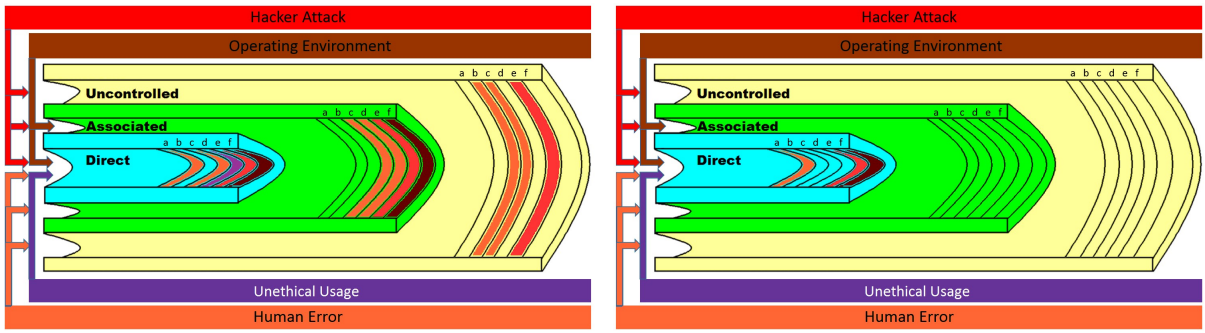


Figure 15 EMDSCRV Model with All Four Causes and Sources, for LEI (Left) and TEI (Right)

Key: Hacker Attacks occurrence are marked in red band, likewise Operating Environment in brown, Unethical Usage in purple, and Human Error in orange.

7.4.15 Causes and Sources of RFID Security Breaches

The EMDSCRV Models for pharmaceutical and jewellery, the LEI and TEI in the study, were displayed side by side in Figure 15. It can easily be spotted that the LEI has a more complex figure compared to the TEI. This is due to the shorter RFID Lifecycle of TEI . In jewellery the RFIDs are tagged in retailer's domain and then they are used only in that domain (apart from retailer who also own manufacture facilities, but it is still a single domain as per Kim's multi-domain interpretation). Indeed, the use of RFID in TEI usually does give only tracking benefits but not all benefits RFID can bring in SCM. While it is good to note this deficient use of RFID (i.e. not giving full benefits) as discussed in section 2.5.2, this short RFID lifecycle is not within the scope of this study.

For SC practitioners who are in the TEI, the EMDSCRV model already serves the purpose as a tool to help them direct the RFID SC breaches to the solutions. For example, in the case of JE1, tag removal and reapplying were reported, and the model has categorized the cause of this

breach as HE, and solution to this problem is training. This flow chart type of solution seeking is easy for TEI SC practitioners to follow. However, in the cases of LEI, since associated and uncontrolled domains were involved, even if the solution is from a single vulnerability, it might be difficult to be applied. For associated SC domains, although they are connected with the direct domain, they still might not entertain business requests from the direct domain. Even worse would be in the uncontrolled domain where the direct domain has no interaction with, solutions of the RFID SC breaches could contradict with some features of RFID systems. For example, an express courier company could have implemented online cargo tracking pages requiring no login / password authentication. A manufacturer of a pharmaceutical product has leaked the tracking number of an expensive drug to a third party. The third party can use the tracking features of the express courier company with the leaked tracking number to tracce the package, causing security breaches in the retailer domain. The courier express tracking system in this case is clearly a well-thought-of information system that purposely provids tracking functions without the need of authentication as a user friendly feature. However, this associated domain's user friendliness is an RFID security vulnerability for the retail domain.

For SC practitioners who are in LEI, the use of only EMDSCRV model is not enough, as RFID security breaches could have causes and sources from multiple domains of the SC, as a result, they have to be considered altogether in order for the EMDSCRV model to provide solution(s) to the breaches.

7.5 Discussion

RFID implementation does not give a clear improvement over security breaches on the SC, as illustrated in Table 25. Both before and after RFID implementation, incidents of SC security breaches have not necessarily been reduced, the value loss even remained in the same level in most cases. Various scholars, including Tenanbaum in 2013 and others (discussed in 2.5.2), claimed that application of RFID in SC brings operational benefits including transparency, but why doesn't security improve in such case? A proposed idea is most RFID systems have been applied with the principle to improve SC efficiency but not overall RFID security.

The conceptual model leads to further research in terms of how different industries will be able to address their RFID security breaches, with respect to its ease of use and ability to directly advise solutions to RFID security breaches. Furthermore, the security breaches were categorized into causes and sources of the breaches. This is important as different security breaches could be caused by one single source. A single cause or source of vulnerability to multiple breaches should be shown to SC practitioners in order to achieve a win-win situation

among all parties, as conflicting thoughts between various parties in the traditional SC are common[37].

The study findings show two forms of the MDSCRV model, which was the combined academic approach in addressing the RFID security breaches. As evidenced from the semi-structured interview, the MDSCRV model did not represent all the cases the semi-structured interview reported. While the MDSCRV model emphasizes on multi-domain and the areas of the security breach, the causes and sources are not illustrated. The EMDSCRV model tries to tackle this issue; it incorporates the semi-structured interview findings to the MDSCRV model and extends it to include causes and sources.

Furthermore, the figure of multi-domain colour bands can show the leading edge industry has a much more complex operation compared to trailing edge industry. If all RFID security breaches happen in the controlled tube, then all RFID security breaches happen under the control of the SC practitioner. The RFID security vulnerability can be directly examined and solved. On the other hand, if RFID security vulnerability appears in other tubes, say in associated or particular in uncontrolled has coloured bands, then the RFID security vulnerability is more complex. Most of the cases the SC practitioners cannot order uncontrolled companies to eliminate such RFID security breach vulnerability, either because resources (say time or money) are needed to eliminate such vulnerability and the companies are not directly connected in the SC, or simply because such vulnerability involves essential features, or provides an ease of use to other systems. For example, RFID tags with serial numbers representing a courier shipment are being uploaded to servers, and it is common practice to have courier tracking information viewable online without login and password authentication, which could provide certain efficiency in modern days' logistics systems. However, this also represents a possible security threat if the RFID information are being exposed to intruders.

For security beaches in trailing edge industries with a SC that has a short RFID lifecycle, usage of RFID does not span across multi-domain, and the model in Figure 14 can directly lead to single solutions to such security breaches. As illustrated in most semi-structured interviews, the jewellery industry has limited usage of RFID, which are mostly used in the retailing domain only, and the uncontrolled RFID vulnerability causing RFID supply breaches is limited. As a result, a simple model that points to a solution is sufficient to handle the identified vulnerability. Indeed, the usage of such short lifespan RFID does not provide the best return on RFID system investment but this is out of the scope of this study. Some trailing edge industries are starting to

[37] Generally and traditionally, supply chain has conflicting situations, for example buyer wants to buy at the least cost while sellers want to sell at maximum price. There are also works that can be done by different supply chain parties where supply chain companies want other companies to take responsibility in order to save cost.

promote the use of RFID with a longer lifecycle, that is, to tag the RFID from end of production until end of retailing. For example, some jewellery retailers with manufacturing capabilities are starting to promote the use of RFID in end-to-end tracking. However, even theoretically the RFID Lifecycle span across multi-domains, they are all in controlled domains as the SC practitioner is the owner of the RFID system and the RFID only covers the product while that company has possession of it.

7.5.1 Shortlisted and Targeted Security Breaches

The security breaches issue in the EMDSCRV model is a subset of academic security breaches that exist in multi-domain SCs. Through careful studies to a LEI and TEI, unbiased comments have been drawn from semi-structured interviews and the subset of RFID security breaches allows logistics practitioners to have a focused view on the possible security breaches that they experience in their SC.

7.5.2 Causes and Sources of Security Breaches

The EMDSCRV model directs security breaches to four causes and sources. The wealth of literature has provided solutions to these causes and sources. A revisit to the literature has been performed to build another design science artefact. These solutions to the causes and sources of security breaches are analysed in the next section.

The model can be used to find causes and sources of the RFID security incidents. Shall a business experiences RFID security vulnerability issues, one can refer to the model and find possible causes and sources of such vulnerability issues. Furthermore, this model will be able to show whether this problem arises from controlled or uncontrolled parties in a multi-domain SC parties, which such problem can then be easily tackled. For example, eavesdropping could have happened in a SC and with the EMDSCRV model an exact domain of possible breach will be directed to easily. Security breach preventive actions or post security beach solutions can be implemented to the right domain in the SC.

7.5.3 Multi-Domain Supply Chains

However, this model has a limitation which is treating all security breaches to be with the same weighting. EMDSCRV model has clearly showed that causes and sources could be from multi-domains in the SC. If all solutions are treated the same then businesses could have limited resources to implement all these solutions. For example, a company found RFID security breach from three domains involving HE, HA, and OP, then the company has to apply all solutions of training, hardware, and software that have been identified in this study. A single solution could have already solved all three causes and sources but since the solutions were not prioritized, there were no hint which one single solution should be applied first.

Another reason for the requirement of considering all the causes and sources of the RFID multi-domain security breaches is that the domains that introduced the vulnerability might be one that is uncontrolled. EMDSCRV model highlighted controlled, associated, and uncontrolled domains, and as illustrated in Figure 15, controlled domain means a domain the SC company has control on it, and shall any problem arise a solution can be implemented immediately. Associated could be the business associates the company works with, for example, a retailer is associated with the importer of the goods, and somehow can influence the importer to apply solutions to RFID security breaches if found. The worst case would be causes and sources of RFID security breaches were introduced from uncontrolled domains in a multi-domain SC setting, and the company cannot effectively deal with this problem. For example, a jewellery retailer found RFID information were uploaded by the manufacturer in a webpage without access control, and customers of the retail shop were using this information to select better jewellery in bulk random selection jewellery lucky draw, this is a HA cause and source in an uncontrolled domain and a UU in the controlled domain. As the retail have no connection with the manufacturer, particular if the manufacturer passes the goods to a few companies, say the exporter, importer, and wholesaler, before reaching the possession of the retail shop. The manufacturer is considered as the uncontrolled domain from the perspective of the retailer, and therefore the retailer can only apply solutions in their own domain.

As a result, EMDSCRV model needs to be upgrade to identify SC security breaches in the multi-domain setting considering all four causes and sources instead of one by one. This would allow a prioritized solution to be applied first, and then if the security breach is solved then there would not be necessary to apply other solutions. The consideration of multiple domain SC problem is a typical multi criteria decision making (MCDM) problem, and will be addressed in the next chapter.

7.6 Concluding Remarks

The mini case studies extended the MDSCRV model to show the RFID security vulnerability in the complex LEI and highlighted the vulnerability in TEI in a much simpler model. The difference in the model shows different vulnerability can come from different domains in LEI cases.

The proposed usage of EMDSCRV Model includes finding possible security breaches, finding causes and sources or these security breaches, and highlighting the domains in the multi-domains where the security breaches exist. It is useful for finding causes and sources of RFID security breaches, as it not only points out the area of possible security breaches in the SC, but also directs the security breach to causes and sources of security breaches. Finally, for multi-domain SCs, MDSCRV Extended model would highlight which domains the RFID

security breaches could happen. This model can achieve certain benefits, as discussed below, in addition to a clear visual recognition to the RFID security breaches in multi-domain SCs.

8 A Practical Framework based on the Developed Model

Research Question 3: What policy framework will reduce multi-domain vulnerability?

8.1 Introduction

This chapter will perform step 4 in the design science framework, Framework Evaluation. The EMDSCRV Model will be evaluated to ensure the model covers Multi-Domain SC and identify all the causes and sources to the security breaches. Focus group intensive discussion will capture the performance of the framework.

This chapter aims to address RQ 3, which describes a practical policy framework based on the MDSCRV model developed in earlier chapters. The framework should complement MDSCRV Extended model that was introduced in chapter 8. The policy framework will lead SC practitioners to causes and sources of the RFID security breach in SC with a prioritized solution and then from there the prioritized solution can fit to existing breaches or precautious measurements can be drawn to prevent future breaches, even if the breach has vulnerability from the *associated* or *uncontrolled* domain.

In Chapter 3 the design science approach was summarized and the following steps are outlined in this study. In step one, relevant literature were reviewed including various academic papers and the Kim et al.'s multi-domain RFID security model. In step two, the "Theory Building", a list was created with elements in RFID Security Framework, incorporated into Kim et al.'s multi-domain model, namely the MDSCRV model. The third step, "Technology Design Invention", the RFID security framework has been included also the causes and sources, as categorized into the MDSCRV model, namely the EMDSCRV Model. In step four, evaluation of the framework over the RFID Lifecycle should be performed

In Chapter 8 the list of vulnerability was shortlisted, and mapped to MDSCRV model, and then the mapping linked to another artefact that list top security breaches. A revisit to literature was done to build another artefact that contains the solutions to causes of these security breaches. By these literature and the EMDSCRV model, a framework can be used for SC practitioners to find solutions to their RFID security breaches. Finally, in this chapter, a focus group study will be performed, in accessing the usefulness of the extended framework.

The EMDSCRV Model is a combination of Kim et al.'s multi-domain theories and the list of RFID security breaches from SCRV, the semi-structured interview in chapter 6, and the revisit to literature where the practical business world shortlists the vulnerability list (literature in section 2.6, discussed in 7.4.10). In order to test the EMDSCRV Model, focus groups was used as the method to verify the usefulness of the model. In addition, this will lead to an understanding of the practicalities of the extended framework. The process first starts from the result of chapter 8, where the study maps the RFID security breaches incidents into the four major causes and sources, a review to the academic journals is then performed, drawing policies to solve the relevant causes and sources, and this forms the MDSCRV Extended model. In this chapter, focus groups will be used to capture pairwise comparison results and later verify the usefulness of such model.

It has been demonstrated in section 7.4.15 that the causes of sources of SC RFID security breaches are HE, HA, OE, and UU. Literature in section 2.7.6 suggests that the corresponding major solutions are application of training, software, hardware, and SOP. For SC practicing businesses, application of all four solutions could create a less required return on investment than applying a single prioritized solution that could solve most, if not all, of the SC security breaches. In a multi-domain SC case, this is even more true because the cause or source of the RFID security breach could come from other parts of SC that the domain has no control over it. In such case, the impact of such causes or sources need to be analysed to find out which of them can be treated with the solutions found.

The four major causes and sources to RFID SC security breaches have been identified, with the prime solutions determined from the second review to the literature. In a multi-domain SC, one single solution might not be enough for multiple causes and sources; therefore, there is a need to rank the solutions in order to allow the framework to deliver solutions to be implemented in a prioritized manner.

This situation is more common in LEI, and in such industries, even if the SC company is willing to apply more than one solution without considering the return on investment that multiple solutions could be costlier, causes and sources that were introduced in *uncontrolled* domains that the company has no control cannot be solved by the company, as it has no control over those causes and sources. Therefore, a policy framework that utilize the MDSCRV model to highlight prioritized solutions that solves multiple causes and sources, as a single solution may or may not fit multiple security breaches; the key point of the policy framework is to prioritize solutions.

8.2 Method

This chapter aims at using a policy framework to find one or more prioritized solutions for any given RFID security breaches. Causes and sources from multi-domain, with multiple solutions applicable is a case where scholars address as multi criteria decision making (MCDM, discussed in section 2.9.2). Tools have been developed to solve MCDM, a remarkable tool would be the Analytical Hierarchy Process (AHP, discussed in section 2.9.3) which is be used to analyze the RFID SC multi-domain breaches problem in this study. AHP is the only tool that can provide stable analysis by the four causes of sources while flexible regarding to the individual SC practitioner RFID security breaches incidents. By using AHP, criteria can be ranked according to the incidents, and if the domains are uncontrolled SC practitioners can use an alternative solution in domains that they can control.

8.3 Data Used

The data used are the twenty-five focus group members as discussed in 5.4. The focus group members have been divided into four mini focus groups based on the RFID security breaches causes and sources categories, namely Human Error Focus Group (HE), Unethical Usage Focus Group (UU), Hacker Attack Focus Group (HA), and Operating Equipment Focus Group (OE). The EMDSCRV Model is being applied to seek solution for the security breach incidents for the companies and the effectiveness of the solutions are further discussed in the focus group. The members have been invited to join more than one group shall their problems involved two or more causes and sources. In such cases their incidents and solutions were documented as two different focus group members in this study.

8.4 Policy Framework

The EMDSCRV model from Chapter 8 highlighted four solutions to the four major causes and sources of RFID security breaches, namely human error (HE), hacker attack (HA), operating environment (OE), and unethical usages (UU) are training, software, hardware, and SOP. Each of the solutions can solve multiple causes and sources of the security breaches. Therefore, diagrammatically, a policy framework based on the EMDSCRV model can be drawn, in Figure 24.

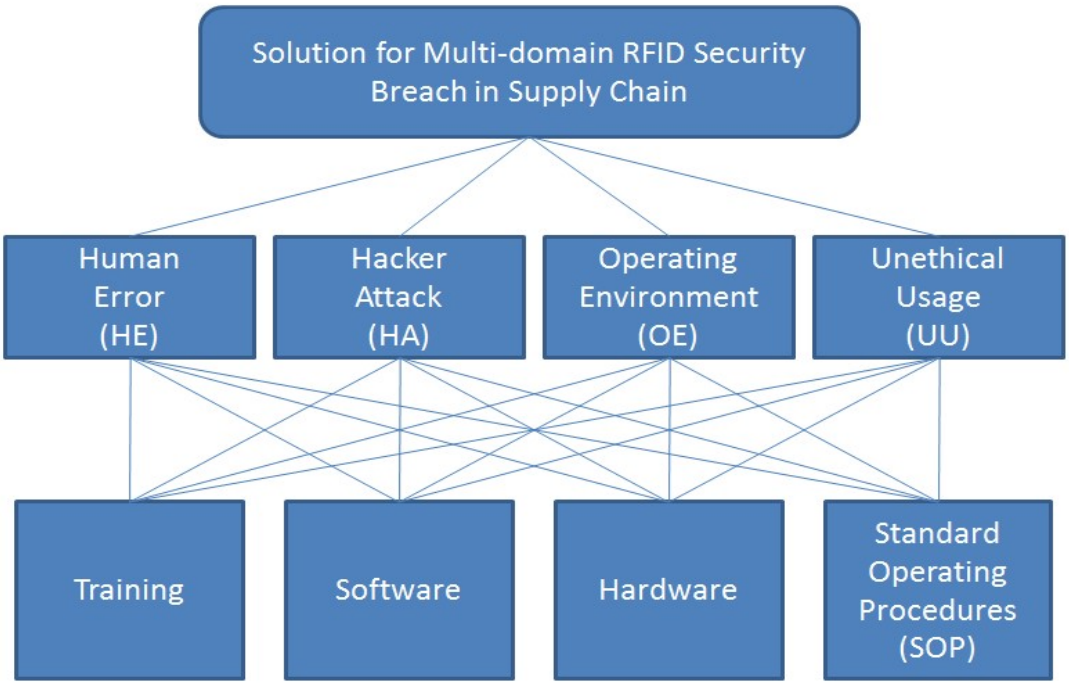


Figure 16 Policy Framework to Apply and Evaluate EMDSCRV

8.4.1 Policy Framework Application in the Focus Groups Meeting

AHP analysis needs to be performed (discussed in 4.5.6). From section 7.4.15, four solutions were found from revisit to the literature, namely training, software, hardware, and SOP. These are the alternative with criteria of cause and source of HE, HA, OP, and UU. Zhao's four steps AHP analysis on fishbone diagram as discussed in section 2.9.3 has been used, and the priorities of the solution of security threats of RFID with the solutions obtained were determined. SC practitioners selected for focus group are all in management level with over 10 years of experience in the field, which fits to these criteria.

Hierarchy Model and Comparison Matrix used in Focus Group Meeting

The policy framework in Figure 16 was explained as the basis for of focus group meeting. Presented in a hierarchy manner, the framework can be used in the first step of AHP as discussed in 2.9.3, where the prioritized solution for the multi-domain RFID security breach in SC can be found by examining the causes and sources of HE, HA, OE, and UU. For the first level analysis, a matrix shall be drawn with two axis, to facilitate pairwise comparison of the multi-domain security breaches. The matrix contains the causes and sources in both horizontal and vertical axis, users of the RFID security framework has to fill in the pairwise comparison indexes. The use of AHP will fill in the individual pairwise comparison of each of the

vulnerabilities that constitute to RFID security breaches in respect to the four causes and sources.

Pairwise Comparison Matrix used in Focus Group Meeting

There are four pairwise comparison matrixes for the solutions, they were built by asking the four focus groups members to compare the four solutions with respect to only the four causes and sources of RFID SC breaches. This process was documented in section 8.4.1 in details. Further to that process, causes and sources of security breaches were identified by the use of online software PoolEV, and the details were discussed in section 8.4.1.

8.5 Results

The results of the focus group study are a fishbone analysis (discussed in 2.9) and AHP results generated by Zhao's four steps of AHP analysis on fishbone diagram (discussed in 2.9.3). The AHP results include a hierarchy model (illustrated in 8.4.1), and pairwise comparison matrix, weight vector calculations, and combine weight vectors (illustrated in 8.4.1).

8.5.1 Sources of security breaches: Fishbone Analysis

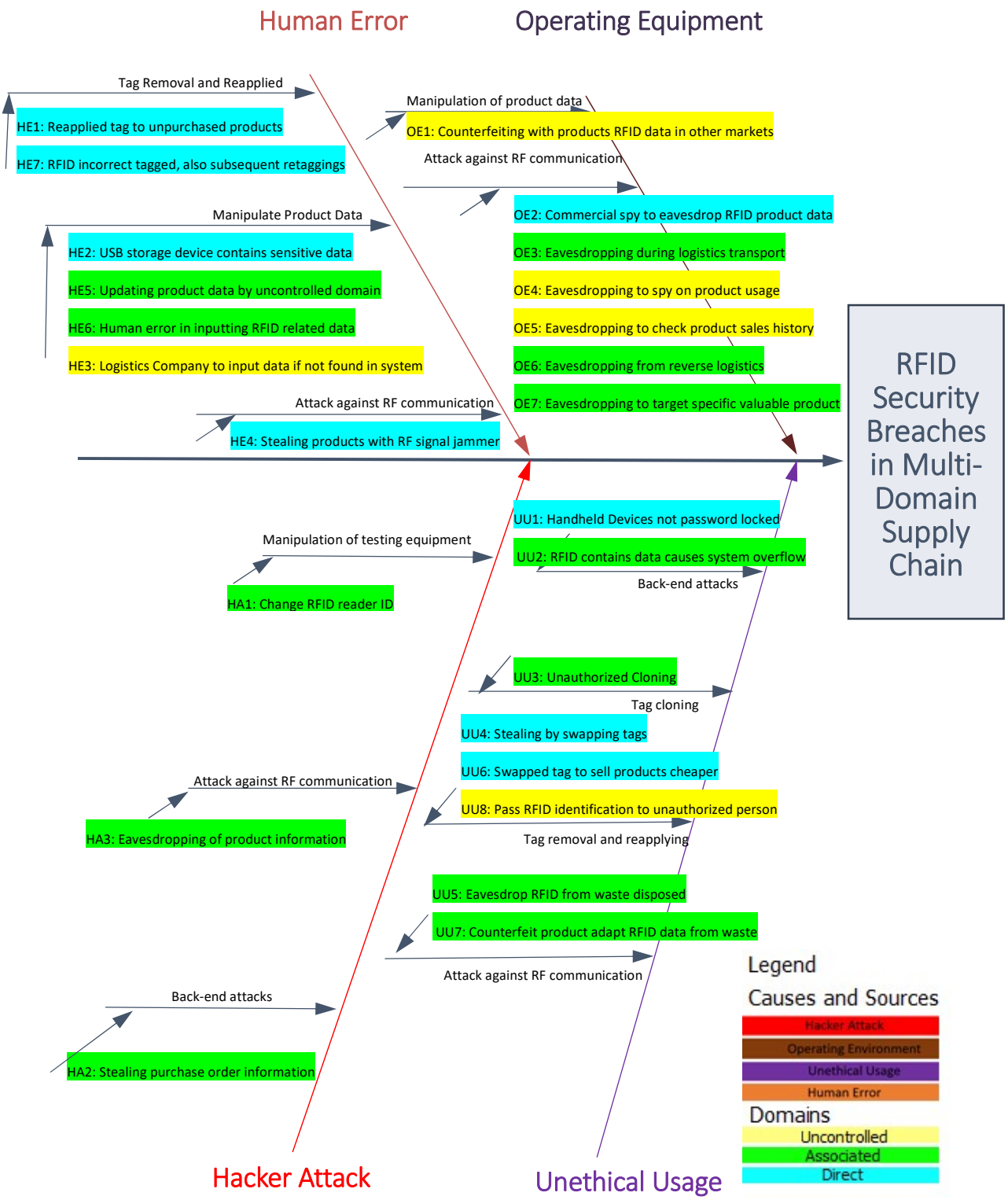
The list of focus group members are summarized in Table 34, and the causes and sources of RFID security breaches were summarized in a fishbone diagram, in Figure 17, to illustrate their cause and effect relationships. Fishbone diagrams can shows causes and sources to issues and can be combined with EMDSCRV model as Kim et al.'s model highlights the multi-domain aspects in RFID security. In the combination of the fishbone diagram and EMDSCRV model, colour codes were used to identify which tier the problem can expand into.

Case No.	Highlight of Details of Security Breach	Solution	Highlights of Details of Solution
HE1	Reapplied tag to unpurchased products	Training	Training to re-tag unpurchased jewellery
HE2	USB storage device contains sensitive data	Training	Training of how to handle RFID data
HE3	Logistics Company to input data if not found in system	Hardware	2D Barcode as second authentication
HE4	Stealing products with RF signal jammer	Software	Real-time information update for checking
HE5	Updating product data by uncontrolled domain	SOP	Medicine enter room before usage
HE6	Human error in inputting RFID related data	Hardware	Vital Signs reading device also read RFID
HE7	RFID incorrect tagged, also subsequent retaggings	SOP	Tag RFID with two lab technicians
OE1	Counterfeiting with products RFID data in other markets	Software	Minimize information written on RFID
OE2	Commercial spy to eavesdrop RFID product data	Software	Unorganized number avoid reading
OE3	Eavesdropping during logistics transport	Software	Shared Key Authentication System
OE4	Eavesdropping to spy on product usage	Hardware	Sleep and Zombie tags
OE5	Eavesdropping to check product sales history	Hardware	Blocker tag
OE6	Eavesdropping from reverse logistics	Hardware	Metal shielded bags for reserve logistics of RFID
OE7	Eavesdropping to target specific valuable product	Software	Data Encryption with unique reader keys
UU1	Handheld Devices not password locked	Software	Password and Real time data transfer
UU2	RFID contains data causes system overflow	SOP	Policies for internal employee pilferage
UU3	Unauthorized Cloning	Hardware	SMS registered phone upon RFID usage
UU4	Stealing by swapping tags	Hardware	CCTV / Weight system on jewellery sold
UU5	Eavesdrop RFID from waste disposed	SOP	Right waste in right bag / dispose tags after usage
UU6	Swapped tag to sell products cheaper	Software	Unique RFIDs and marked as sold in POS
UU7	Counterfeit product adapt RFID data from waste	Software	Online servers to mark drug usage
UU8	Pass RFID identification to unauthorized person	SOP	Dispose RFID tags after product used
HA1	Change RFID reader ID	Hardware	Middleware
HA2	Stealing purchase order information	Software	Software Development Life Cycle Policies
HA3	Eavesdropping of product information	Software	Public Key Infrastructure

Table 34 Security Breaches and Solutions of the Focus Group Member Lists.

Details of each member is documented in Appendix I

Figure 17 Fishbone Diagram of Focus Group Study RFID Security Breaches in Multi-Domain Supply Chain



8.5.2 Pairwise Comparison

Pairwise comparison results of HE are tabulated in Table 35. With respect to human error in RFID security threats, focus groups members reported training is nine times more effective as a solution than the use of software as some HE issues cannot be fully avoided by software. Likewise, for training against hardware, some companies implemented RFID scanning in point of sale system but still there were untrained staffs who use the system with mistakes. The use of SOP as a solution to solve HE issues is three times more favoured compared to both software and hardware, but still against training, it would be three times less favoured.

Training	9	Software	1
Training	9	Hardware	1
Training	3	SOP	1
Software	3	Hardware	1
Software	1	SOP	3
Hardware	1	SOP	3

Table 35 Pariwise Comparison of the Four Solutions to the Cause and Source Human Error

Similarly, the result tables for HA, OE, and UU are as follows:

Hacker Attack

Training	1	Software	9
Training	1	Hardware	5
Training	1	SOP	3
Software	3	Hardware	1
Software	5	SOP	1
Hardware	3	SOP	1

Unethical Usage

Training	1	Software	3
Training	1	Hardware	5
Training	1	SOP	9
Software	1	Hardware	3
Software	1	SOP	5
Hardware	1	SOP	5

Operating Environment

Training	1	Software	5
Training	1	Hardware	9
Training	1	SOP	3
Software	1	Hardware	3
Software	3	SOP	1
Hardware	7	SOP	1

8.6 Analysis

AHP analysis were performed on the results given by focus group. Table 35 is a matrix that explains the relationship in a 2-way tabulated way. A more general 4-way comparison matrix that consists of all four solutions to the human error cause can be demonstrated in Table 36.

This is the same pairwise comparison matrix that explains the relationship in a 4x4 matrix. Following the above example where training is nine times more effective to be used as a solution to HE problems, instead of only 1 and 9 recorded, inverted of the results 1/9 is also recorded. This comparison indexes are recorded in column one row two, and row two column one, whenever training and software intersects. Tabulating the pairwise comparison figures this way is the first step of AHP analysis.

HE	Training	Software	Hardware	SOP
Training	1	9	9	3
Software	1/9	1	3	1/3
Hardware	1/9	1/3	1	1/3
SOP	1/3	1/5	3	1

Table 36 Pairwise Comparison Matrix of All Four Alternatives to the Cause and Source Human Error

Next, normalization is being performed to the pairwise comparison matrix. This is done by taking sum of the columns in the pairwise comparison matrix, the total column will describe the weighting. The lower the score is the more important criteria. The result is shown in Table 34.

HE	Training	Software	Hardware	SOP
Training	1	9	9	3
Software	1/9	1	3	1/3
Hardware	1/9	1/3	1	1/3
SOP	1/3	1/5	3	1
Total	**1.5667**	**13.3333**	**16**	**4.6667**

Table 37 Sum of the Columns in the Pairwise Comparison Matrix

Normalization is an important process for as the AHP requires a normalized pairwise comparison matrix. The pairwise comparison table is being normalized by take each value and divide by each column total, as in Table 38, and the operation being repeated horizontally, by taking sum in each row, as shown in Table 39. This is the normalized matrix of the pairwise comparison of all alternatives to the cause and source Human Error. It is also worth to note that four decimal places are taken from all interim calculation processes, and final results are presented in two decimal places.

HE	Training	Software	Hardware	SOP
Training	0.6429	0.675	0.5625	0.6429
Software	0.0714	0.075	0.1875	0.0714
Hardware	0.0714	0.025	0.0625	0.0714
SOP	0.2143	0.225	0.1875	0.2143
Total	1	1	1	1

Table 38 Normalization of Pairwise Comparison Matrix in Progress

Next, the normalization process repeats, while the interim figures provide no value to the results, they are then added up to the total before taking the weighting of each individual items.

HE	Training	Software	Hardware	SOP	Total
Training	0.6429	0.675	0.5625	0.6429	**2.5232**
Software	0.0714	0.075	0.1875	0.0714	**0.4054**
Hardware	0.0714	0.025	0.0625	0.0714	**0.2304**
SOP	0.2143	0.225	0.1875	0.2143	**0.8410**
Total	1	1	1	1	

Table 39 Normalized Matrix of Pairwise Comparison of All Alternatives to the Cause and Source Human Error

For AHP comparison, the weighting is important as this describes the prioritized solution. Each row values will be totalled and divided by the total number of alternatives. The result is shown in Table 40.

HE	Training	Software	Hardware	SOP	Total	AHP
Training	0.6429	0.8544	0.5625	0.3214	2.3812	**63.080%**
Software	0.0714	0.0949	0.1875	0.5357	0.8895	**10.134%**
Hardware	0.0714	0.0317	0.0625	0.0357	0.2013	**5.759%**
SOP	0.2143	0.0190	0.1875	0.1072	0.5280	**21.037%**
Total	1	1	1	1	4	**100%**

Table 40 AHP Values on All Alternatives of the Cause and Source Human Error

Therefore, from our AHP analysis, for HE, the study group believed that training is the greatest preference and has the first priority by 63.080%, follow by software as a solution with 10.1347%, and then hardware with 5.759% and finally SOP by 21.037%. The summarised results for all four causes and sources (including HA, UU, and OE) are tabulated as shown below.

Hacker Attack AHP results

HA	Training	Software	Hardware	SOP	Total	AHP
Training	0.0556	0.0676	0.0441	0.0357	0.2030	**5.07%**
Software	0.5000	0.6081	0.6618	0.5357	2.3056	**57.64%**
Hardware	0.2777	0.2027	0.2206	0.3215	1.0225	**25.56%**
SOP	0.1667	0.1216	0.0735	0.1071	0.4689	**11.73%**
Total	1	1	1	1	4	**100%**

Table 41 AHP Values on All Alternatives of the Cause and Source Hacker Attack

UU AHP Results

UU	Training	Software	Hardware	SOP	Total	AHP
Training	0.0556	0.0357	0.0306	0.0735	0.1954	**4.88%**
Software	0.1667	0.1071	0.0510	0.1324	0.4572	**11.43%**
Hardware	0.2777	0.3215	0.1531	0.1324	0.8847	**22.12%**
SOP	0.5000	0.5357	0.7653	0.6617	2.4627	**61.57%**
Total	1	1	1	1	4	**100%**

Table 42 AHP Values on All Alternatives of the Cause and Source Unethical Usage

OE AHP Results

OE	Training	Software	Hardware	SOP	Total	AHP
Training	0.0556	0.0441	0.0700	0.0294	0.1991	**4.98%**
Software	0.2777	0.2206	0.2100	0.2647	0.9730	**24.33%**
Hardware	0.5000	0.6618	0.6300	0.6177	2.4095	**60.23%**
SOP	0.1667	0.0735	0.0900	0.0882	0.4184	**10.46%**
Total	1	1	1	1	4	**100%**

Table 43 AHP Values on All Alternatives of the Cause and Source Operating Equipment

8.6.1 Consistency Test of AHP Matrixes

Section 4.2.5 addressed the importance of identifying and controlling research biases and the consistency test should be done. Section 4.4.2 explained the three steps of checking consistency of AHP results. All the results of AHP were tested for consistency.

The consistency measure of the relative four factors are given by matrix multiplication of the raw pairwise comparison score and the AHP results, dividing by the AHP result of the given AHP percentage. For Training, the score is 1/9/9/3 from Table 36 and the AHP results are 63.080%,10.134%,5.759%,21.037%, the matrix multiplication is (1)(0.63080)+(9)(0.10134)+(9)(0.05759)+(3)(0.21037)/0.63080 or 4.2675. The consistency measure vector including the remaining values of software, hardware, and SOP are in Table 44.

Training	4.2675
Software	4.0881
Hardware	4.0206
SOP	4.2675

Table 44 Consistency Measure Vector for the Four Solutions as Alternatives in AHP Studies

Consistency Index can be calculated by taking the sum of the consistency measure vector minus n divided by n-1, since we have 4 values, this would be ((4.2675+4.0881+4.0206+4.2675)-4)/3 or 0.0537. With the random index retrieved from Table 45 (Saaty, 1980), the random index is 0.90 and the consistency ratio would be 0.0537/0.90=0.0596. As consistency ratio is less than 10%, the pairwise comparison table is considered to be consistent and the AHP is dependable.

Matrix order number	1	2	3	4	5	6	7	8
RI	0		0.52	0.90	1.12	1.25	1.35	1.42
Matrix order number	9		10	11	12	13	14	15
RI	1.46		1.49	1.52	1.54	1.56	1.58	1.59

Table 45 Saaty's (1980) Random Index for Analytic Hierarchy Process

Similarly, the consistency test process is repeated for all HA, UU, and OE study. For HA, the computed CI is 0.0257, and CR is 0.0285. For UU, the computed CI is 0.0617, and CR is

0.0685. Finally, for OE, the computed CI is 0.0298, and CR is 0.0331. All studies give result of CR under 10% and the answers given in the focus group are consistent.

8.6.2 Interpretation of AHP Analysis Results

AHP analysis results are presented in Table 46, showing priorities of causes and sources of RFID security breaches based on mean of all focus group member responses. The result shows us that with respect to the RFID security breach HE, training has a priority of 63.08%, while software has 10.13%, hardware has 5.759%, and SOP has 21.037%. While only HA is considered, training has 5.07%, software has 57.64%, hardware has 25.56% and SOP has 11.73%. Likewise, for UU, training has 4.98%, software has 24.33%, hardware has 60.23% and SOP has 10.46%. Finally, if only OE is considered, training has 4.98%, software has 24.33%, hardware has 60.23% and SOP has 10.46%. The table also highlight the solution with the first priority.

	HE	**HA**	**UU**	**OE**
Training	**63.080%**	5.07%	4.88%	4.98%
Software	10.134%	**57.64%**	11.43%	24.33%
Hardware	5.759%	25.56%	22.12%	**60.23%**
SOP	21.037%	11.73%	**61.57%**	10.46%

Table 46 Final Result of AHP

If the RFID security breaches are single domain, as previous authors attempt to solve, then the finding is already useful to SC practitioners to solve the problem of RFID SC security breaches. However, as adapted from MDSCRV and also agreed by the interviewees in the semi-structured interview in chapter 7, the problem in SC has a multi-domains attribute, and causes and sources could be multiple from different domains on the SC. Therefore, the application of the AHP results requires a further step that synthesizes the final priorities.

8.6.3 Application of AHP Analysis Results

The practical application of AHP analysis results for a logistics practitioner is another AHP analysis synthesising the logistics practitioner's own RFID security breach incidents, and can be summarized by the following four steps:

Step 1: Determine the causes and sources of the multi-domain security breach. List down priorities in the four categories HE, HA, UU, and OE.

Step 2: Perform pairwise comparison of the security breach incidents. This could be computed by the incident count or financial impact of various causes and sources from multiple domains.

Step 3: AHP study on the four categories to retrieve a single number as priority percentage. The four percentages should add up to 100%.

Step 4: Perform the synthesizing final priorities to find out the solutions priorities.

A case was discussed in the focus group meeting as an example illustrated to the focus group members of the use of the AHP analysis results, subsequently all focus group members used computer software to analyse the results (discussed in next section). Jewellery retail shop ABC has found various RFID security breaches. The major incident was their shop manager was able to retag expensive jewellery items with inexpensive items RFID tag (an UU vulnerability). There were also causes and sources in their multi-domain SC that enables this and other lost. Supplier has sent shipping schedule of valuable jewellery via regular email without using passwords (a HE vulnerability), which the shop manager is able to read from files in network drives not intended for him (a HA vulnerability), the jewellery and tag being shipped by logistics service provider, applied, and reapplied did not go through any RFID scanning devices, and in some areas should have sounded alarm but missing (an OE vulnerability).

For this multi-domain SC error, the jewellery shop had difficulties to identify a single percentage of causes and sources that impacted to the lost, pairwise comparison with AHP have been applied in this case. The company had counted the RFID security breaches incidents and rounded to the follow table for pairwise comparison.

The SC practitioner is asked to compare the four causes and sources of their SC RFID related security breaches. Or in short, fill in the table with thoughts only to causes and sources that relates to this particular RFID security breach.

HE	1	HA	3
HE	1	OE	1
HE	1	UU	9
HA	3	OE	1
HA	1	UU	7
OE	1	UU	7

Table 47 Pairwise Comparison of Real World Application of RFID Security Framework

The contribution of the use of AHP in the RFID security framework is the prioritized results can already be shown to the SC practitioner with this minimal amount of pairwise comparison work. The background work including semi-structure interviews and previous pairwise comparison table done with the focus group practitioners enable the entire calculation to be done with simple arithmetic in all future studies.

AHP is then performed on Table 47, with the results are listed in Table 48. Based on pairwise comparison, the AHP inspires the SC practitioner believed that HE constitute 6.82% to the RFID security breach, while HA has 17.05% of the cause, OE has 7.39%, and UU being the major cause which constitute 68.74% to the breach.

	HE	HA	OE	UU	Total	AHP
HE	0.0714	0.0384	0.0833	0.0795	0.2726	**6.82%**
HA	0.2143	0.1154	0.2500	0.1023	0.6820	**17.05%**
OE	0.0714	0.0385	0.0833	0.1023	0.2955	**7.39%**
UU	0.6429	0.8077	0.5834	0.7159	2.7499	**68.74%**

Table 48 AHP Values of Real World Application of RFID Security Framework

The computed CI is 0.0430, and CR is 0.0477, under 10% and consistent.

The next step is to synthesize the final results, the four AHP percentages Table 48, will be used against to the AHP results of the focus group member's pairwise comparison of solutions in Table 46. The process of synthesize of data will be a weighted calculation of the AHP results of both tables.

Criterion	**Priority vs Goal**	**Alternative**			
HE	6.82%	Training	59.53%	x 6.82%	4.0595%
		Software	22.24%	x 6.82%	1.5166%
		Hardware	5.03%	x 6.82%	0.3430%
		SOP	13.20%	x 6.82%	0.9001%
			100.00%		
HA	17.05%	Training	5.07%	x 17.05%	0.8644%
		Software	57.64%	x 17.05%	9.8268%
		Hardware	25.56%	x 17.05%	4.3576%
		SOP	11.73%	x 17.05%	1.9998%
			100.00%		
OE	7.39%	Training	4.98%	x 7.39%	0.3679%
		Software	24.33%	x 7.39%	1.7974%
		Hardware	60.23%	x 7.39%	4.4494%
		SOP	10.46%	x 7.39%	0.7727%
			100.00%		
UU	68.74%	Training	4.88%	x 68.74%	3.3548%
		Software	11.43%	x 68.74%	7.8575%
		Hardware	22.12%	x 68.74%	15.2064%
		SOP	61.57%	x 68.74%	42.3262%
			100.00%		

Table 49 Final AHP results with weighting from Table 48

The final values are added with respect to the four solutions, Training, Software, Hardware, and SOP to calculate the final score of the solutions. The results are overall priorities for all the solutions, with respect to the input from the pairwise comparison table.

	HE	HA	OE	UU	Total
Training	4.0595%	0.8644%	0.3679%	3.3548%	8.6465%
Software	1.5166%	9.8268%	1.7974%	7.8575%	20.9983%
Hardware	0.3430%	4.3576%	4.4494%	15.2064%	24.3564%
SOP	0.9001%	1.9998%	0.7727%	42.3262%	45.9988%

Table 50 Overall priorities for all the solutions

It is clear that the SOP should be used as the prioritized solution, with a weight of 45.99%. The results led to the case of UU4, where SOP was used as the solution to solve the security breach of reapplication of tags for unsold jewellery.

8.6.4 Application of AHP Analysis with Computer Software

The same calculation has been performed for all the focus group members with the help of AHP Priority Calculator[38] as shown in Figure 18. At the end of the focus group meeting, all members were provided with priority weightings to the four solutions HE, HA, UU, and OE. Discussions were made between focus group members to enlighten other members, including what practical application of the solution could be. For example, the case UU4 has SOP was advised from the framework as the prioritized solution, the UU focus group members suggested to added two SOP of weighting and image comparison of jewellery being sold, and finally this prioritized solution became the only solution that was used to solve the RFID security breach UU4 below. Full solutions of all the focus group member with background of this SC practitioner has been documented in the next section.

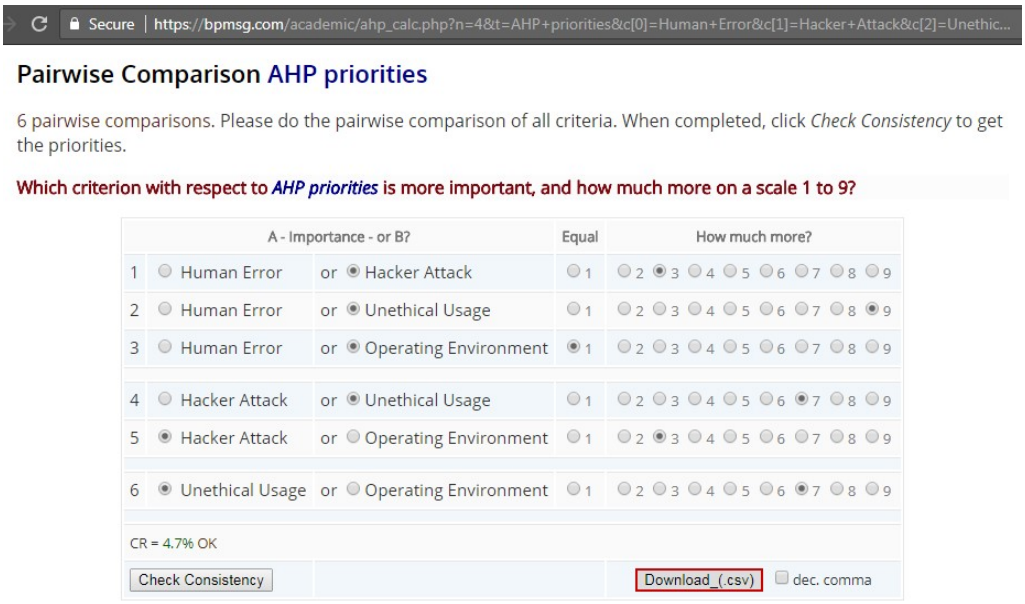


Figure 18 Free online AHP Priority Calculator with Consistency Check, from BPMSG (2018).

[38] Free online AHP Priority Calculator with consistency check. https://bpmsg.com/academic/ahp_calc.php. This tool supports alternatives to pass in from html header, simplified comparisons generation by scripts. For example: https://bpmsg.com/academic/ahp_calc.php?n=4&t=AHP+priorities&c[0]=Human+Error&c[1]=Hacker+Attack&c[2]=Unethical+Usage&c[3]=Operating+Environment

Human Error Focus Group

The human error focus group focuses on all human error that is incurred in a multi-domain SC as a breach to the RFID system. Typical error could include mis-tagging RFIDs, miss scans of RFID during busy peak operating hours, retagging RFIDs to wrong products. If the human operator who has intention to mis-operate the RFID system this is not considered as human error but rather unethical usage, which is another cause and source of RFID security breach. In total, there were 7 cases in the focus group (Abbreviated HE1 to HE7, and together with all other focus group member details are documented in Appendix I).

The Unethical Usage Focus Group

Similar to the human error subgroup, the unethical usage focus group deals with RFID security breaches from human operator to the RFID system. However, the incidents were from a very different angle because this is when the human operator purposely breaks the RFID system in an unethical way. The reason of breaking the system could be to achieve some financial benefits such as stealing goods or saving operating times. In most cases, the operator who breaks the RFID system has knowledge of the loophole in the system. In total, there were 8 cases in the focus group (Abbreviated UU1 to UU8).

Operating Environment Group

Operating environment group consist of members who have suffered from all RFID security breaches due to the operating environment. Examples of which including the use of civilian RFID devices without the knowledge of jamming RFID signals, or professional business espionage who read RFID data from a distance in an unauthorized manner, which is known as eavesdropping. In total, there were 7 cases in the focus group (Abbreviated OE1 to OE7).

Hacker Attack Focus Group

Finally, the hacker attack focus group contains hackers who have purposely hack into the RFID system to gain benefits. The hacking usually break into RFID systems entirely but not jeopardizing individual tags to gain benefits that are larger scale. Hacker attack requires advanced information technology knowledge while unethical usage group breaks RFID systems in a layman manner and operating environment group breaks RFID systems by just using civilian devices. Hacker attack group uses professional hacking software and hardware to achieve hacking results. In total, there were 3 cases in the focus group (Abbreviated HA1 to HA3). Details of all the cases with original quotes from the SC practitioner were documented in Appendix I, and summarized in Table 34.

8.6.5 Evaluation of the RFID Security Framework

As illustrated in Table 16 and discussed in section 4.4.2, design science artifact must be evaluated. The RFID security framework is being evaluated by the eight criteria half year after

the solution has been deployed. The eight criteria are completeness, extensibility, usability, functionality, reliability, interoperability, scalability, and efficacy. A telephone survey is being constructed to the focus group member to rank the eight criteria by Likert scale with example as illustrated in Table 51.

Strongly Disagree	**Disagree**	**Slightly Disagree**	**Slightly Agree**	**Agree**	**Strongly Agree**
1	2	3	4	5	6

Table 51 Example Likert Scale for use with Answers to Evaluation of the RFID Security Framework

Completeness

An attempt to evaluate the following:

Does the framework cover the entire scope of study, i.e. The proposed RFID Lifecycle?

Survey Question 1: Can the identified prioritized solutions solve RIFD security chain breaches introduced from all supply chain domains?

No	0
Current domain only	1
Current domain plus upstream or downstream	2
Current domain plus upstream and downstream	3
All domains on supply chain	4
All domains on supply chain plus opportunity for future domains	5

Table 52 Answers in Likert Scale for Evaluation of the RFID Security Framework to Framework Completeness

The completeness of the question determines whether the framework cover the entire scope of study, i.e. the proposed RFID Lifecycle. Some study target explained the high score is being given due to the nature of RFID security framework addressed multi-domain RFID security breach by synthesizing the AHP values which considers the multi-domain SC completely. It was also noted to the study target that the prioritized solution that is synthesized by AHP in this study has not considered the distance from the SC being studied, apart from emphasizing in the study, that uncontrolled domains (denoted in yellow color in the framework) could have difficulties in applying solutions even if identified by the AHP model. The framework could have difficulties in tackling a SC cause and source that is introduced from the parties further away from the SC. For example, if a jewellery retailer experiences a security breach due to the details of RFID tag information on a server being exposed from the manufacturer (in the uncontrolled area), and the SC involves several parties in between the manufacturer and such retailer, say the exporter, importer, and distributor, the prioritized solution could be less effective or even useless in capturing the causes and sources introduced in such a way. The mean score of the answer is 4.72.

Extensibility

An attempt to evaluate the following:

Can the framework be extended to cover supply chain that is out of the location being studied, i.e. beyond Pearl River Delta, China?

Survey Question 2: The proposed framework can be used for supply chain practitioners outside the study area Pearl River Delta, China. Do you agree with this statement?

Strongly Disagree	0
Disagree	1
Slightly Disagree	2
Slight Agree	3
Agree	4
Strongly Agree	5

Table 53 Answers in Likert Scale for Evaluation of the RFID Security Framework to Framework Extensibility

Extensibility concerns about whether the framework can be extended to cover SC that is out of the location being studied, i.e. Pearl River Delta, China. As the study provides generic figures and robust calculation methods, study targets have no worry of extending the study to other SC domains they have. The mean score for this question is 4.32.

Usability

An attempt to evaluate the following:

Can the framework be used to analyze supply chain?

Survey Question 2: How many times do you have difficulties in using the framework apart from understanding the issues?

0 – never had any difficulties	5
1	4
2	3
3	2
4	1
>=5	0

Table 54 Answers in Likert Scale for Evaluation of the RFID Security Framework to Framework Usability

Usability covers whether the security framework is usable for multi-domain SC RFID security breaches. SC practitioners are required to perform pairwise comparison to the four causes and sources of SC security breach that they experienced. If there are difficulties in comparing the alternatives then this framework is highly unusable; on the other hand, if the users understand how the comparison works then the framework is a very simple tool and identifies the solutions. For the focus group members, usability has a mean score of 4.16, meaning the framework is highly usable.

Functionality

An attempt to evaluate the following:

Can the framework address security vulnerability?

Survey question: How many RFID security breach experienced cannot be categorized in the four causes and sources of the framework?

0 – all can be categorized	5
1	4
2	3
3	2
4	1
>=5	0

Table 55 Answers in Likert Scale for Evaluation of the RFID Security Framework to Framework Functionality

The next question is about functionality, the framework is based on a semi-structured interview that categorizes the causes and sources of four major categories. If users of the framework experience a single domain, single cause and source RFID security breach, the prioritized solution requires no pairwise comparison and it's easy to lead to the solution. However, what happens if the solution is actually not within the four causes and sources? In such case, semi-structured interviews need to be redone to capture other causes and sources as there could be a new category of cause and source in the future. The research methodology has no issue but as business environment updates from time to time it is required for such updates. In fact, design science principles suggest an artefact to be rebuilt in a recursive manner to cope with ever changing business environments. Indeed, the functionality of the framework received a score of 5, all the security breaches of RFID can be categorized in the four causes and sources, and this was known in question 3 in the initial survey to select focus group members, there were no "others" selected in all answers. The mean score for this evaluation is 4.32.

Reliability

An attempt to evaluate the following:

Can the framework reduce security vulnerability?

Survey Question:

Have you used the framework more than once? If no, go to question 6.

The framework provides the same functionality every time you used it. Do you agree with this statement?

Strongly Disagree	0
Disagree	1
Slightly Disagree	2
Slight Agree	3
Agree	4
Strongly Agree	5

Table 56 Answers in Likert Scale for Evaluation of the RFID Security Framework to Framework Reliability

A framework that can be used more than one time, robustly providing solutions that are required, is a reliable framework. There are two participants (HE5/6/7/OE1 and UU5/6) who have used the framework more than once, who were invited to answer this question. Both repeatedly mentioned the multi-domain SC fits their SC, the four categories do cover the

causes and sources of their multi-domain SC RFID security breaches and the pairwise comparison can be performed without issues. A mean score of 4 were achieved.

Interoperability

An attempt to evaluate the following:

Does the framework work with other supply chain operation reference

Survey question: Are you using other supply chain models when you were using the RFID security framework? If no – go to question 7.

Identify the number of unintentional conflict decisions for the framework in working with other SC models.

0	5
1	4
2	3
3	2
4	1
>= 5	0

Table 57 Answers in Likert Scale for Evaluation of the RFID Security Framework to Framework Interoperability

The question relates to other established SC models the study target was using alongside with the framework. As a security framework that provides solutions that can be interoperable with other established SC models, conflicting situations reduces the effectiveness of the framework. Multi-domains concept has been adopted from Kim et al.'s multi-domain model, and this framework attempts to highlight prioritized solutions to be applied in controlled domains even if RFID security breaches were introduced from the uncontrolled domains. For example, if the user used the framework and found a prioritized solution to enforce a policy as a SOP, with SCOR model running in place in the company, does the user has difficulties in identifying the SOP in an already devised SCOR number? Or multiple SCOR areas have to have the same SOP updated? Or even worse, does the existing SCOR model need to be revamped in order to work with the framework? The mean of the score is 6, meaning the framework has no issue working with other existing SC models. For study targets currently not running other models, the mean calculation of this question has been ignored. A mean score of 3.92 was reported from 14 study targets who run the framework with another SC model.

Scalability

An attempt to evaluate the following:

Can the framework apply to the extreme case studies selected?

Survey question: The framework can handle bigger and smaller RFID security breach in supply chain. Do you agree with this statement?

Strongly Disagree	0
Disagree	1
Slightly Disagree	2
Slight Agree	3
Agree	4
Strongly Agree	5

Table 58 Answers in Likert Scale for Evaluation of the RFID Security Framework to Framework Scalability

A quantitative question is being asked for the evaluation of scalability. In a six-month period no study target that has experienced another RFID security breach that has grown or shrink in size. A mean score of 4.44 was received. However, it is worthwhile to note that the study group members have problems with financial impact from the loss of a single piece of jewellery of few thousand Australian Dollars up to financial impact of 10 million dollars of radioactive cancer treatment cases; not to mention non-financial impact of this case. The framework performed in both cases without issues.

Efficacy

An attempt to evaluate the following:

Does the framework reduce security vulnerability solely based on the prioritized solution identified?

Survey question: How many prioritized solutions have to be applied for the identified RFID security breach in multi-domain supply chain totally solved?

1 – just the prioritized solution	5
2	4
3	3
4	2
Not totally solved even applied all 4 solutions	1
No impact at all even applied all 4 solutions	0

Table 59 Answers in Likert Scale for Evaluation of the RFID Security Framework to Framework Efficacy

Reliability tests whether the framework reduces security vulnerability, and this is a qualitative question. RIFD security breaches in multi-domain SC incidents or lost amounts are counted before and after the application of the prioritized solution breaches. For a solution to be successful, a six-month period of application of solution requires all incidents of the breach being identified to be totally resolved in order to achieve a score. For score of 5 requires an application of just the prioritized solution, 4 for 2 solutions, 3 for 3, 2 for 4, and 1 for improvement of situation after 4 solutions were all applied, reflecting minimal effect on prioritizing the solutions but the solutions were somehow effective. A score of 0 meaning all solutions applied but the RFID security breaches in multi-domain SC were not reduced at all. A mean score of 5 was received.

	HE							OE							UU								HA			Mean
	1	**2**	**3**	**4**	**5**	**6**	**7**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**1**	**2**	**3**	
Completeness	5	5	5	5	5	5	5	3	5	5	5	5	5	4	5	5	4	5	4	5	5	5	3	5	5	4.72
Extensibility	4	4	4	5	5	5	5	4	4	5	5	4	4	5	4	4	4	5	5	5	3	3	4	3	5	4.32
Usability	5	3	3	5	5	4	4	4	3	2	4	5	5	4	4	4	4	4	4	5	5	4	5	4	5	4.16
Functionality	3	5	5	5	4	5	5	4	4	5	5	5	3	4	4	4	5	5	4	4	4	4	5	3	4	4.32
Reliability					4	4	4	4											4	4						4.00
Interoperability	5				4	4	4	4	4	2	5				4		4				3	4		4	4	3.93
Scalability	4	4	5	4	5	5	5	4	3	5	4	5	5	5	3	5	5	5	5	5	3	5	4	5	3	4.44
Efficacy	3	5	5	3	5	5	5	4	5	3	4	5	5	5	5	5	4	4	5	4	3	3	4	5	4	4.32

Table 60 Evaluation of Framework by Focus Group Members after Application of Prioritized Solutions

8.6.6 Evaluation Result of the Framework

The focus group members generally endorsed the framework, with a score >= 4.0 were received from the survey, apart from interoperability which a score of 3.93 was scored. This represents the framework being approved by users who have been using it. The scores are tabulated as shown in Table 45.

One might argue that the use of Likert scale or interpreting the Likert scale by mean instead of median is not sufficient. Of course, more complex analysis exists such as frequencies[39], contingency tables[40], χ^2 tests[41], the Spearman's rank correlation coefficient[42], or the Mann-Whitney *U*[43] could be used. Though, for the simple question whether the framework is endorsed, Likert scale with ordinal data should be used. Jamieson (2003) suggests the use of parametric tests should be used with Likert scale ordinal data for adequate sample size of 5–10 observations per group and data are nearly normally distributed, which fits the focus group study.

8.7 Discussion

The use of AHP Analysis to apply the policy framework is extremely easy to understand, as SC practitioners can just follow the multi-domain SC and find out the areas of possible security breaches. Manual counting RFID security breach incidents or calculating each security breach financial impact can easily determine the four priorities, with simple arithmetic or the use of pairwise comparison if necessary, to retrieve the four percentage numbers. The use of AHP Analysis can direct the RFID vulnerability to the policy framework and SC practitioners can then prioritize RFID security threats solution just by using four numbers.

---

39 Statistics studies including percentage that represent positive responses

40 Correlation study between two variables by a table showing the distribution of variables in rows and columns

41 χ^2 test, or chi-squared test, a statistical hypothesis of samples in chi-squared distribution

42 A nonparametric measure of rank correlation named after Charles Spearman.

43 A nonparametric test of the null hypothesis that compares randomly selected values from different samples.

The evaluation of the framework by focus group member shows the framework has been highly praised by the focus group practitioners. A focus group member was able to further ask only four pairwise comparison questions with simple arithmetic to give meaningful analysis to his management, in order to support his business initiatives. "*Amazingly easy to use, systematic approach for management based on facts and data*" was the exact wording given after he analyzed his business case without the aid of the researcher. Full report of focus group members' business case applications are documented in Appendix I.

9 Summary and Concluding Remarks

9.1 Introduction

The research objective of this study is to develop a multi-domain RFID security model for global SCs, and a practical framework for adoption. Throughout nine chapters, the objective was met with details as follows.

9.2 Summary

This study attempted to solve the RFID security vulnerability problem by providing a policy framework directing to prioritized solutions to such problem. Various authors attempted to tackle this problem, but they are either too generic to all RFID vulnerability or not specific to supply chain, focus only in the context of single domain's supply chains, or too convinced to a type of RFID standard being used. It emerges that there is no existing security policy and standard in worldwide practices. This study will supplement this missing element in research literature in analysing the security breaches, using design science approach (detailed in section 4.3) as the basis of design methodology, to solve RFID vulnerability in supply chains.

Design science was used in this study, where qualitative methods were adopted to enhance understanding of the motivation and reasons behind the study, followed by quantitative methods to analyse and validate the results. Visit to past literatures forms the scope of this study, with a model that is drawn from mini-case study's semi-structured interview results, and a policy framework to test the model through focus group members' actions . Artefacts were built in every step of the way, as suggested in the design science approach.

Such artefacts included a comprehensive list of RFID security vulnerability retrieved from the scholar literature that was generalized in a multi-domain SC, i.e. the "Direct", "Associated" and "Uncontrolled" domains. These domains also formed the basis of the RFID Lifecycle, another artefact conceptualized to define the start and end of an RFID in a SC. These two artefacts explained why RFID implementation in SC does not give a clear improvement over security breaches on the SC (illustrated in Table 25). Scholars identified that application of RFID in SC brings operational benefits (discussed in 2.5.2) but will not improve security .

A conceptual model, EMDSCRV, was then built with different RFID Lifecycles in SCs. The model directs security breaches to four causes and sources (namely, UU, HA, OE, and HE). The model highlights areas of security breaches in different domains of SC by categorizing security breaches by their causes and sources. Two forms of models were used to show the

security breaches in TEI and LEI. Literature provided solutions to these causes and sources that can be applied to TEI SCs as they are relatively simple. A single cause or source of vulnerability can be directed by mapping the causes and sources to literatures.

However, for more complex LEI SCs, it might be more difficult to apply such solutions to associated and uncontrolled domains' vulnerability, since there are limitations in real life business environment, especially inside the uncontrolled domain. The model can present RFID vulnerability in multi-domain SC visually to controlled or uncontrolled parties for them to trace these vulnerability issues easily. However, this model treats all security breaches with the same weighting. Hence when we want to apply EMDSCRV model practically in our real business world, multiple solutions identified should be prioritized before applying any of them.

A policy framework was built to prioritize solutions for application in various domains. The practical policy framework is easy to apply and test the EMDSCRV model (done by focus group, documented in chapter 9). These tests include steps of analysing the practical policy framework via a MCDM problem, using AHP. AHP Analysis was addressed by the focus group as extremely easy to understand with just manual counting RFID security breach incidents and simple arithmetic calculation for suggesting prioritized solutions to certain RFID vulnerability. The use of pairwise comparison is intuitive, and concludes such priority by giving only four numbers (the ranking).

Design science methodology also suggests evaluation needs to be performed to artefacts, and the focus group's application of the EMDSCRV model by the practical policy framework was evaluated by Likert scale on all the evaluation criteria. Final results have shown an average score of 4.7 as approval and satisfaction rates, and the practical policy framework was highly praised by the focus group members (documented in chapter 9).

9.3 Concluding Remarks

Multiple solutions can be applied to multi-domain RFID threats. Many scholars (discussed in section 2.7) highlighted common solutions where they were only considering the problem itself but not the whole picture of the security vulnerability. However, in real world business cases, especially applying RFIDs in LEI , where longer lifecycle of RFID spans across multi-domains in a SC, vulnerability could arise from domains where SC practitioners have no control over.

In the cases reported from focus group meetings, the causes HE, UU, HA, OE have different vulnerabilities that constitute a single security breach, and after pairwise comparison and AHP, the prioritized solution found could be different. So the question is, why could the same RFID

security breaches have different causes and sources, and why can't a simple and single solution solve a similar security breach?

The following discussion was reasoned with the collective ideas from the focus group, where most of the group members shared from their experience of current difficulties they were facing. Most of the focus group members tend to complain about information systems and solutions, while others believe that information system is a separate topic from business in general, unlike traditional business studies such as accounting, finance, legal, marketing, and others. The following summary and analysis are going to show possible reasons why are there multiple solutions to SC RFID security threats, while security threats of other businesses tend to have single solution as evidenced from the literature.

9.3.1 Impact of Length of RFID Lifecycle to RFID Vulnerability

RFID lifecycle in LEI is longer than that of TEI, and the application of RFID can span across multiple domains. The jewellery industry, a TEI, was studied and the application of RFID was limited only to the retailer domain. On the other hand, the pharmaceutical industry, a LEI, has RFID covering various domains on the SC. Longer RFID lifecycle could have more causes of RFID vulnerability and such multi-causes high complexity vulnerability needs multiple solutions to them, as longer RFID lifecycle SCs have certain characteristics that is different from shorter RFID lifecycle SCs.

Supply chains are multi-domain, so are its breaches.

Therefore, a generic solution that exist for a specific cause or source could not be applied because the problem happened in a place that falls in to "uncontrolled" or "associated" domains. For example, shall "training" be the solution for RFID re-tagging to ensure tags are re-tagged in a right manner. In the case of "uncontrolled" domains, the solution could be an "operation policy" so that no re-tagging shall exist at all, simply because training cannot be achieved easily and even if so its results are not guaranteed.

SCs by definition are three or more interdependent companies from the upstream to the downstream in managing supplies. The key word here is "interdependent". SC members are independent companies but they are also highly dependent on other members in the SC. For example, a brand owner would outsource certain key operations to third party logistics providers. However, this is not the case in other industries. For example, an accounting firm might not have key operations outsourced to other parties. The SC industry are by definition multi-domain as it attaches to trading, which generally involves more parties.

Supply chains tend to suffer from longer distance, so are its breaches.

As last section suggested SCs are attached to trading and involved with more parties. GIn general, factories are highly specialized in one field and hence goods need to be transported to far distance. The breaches would also suffer from long distance as well. For example, operating environment changes much along the long travel distance of goods , and attacks can come to the weaker link in the SC than environments with good control. A shipment with goods from original to destination could be in well controlled environments before its port of original and after port of destination, but in between transit points there could be operating environments that are easy targets for attacks. Attacker could use long range reader in transit points with more exposed operating environment to capture RFID information. These lead to multiple solutions for a single RFID security threats.

Supply chains tend to be complex, so are its breaches.

SCs are complex as it involves various operations. Previously scholars tackled problems taking place in environments with just one or two operations, but in a normal SC environment, 20 to 30 operations are considered common. A typical SC in the SCOR model would involve Plan, Source, Make, Deliver, Return, and Enable. If the pharmaceutical and jewellery SCs are taken as examples, parties involve in the Plan stage could include sourcing, factories, and various work in progress vendors, and any parties that balances aggregate demand and supply for sourcing, production, and delivery requirements. Source stage could include the above parties that procure physically for goods and services to fulfil planned or actual demand, say for example the freight forwarders who expedited the goods. Make is the stage that takes the product and transform to the finished state to fulfil planned or actual demand, in the case of jewellery, it will be the steps of cutting diamonds, meltdown and assembling them into jewellery pieces include specific factories and craftsmanship; whereas in pharmaceutical case, it would include outsourced packaging companies. For delivery process, the retail shops would be involved in the jewellery SC, and while the hospitals, medical clinics, and pharmacist would be included in the pharmaceutical SC, as finished goods and services are delivered to fulfil planned or actual demand. Return process includes courier companies, as they are associated in the stages of returning or receiving returned products. SCOR model also includes an additional process, namely Enable, as SCs are getting more complex, outsourced fourth party logistics professionals enabling the SC would be involved. SC's businesses are more complex compared to general businesses.

Supply chains tend to be globalized, so are its breaches.

SCs can span across thousands of kilometres and therefore a globalized approach to the problem is needed. For example, local legislative laws and requirements such as tax could lead to potential problems of RIFD disposal. So a problem exists in one domain in a particular country, say retailing, might not exist in the same domain in another country. In the study, businesses in Pearl River Delta of China exporting to Perth in Australia has been selected as primary targets of semi-structured interview, before the study expanded into the SCs of these primary targets. This is just one simple example of SC, involving China and Australia governments. Indeed, for all the complex processes that enables SC behind the scene, a lot more stakeholders are included. For example, Hong Kong ports which handle most logistics for the Pearl River Delta goods from China could have a different legal system to follow instead of the Mainland Chinese and Australian ones. Especially for products that are sold in different countries globally, the rules and regulations are different which made the solutions to RFID security breaches more complex. For example, the use of long range reader to eavesdrop RFID information is illegal in some places but not in others, so the solution to eavesdropping in these places could involve both policy cultivation and hardware enhancement, where one simple solution would not suffice.

Supply chains tend to be multi-aspect, so are its breaches.

SCs involves areas in marketing, accounting, legal, information systems, transportation, distribution, just to name a few. For past studies by various scholars the cause and source problem were viewed from a single angle: information systems. For example, hacker attacks in finance systems have only one single database to target. However, since SC involves different aspects, attackers could attack the system based on the EDI inputs from the transportation database, creating an error with EDI imports, and then penetrate into other module of the system. For general companies, such as finance system, this would not be possible as not many parties are connected to the financial systems with direct EDI imports compared to the SC.

Supply chains tend to be under-rated, so are its breaches.

SC systems could already be vulnerable before the application of RFIDs, since SC systems are comparatively less important compared to other professional systems. For example, financial systems could have strong firewall and other network intrusion detection systems, while SC systems are relatively weak in protection. When RFIDs are implemented to an already vulnerable system, then the security breaches could be rather straightforward. For example, a financial system server that records daily financial transactions could be more difficult to hack

compared to SC transaction systems. Therefore, SC systems that RFID apply to is easier to hack compared to other systems, due to already in place security measures.

Supply chains tend to be operated by frontline workers, so are its breaches.

SC operators are generally more front line junior staff instead of management personnel in comparison to other fields such as legal, finance, accounting, and medical. These junior operators could have less, if not lacking altogether, common sense in business computing to operate these RFID systems, which might create more human errors easily. However, training, the top solutions to general human error, could be too difficult for general SC operators. For example, sole solution training could be sufficient for bank tellers for RFID bank customer card problems, but in SC, training could be difficult for warehouse operators due to the nature of bank tellers might have higher general knowledge than warehouse operators. Additional standard operating policies, which could be common sense to bank tellers would be required in the case of multi-domain SCs.

Supply chains tend to be difficult to plan, so are its breaches.

In view of the SCOR model, the first process is Plan, which a lot of SC fails because of bad planning. Lack of planning is the primary reason for a SC to fail. For example, a typical process in the planning stage is to forecast demand, in theory if the forecast demand is 100% equal to the actual demand, then there is no inventory and out of stock problem, which costs SCs a lot. A failure to plan demand properly will also cause the RFID systems to fail too. For example, the stock level fluctuation could create RFID interference, reduce reader's speed so that it could not handle automatic scanning, or increase the number of RFID tags being scanned per second beyond the capacity limit. These are RFID breaches that cannot be solved just by increasing hardware units but maybe software data limitation as well.

Supply chains tend to evolve in nature, so are its breaches.

SC are not only difficult to plan, it has an evolving nature as well. Business situation changes every day, and companies could be engaging into new markets without proper knowledge. For example, a pharmaceutical trading company had to repack drugs that formerly were not packed by them in order to reduce the shipping cost. This created issues as RFID that were tagged by manufacturer previously were now required to be tagged by distributors, and the company had evolved in the SC, from the domain of distributor to manufacturer as an assembler. Solutions to such RFID breaches would therefore need to cater to the evolving nature of those RFID security breaches themselves, and more than one solutions could be required as a result.

Supply chains solutions tend to launch before substantial preparation, so are its breaches.

SC solutions are always launched in a short time due to they are being revolutionary in nature, less time are allotted and testing are really basic compared to other businesses. Sometimes, pilot testers are customers and they are taken as the "guinea pigs" . As a result, most problems that can be fixed before launching are skipped until the problems grow bigger, to a stage where a single solution is no longer enough to fixed the system. For example, an online shipping tracking and tracing system using RFIDs might encounter security breaches of misread from peak time sorter in an express company. Instead of changing hardware solution prior to the launch, the system can't be stopped due to the express company's nature for additional hardware systems to be installed. It will then involve a policy solution for a verification of RFID scans in operations. This inclusion of policy as a solution is due to a system being launched without fully tested, which is unlike all other systems with adequate time for testing.

Supply chains tend to be lack of risk control, so are its breaches.

Similar to lack of time for testing, risk control also tend to be weak compared to other systems. In risk management, the basic idea is not to use more resources to control a risk, as the threat might or might not happen. The stage of unknown whether a threat would happen is called "at risk". In a SC, most of the time the loss for such risk is the cargo value, and that can be predetermined before such a risk happens for the company to absorb, or to perform risk transfer to insurance companies. This is true in all of the cases of jewellery SC, where application of RFID, or risk reduction of SC loses, is absent in domains that are uncontrolled. Risks are simply transferred to insurance companies. A solution without proper risk management procedures could incur multiple sources of security threats and therefore solutions are also tend to be multiple aspects basis.

Supply chains tend to be lack of backup and contingency plans, so are its breaches.

The study of risk management includes also backup and contingency plans in the stages of risk control. As SC is relatively weak in risk control which provides backup and contingency plans, when loss happens in risk management, they don't fall immediately to the backup plans. In such scenario, a solution needs to be deployed immediately instead of having backup plans in place to minimize the loss. For example, if an RFID misses a scan due to peak time sorting, there should be a manual fall back control as backup and contingency plan available. However, if such plans are not available, then both hardware and policy solutions should be in place to confirm a successful scanning. This could require additional solutions to a single problem .

Supply chains tend to different tolerance levels, so are its breaches.

Different SC operations are equipped with extreme tolerance levels to RFID system downtime. Some SC operations, such as warehousing and freight management systems, require immediate response time. Even a few seconds' downtime of the system could mean warehouse could not receive or export goods and freight management system could not ship goods in the port or at the loading docks. It is easy to understand that such situations are not tolerable. However, for back office operations such as demand forecasting units matching supply and demand, or planning and enabling SC operations, the tolerance level of system down time are much greater, due to the non-frontline nature of the operations. Therefore, the solutions to the RFID security breaches also come in extremes, a fast response, high cost solution to those front line operations, and low cost cum slow response solutions to those back office supporting roles. For example, a freight forwarder and warehouse operators require RFID systems that gives zero downtime while logistics planner could allow downtime for systems, therefore, both hardware and policy solutions could have taken place for the SC.

Supply chains tend to work in sequential steps, so are its breaches.

SC operations are dependent on previous steps and its results would affect subsequent operations, therefore, solutions of preceding steps and post operations must also be applied. For example, a freight forwarder would have forwarded pharmaceutical products to a pharmacist, carrying a policy solution for mis-tagged RFID tag. Such solution will continue to the pharmacist's domain, although it can have its own solutions for a point of sale (POS) system. This will incur additional solutions for RFID security threats as products moves along the SC.

Supply chains tend to be lack of understanding, so are its breaches.

SC solutions are built by computer scientists, who are trained with science and mathematics background in general. However, SC are also business studies of how goods move around and fulfill customer needs. While a computer scientist could understand perfectly some information systems, SC systems are considered to be more difficult to understand. As reflected by some focus group members, it was very difficult to hire talents who understand SC, as individuals without frontline operational experience have difficulties to recognize business needs. For that reason, a single and effective solution could be hard to achieve.

9.3.2 Research Limitations and Implications

The initial study was based on qualitative approach, and the research limitation hindered a more generalized result. The study was limited to the semi-structured interview performed with two groups of 25 companies from each of the two industries, and the four focus group meetings to evaluate the framework. Although efforts have been made to reduce bias (discussed in section 4.2.5), such as focus group meetings members were not selected from the semi-structured interviewees, further policy framework application and testing (discussed in section 8.6.5) are encouraged to be established and tested. Furthermore, the uncontrolled domains of the SCs are the reason for the framework to undergo a quantitative analysis (such as AHP and pairwise comparison matrix in section 8.6). Scholars suggested the transparency of SC and management should be done in a systematic way. It is expected SCM will continue to eliminate the uncontrolled domains by the introduction of ERP, Materials Requirement Planning (MRP), Vendor Managed Inventory (VMI), and other SCM insights. As a result, the conflict thinking between various parties in the SC might be addressed and weighted, in order to achieve mutual benefits among all parties.

9.3.3 Practical Implications

The EMDSCRV model leads to further research in terms of how different industries will be able to address their RFID security breaches, with respect to the ease of use and evaluation for analysing financial and other impacts that can be saved by the organization. The framework provided a way to find prioritized solutions by the use of AHP and quantitative approach. Practical implication of this study includes a relatively easy framework for highlighting areas of RFID security breaches, enabling the use of models in SC in relation to RFID security breaches. Prioritized closure of RFID security loopholes for solutions to several security breaches can be performed, providing systematic approaches that can lead to robust solutions to tackle RFID security breaches issues.

A tool that Highlight Areas of RFID Security Breaches

The results in RFID security causes and sources by investigating major security breaches leading to a study that is easy to understand. Areas of RFID security breaches are highlighted and further study of causes and sources can be studied. Proven solutions from scholar writing to these causes and sources could be solutions to these RFID security breaches.

Relates Security Breaches to Supply Chain Operation Reference

Extensive research work has been done by the SCOR model (discussed in 1.9.4) and each SCOR level activity can be further matched to identify SC activities where security breaches might occur. For example, relationships between variables in improving performance in SCOR

model[44] and tools for assessing supports[45] can also be related to possible RFID security breaches in such SCOR sections. Relating security breaches to SCOR can give a wealth of knowledge to researchers including relationships and supports, and other information that can link security breaches to previous studies that has been categorized by SCOR.

Prioritize Closure of RFID Security Loopholes for Solutions

This approach also adds to academic knowledge of prioritizing fixing of security loopholes in security management[46]. As tackling a single cause/source of security breaches can possibly eliminate multiple RFID security breaches, actions can be taken in a prioritized manner to fix a maximum of RFID security loopholes while minimizing efforts.

Robust Solutions to RFID Security Breaches Issues

Robust solutions have to be adopted to tackle RFID security breaches, as RFID applications tend to be robust in SC operations[47]. The study has been performed in a systematic manner, whereas quantified results can be further used to evaluate performance or make improvements.

Link up with Other Approaches

Other approaches to manage various causes of RFID vulnerabilities include linking the impact of each vulnerability issue on SC performance. One of the commonly used performance models in SC is the SCOR model. It would help us understand which vulnerability will have more impact on the performance of one preferred SC. That would help various domains decide which area would need more effort to implement a particular approach to manage the RFID vulnerability. As the SCOR model addresses the SC as a single entity, this model should give a good understanding of RFID vulnerability under the SCOR model categorization.

Another research can be performed to apply the results to the balanced scorecard, where further studies on the interviewees can be done in seeking for the results of these security breaches. For example, reapplying a tag incorrectly could lead to possible loss in return on investment of financial growth perspective in a balanced scorecard. While the RFID security breaches are identified and solutions applied, a framework on RFID security breaches cause and effect relationship model can be constructed, based on the balanced scorecard model.

It is also interesting to study the resource requirements for applying the conceptual model in comparison with the likely benefits. Semi-structure interviews and focus groups performed in

---

44 Ganji et al (2015) identified variables in SCOR model.

45 Peiris et. al (2015) used tools that support the SCOR model.

46 Jerhotova et al (2015) studied prioritizing security loopholes in security management.

47 El-Awamry et al., 2015; Scherhäufl et al., 2015

LEI and TEI for assessment might not be practical in some industries. A further interesting point would be to investigate the comprehensiveness of the conceptual model generated. These issues will be the focus of further research in the area.

9.3.4 Social Implications

The proposed research will provide a crucial contribution to a safer production environment in factories. Buyers will be assured that all items produced are tagged with RFID that is secure across the entire SC, reducing direct and indirect financial impact on services and products. For SC systems designers, the research will provide an effective and efficient guideline to direct technology and application development.

9.3.5 Originality and Value

The prime value and uniqueness of this study lies in the generalized study considering all types of RFIDs in a multi-domain SC. Previous researchers either tried to deal with the situation in a single-domain SC or were too convinced with a particular format of RFIDs being used. To the best of the author's knowledge, this is the first literature to put forward a generalized conceptual policy framework with a quantitative analysis, and specific suggestions are made for future researches in this area.

10 Appendix – Real World Application of RFID SC Security Framework

Note: The application of the prioritized solution in RFID SC Security Framework might not totally solve the RFID vulnerability problem in SC. However, some focus group members believed applying only a prioritized solution will give the best return on investment to the RFID vulnerability problem in SC. The cases in this appendix has no intention to lead to any believe of the entire RFID vulenrabiltiy problem is solved by applying only the highest priority solution.

Focus Group Member HE1:

"Reapplying RFID tag caused messes and shall not be practiced at all"

– Focus group member

The focus group focal company is a single shop small jewellery retailer that uses RFID to aid point of sales management. The RFID tags are carried on a piece of small paper price tag, and often removed for customer inspection on jewellery, the price tag contains only the price and few pieces of information that are coded so only shop keepers know the details about the jewellery.

Security Breach

Security breach was reported when a customer did not purchase pieces of jewellery with tag removed; the removed tag was reapplied back to the piece of jewellery by the shopkeepers. Chances are human error to have reapplied the tag to the wrong piece of jewellery, especially in the cases where two pieces of jewelleries with tag removed, and the tags were then swapped.

The solution of this security breach is standard operating procedure (SOP) for to the staffs handling the RFID tags. The SOP indicates clearly that no detach of RFID tag until the product is fully paid by the customer. There was also software changes where the tag can be temporary hold in the computer system to indicate that this piece of jewellery is being held by a customer. In addition, the re-application of the RFID tag is now done by a management level of staff that is with higher level of training and the problem of re-tagging to wrong jewellery merchandise does not exist after such changes.

Users were also reminded that the RFID paper tags were not supposed to be trashed even though the product is being purchased. A manual form was introduced, which will be filled in

with dates and the RFID paper tag being taped to it, within the allotted period where the jewellery is be allowed refunded. Shall the jewellery be refunded; a manager level store staff has to re-apply the tag with a RFID handheld reader to verify the tag data. Otherwise, the form is stored with a RFID reader to read the tag for verification of product sold in addition to the normal process. After the application of these new SOP, no further RFID security breaches were reported.

Focus Group Member HE2:

"RFID reading is the key to data, the key can be accessed remotely by people from a distance so data must be stored properly"

– Focus group member

The second focus group member is a pharmaceutical company. The company uses USB storage devices and were purchased and kept by the Secretary of General Manager but without proper housekeeping procedure to follow. It is reported that a file storing barcode numbering information had been leaked to third party in the past months. After checking, it is found that some information was stored in USB storage devices, where these has not been properly deleted before passing to a new user of that USB.

Security Breach

Their RFID security breach is related to the mismanagement of the company's storage device, which had resulted in leak of confidential information to third party. There were three storage devices for use by different Departments, and every single staff has their way of file management. Some simply left it on the USB storage device, some deleted the confidential files with undelete possibility. Some wiped out the USB storage device by software tools.

The above problem not only creates risk of information leakage, but also reveals the loophole in managing fixed assets in the company. To address the problem, the General Manager defined the responsibilities that were assigned to relevant departments with the following operation flow regarding such USB storage devices with RFID information.

Administration and Accounts Departments

1) Purchase of fixed assets should be approved by authorized staff in advance.

2) Purchase of fixed assets will be handled by relevant department who has the expert knowledge on the items. For instance, purchase of USB storage devices will be handled by IT Department.

3) Accounts Department will maintain and update the list of fixed assets. Information like department owner, purchase date, items details, purchase price should be recorded properly.

4) Each item under the fixed assets list should be labelled properly and checked every year-end.

5) A procedure of lending USB storage device should be set up and followed properly.

a) A staff should present his/her company ID card to Administration Department for registration before the recording device is handed over to him/her.

b) The staff lending the USB storage device has the responsibility to empty the files before returning it to the Administration Department.

c) When a staff returns the device, Administration Department will check whether there are any leftover files from the device. If company files were found, the staff will be issued an email warning. If the same happened again, the staff will receive a written warning letter, which will be filed under his/her appraisal records. The warning will be given by HR Department, which will be contacted and updated by the Administration Department of the incidents. On the other hand, if no files were found, Administration Department will keep the device until next lending. The responsibility of Administration Department is to ensure each USB storage device contains no files during their custody.

IT Department

1) IT Department has the responsibility to select suitable USB storage device with password or fingerprint for each Department by exploring their requirements and the features of each USB storage device model.

2) IT Department has to consider the efficiency of the USB storage device in matching with company's IT system.

3) IT Department has to give training to the staff who needs to use the USB storage device, and write policies regarding saving and removing files in USB devices.

4) For any malfunction or damage of the USB storage device, the staff should contact Administration Department who will contact IT Department to fix the problem.

5) If any device will have to be written off, IT Department has to report to Accounts Department.

With such operation flow in place, the focal company was able to reduce RFID security breaches to zero incidents. The focus group meeting attendance further suggested a standard operating procedure (SOP) should be written in order to prevent future human error in this area.

Focus Group Member HE3:

"RFID is not perfect as I still need to read from the RFID handheld display and verify paper based information, adding a 2D barcode scanning for further automation improved accuracy"

– Focus group member

The focus group member works in a pharmacy with a small warehouse to keep medicine stock in between deliveries. When the storekeeper manually compares medicines against reorder level, they will report to the procurement team. Then procurement team verifies item sales record and make orders with the supplier, which is a pharmaceutical company.

When an order arrives to the pharmaceutical company, they will acknowledge the purchase order shall stock is present in warehouse. Outsourced logistics department will pick and pack the required pharmaceutical products from their warehouse in correct quantity and sent out to the required pharmacy store.

In this particular pharmaceutical supply chain, RFID is used in item level, attached to every single drug box. Scanners can check and confirm on quality (say expiry date) and quantity. An enterprise resource planning (ERP) system is used for input, while communications of purchase orders are done by electronic data interchange (EDI). Product information are verified by handheld scanner, cross checking the product physical RFID including brand name, batch number, expiry date, pack size, and quantity match with the ERP database. After checking the picked and packed box content, a new label with RFID is being printed with a unique number and the box content.

The delivery team of the logistics company only works with this new label, and RFID scanning is performed in every checkpoint of the delivery chain. At each step of the way, the pharmacy store can check the goods delivery status by smart phone applications or webpage.

Upon delivery, the pharmacy store checks the items to make sure they match with the invoice and purchase orders.

Security Breach

Security breaches experienced by the case study focal company includes Human Error, where the delivery chain RFID scanning matching are still verified by eyeballing (RFID hand held reader display matched against purchase order number and delivery address). Shall the data do not exist in the system; the logistics company is allowed to input data to the drug importer's computer system at the time of scanning, which introduces human error. Errors occurred from time to time and the current prevention plan is to print a 2D barcode in the purchase order, and the handheld scanner to scan the RFID with a verification of a second scanning to the 2D barcode printed on the purchase order. Delivery address approximation to proximity of 150 meters was also verified by this handheld device with mobile location positioning systems.

Focus Group Member HE4:

"Information retrieved by RFID scanning must be real time to make system works for Make-To-Order Jewellery, and I believe this is a requirement for all businesses"

– Focus group member

The focus group member is a Hong Kong jewellery retailer with manufacturing operations in a make-to-order mode to produce jewellery, in which they can react to customer requests very fast, and customers expect them to promptly confirm orders, make on-time deliveries and carry out the high-quality standards.

For the supply chain execution of this focal company, employees need to work manually with documents to track-and-trace order fulfilment status one by one. If there is any order inquiry about its status, the employees have to look into many paper-based forms and reports to find out the track-and-trace status.

With such manual work, workload is heavy and human error is unavoidable. Statistics and calculations for company management are also calculated by hand. This is not only slowing down the progress of the operation, and information is often wrong with delayed information being used in making business decisions.

In order to solve the track-and-trace and delayed business reporting issue, RFID was applied for the benefits of faster tracking and tracing and real-time information availability. Distribution centre can be improved by automating the handling of thousands of products parts daily on conveyor belts, with RFID readers built on the side. When RFID tag with jewellery goes through the RFID reader, the transport belt will auto distribute the jewellery to the branch of retail shop's tray. This distribution process can maximize scalability, decrease human error and save time.

In the past, when employee worked without RFID system, same day finished make-to-order jewellery were not able to deliver to retails shop within the day, but was made possible with this RFID system. Stocktaking was done by one-by-one eyeballing and counting has been improved by the use of an RFID to scan the display window, which individual counts of categorized products are counted at once.

Security Breach

The focal company suffered from security breach of physical stolen of jewellery in the shop. While most jewellery shops have implemented counting and alarming system for the count of RFID in display cabinet, which should be equal to the computer inventory record. This case study focal company has difficulties to implement such system due to the business model of this company being a make-to-order one. Replenishment of jewellery count is based on real-time figures of jewellery workshop whereas traditional jewellery shops have purchased and delivery orders for jewellery counts.

Normally in this focal case study company, jewellery salesman process jewellery in a one-on-one and a one-to-one basis, which means one salesman takes care on one customer, and every single customer can only view one single product on hand; to view another piece of jewellery product the customer has to first return the last piece of product back to the cabinet, unless two salesmen simultaneously serve one customer. However, retail shop environment would be crowded at peak hours and theft of jewellery always happens during peak hours.

The case study focal company experienced thieves pretending as buyer and take advantage of peak hour's chaotic environment to steal and escape, with the aid of RFID signal jammer. Indeed the case study focal company has setup security systems, such as closed circuit television (CCTV) System, alarm systems that connect to police departments, and in-shop product temporary use safe & vault for extremely valued diamonds and gems. However, the above-mentioned security equipment is used for theft deterrence, insurance requirements, and videos recorded to contribute to police after stealing already happened.

In order to prevent further RFID security breaches, the company has applied real-time update for the computer system to update the count of the jewellery in the display cabinet, right from the completed make-to-order from the jewellery workshop. Although in real practice the update of this jewellery count is more difficult compared to a traditional jewellery shop where all products were standardized, efforts were made to build this real time system in order to avoid RFID security breaches.

For extremely expensive diamonds and gems, the case study focal company sets up user authentication, which has an entry limitation for the retails shop. Customers must register their

individual information to company headquarter directly prior to entrance of the extremely valued diamonds and gems areas with the customers' full name, contact number, identification card or passport number's first 3 alphanumeric characters and email address. Upon arrival to the shop, the customers must provide the proof of registered identity to employees for verification.

Crowd control was also implemented to avoid theft. Strict rules of one visitor per salesperson were enforced in addition to the one-on-one and one-to-one rule. At any point of time, the number of customers cannot be more than the number of salespersons in the retail shop; extra visitors have to line up outside the retail shop with product catalogue provided for reading while waiting. Interestingly, this customer line up arrangement, along with pre-registration requirement for viewing extremely valued diamonds and gems, started as a security measures due to RFID security threat of make-to-order jewellery, delayed information has created customer's interests in marketing possession desire as a side benefit.

Focus Group Member HE5

"Our drugs are time sensitive, RFID scanners verifying good operation policy in practice could reduce human error"

– Focus group member

The case study HE5 focal company produces a nuclear product for healthcare and leads the development of Turkey's nuclear medicine market through the production of high-quality radiopharmaceuticals mainly for cancer diagnosis and treatment.

The focal company has a supply chain that highly focuses on speed. Radioactive materials have half-life issue and therefore once the production finishes, medicine has to be consumed within a short time compared to traditional drugs. For example, one of the company's medicines with 110 min half-life radioactive component has to be tested, safely packed, transported and consumed within 8 hours after production is completed. Otherwise, it will not only be a waste but some could be hazardous for taking. For this reason, fast supply chain actions from production plant to hospitals are very important. The focal company uses RFID system mainly for this reason with a good financial justification. A small bottle of medicine could have a selling rate of US$ 350 or more. If one considers non-financial benefits then the justification of using RFID is even sounder, the rarity for treatment made the bottle of medicine simply not being easily resent. As a result, that particular patient's life might be at stake.

Security Breach

The case study focal companies have three RFID security breaches. The first one is the skipping of tag reading. Due to very short half-life issue for some radioactive materials, this kind of medicines has to be transported and consumed as soon as possible. Hospitals have been encouraged to read the RFID tag at the destination before distributing to patients to make sure the medicine's shelf life is not over. Sometimes medical nurses may skip to read the tag at the destination (hospital/nuclear medicine centres) as they would be in a rush to use the medication, due to possible peak time or awareness of the shelf life of the medication itself. In such cases, product data are manually updated by the nurse. In hospitals RFID tags are generally being read by handheld RFID readers, and so if medical nurses skip the RFID tag-reading process, there is no way to ensure the medication consumption time.

Due to the specialty of this drug, a hospital has a specific room to handle all patients requiring the taking the drug. A solution to solve this security breach is to make sure product will enter to this room minutes before consumption, which is the current case of the hospital. Then in this entrance, an automatic RFID reader is installed at the gate and recording the drug entrance time.

Focus Group Member HE6:

"From medical practitioner point of view, combining existing medical equipment with RFID reading functions can reduce misidentification of everything – patient, drugs, samples, whatever…"

– Focus group member

This focus group member works in the same company as the member in HE5, but in another department. This member works with the same radioactive drug for cancer cure and manufactures vital signs clinical measurement devices while reading patients wristband to avoid human error.

Security Breach

The security breach is about data collection of this drug after used by patients. Every patient using this drug has been provided an RFID wristband because clinical measurements of health information such as pulse rate, temperature, respiration rate, and blood pressure, that indicate the state of a patient's essential body functions, called vital signs in medical terms, needs to be reported to the case study focal company, due to the special nature of this drug. The case study focal company needs to capture and analyse such data for the company's further developments and improvements of drugs. Apart from patient safety, such data is useful for marketing purposes of next medical equipment, and current and next generation of drugs.

Currently, medical nurses take clinical measurements and re-key in the vital signs into handheld machines after scanning patients wristbands, and human errors have resulted from this as many times several patients take this medication simultaneously. The solution is to make an all in one machine to take this data while scanning the RFID wristband, however, the machine for measurement is not common as radioactive levels and effects measurements have to be taken by special and separate machines.

Focus Group Member HE7:

"Tagging RFID starts the automation process of everything and it cannot go wrong. We use two lab technicians to test all raw material arrival at quality control phase with RFID tagging at the same time; one technician is simply not enough"

– Focus group member

This focus group member is working in the same company as case HE5, in another department; he also suffers from the security breaches of human error. The case study focal company uses more than 200 chemical materials for the entire product range, all tagged by RFID, not counting the packing material. Patient's specimens are also tagged by RFID, and it is an important and risky job to manage raw materials, especially when it comes to deal with chemicals, which are highly similar, with human life at risk.

Security Breach

Even though the company uses RFID system to start identification from material level, and in fact, it is very useful and speedy to reach information easily and quickly, a very small mistake on initial tagging, removal or retagging may cause a big danger including radioactive explosion or patient deaths. A solution now is to tag RFID with two lab technicians. Every single materials reception are going through 100% chemical engineering lab-test, while tagging the RFID with the two lab technicians cross-checking with the tag ID. As an obvious risk management, production of any radioactive drugs without this tag confirmation is strictly prohibited.

Focus Group Member UU1:

"Our customer information were stolen together with RFID Handheld Device, luckily the software system limited our loss."

– Focus group member

The focus group member UU1 is a Hong Kong-listed jeweller in the main stock exchange board, with an extensive retail network comprising over 2,300 stores covering more than 500

cities, as well as a fast growing eCommerce network. The company has vertically integrated business partners for its tight control over the entire operation chain from raw material procurement, design, production, to marketing and sales through its extensive distribution channels.

The application of RFID is to improve accuracy, safety and efficiency as well as to support to future initiatives. The company built an "Automated Logistics and Distribution Centre" in China to streamline the logistics and inventory replenishment. They make use of RFID-enabled devices to enhance the traceability of each single jewellery product, ensure accuracy in stock in and out with matching computer records. In addition, RFID has been integrated with Internet of Things (IoT) technologies into the Inventory Control System, which are comprehensively applied on all inventory, logistics and retail chains along the supply chain. RFID technology and devices help the company to collect big data for timely understanding of the market development, customer preferences and shopping behaviour. The company believes the RFID system can improve their service quality and offer customers a brand new jewellery shopping experience.

The company uses smart devices, including RFID tag, logistics tray, a software named "mHand" and Smart Tray. The RFID-enabled product-serving tray helps sales assistants quickly and accurately provides product information to the customers, such as product specifications, special features and prices to exchange rate conversions. mHand is the software implemented by the company, integrating with the portable handheld RFID device to carry out stock taking quickly, easily and accurately by scanning products inside the glass counters. It enhances efficiency and accuracy in stocktaking.

Logistic Tray integrated with the Inventory Control System developed by the company is being setup in all distribution centre and points of sale. The tray is equipped with a built-in RFID sensor, and can read tens to more than one hundred of products at one time accurately. The logistics tray smoothen the sales process by omitting manual counting and searching for information operations.

With the RFID system, customers are concerned about how their data is being used, whether they are subject to more direct marketing, or whether they can physically track by RFID chips. Personal identities can link to a unique RFID tag, individuals could profile and track without their knowledge or consent. For efforts to protect personal privacy, the company guarantees the RFID tag will be removed once the jewellery pieces were sold, therefore prohibiting tracking.

Security Breach

An incident of personal privacy breach where personal data of customer information were being stolen with the RFID hand held machine with the software mHand installed, with data that are downloaded to the RFID hand held device to provide offline software functionality in a jewellery show. As the login and password of the mHand software were just merely a common password shared by all staffs, essentially all customer information was stolen as well.

The solution is to employ a strict password system and every single RFID hand held machine should be monitored. It is also recommended by the IT team to enable data services on these RFID hand held machines for real time database transaction process instead of data being downloaded to the RFID hand held, or to setup location tracking to these RFID hand held machines, when the machines are physically out of designated areas a data wipe or encryption will be take place.

Focus Group Member UU2:

"Employee pilferage is biggest threat in our industry and can be stopped by application of RFID with appropriate operating procedures"

– Focus group member

The focus group member is one of the largest pharmacy chains in the United States providing comprehensive services across United States. Different from their competitors, who specialize in mail order pharmacies and infusion services, they have more than 10,000 retail locations and medical clinics that supply millions of people each day with health care products and services. As pharmaceuticals affect millions of people's health directly, each level of the supply chain has to be very strict to ensure the quality and safety of drugs. Making sure that the company's well-being is intact, the pharmacy understands the importance of having an advanced logistics infrastructure to integrate their own facilities with third-party providers.

However, the pharmaceutical industry is facing numerous challenges and high turnover companies. Weak SCM structure has long been considered as the main cause of huge waste because of poor inventory management, medication errors, counterfeit drugs, laws and regulations.

The nature of the health-care distribution system, in all its complexity, may reduce the overall reliability of the entire pharmaceutical supply chain as it involves a wide variety of parties like manufacturers and their affiliates, drug wholesale distributors, retail warehouses, stores and clinics. Any mishandling throughout the supply chain could lead to big losses and even harm the public's health. Therefore, the pharmacy company has implemented RFID technology in their supply chain and inventory management systems to minimize losses and protect against any risk.

The company applied RFID to track object and input information associated on the tag automatically. It is a system composed of a tag, reader, antenna and software. Each RFID tag contains an EPC, a unique identifier for each item and associated with a wide range of information, including product-related information and distribution history of all parties involved in each transaction. Further to standard EPC implementation, the companies also use sensors to record temperature or humidity, for monitoring location of the product and its condition. These sensors work side by side to the RFID to identify the product that is being tracked. Therefore, in the particular case, RFID helps to provide a quick way to track pharmaceuticals, retrieve information, and ensure the authenticity of medication throughout the supply chain. In addition to reducing the operation cost and possible losses by providing instant inventory management, RFID can also be adopted to fulfil the health-care regulations in USA.

The USA Centres for Medicare and Medicaid Services faces medication errors every day and such errors are an added financial burden in the health-care system, which are reimbursed by the Centres for Medicare and Medicaid Services apart from those involving malpractice claims. In terms of financial perspective, malpractice claims must be reduced, as this would not be reimbursed. The use of RFID can help reduce the dispensing errors, as it can generate a list of consumed, expired, soon to expired medications and basic information like manufacturer, drug identification number and medication name only in a matter of seconds. Thus, other than providing an accurate data, speeding up the process and whittling down the error rate, it also helps to decrease malpractice claims by improving the safety and consumer's satisfaction to reduce losses.

Title II of Drug Quality and Security Act (DQSA) is a law in the United States, which outlines critical steps to build an inter-operable electronic system to provide the information of distribution history starting from the production till the date of sales, enabling the United States Food and Drug Admission (FDA) to have a better control in the pharmaceutical supply chain, enhancing their ability to improve detection and removal of dangerous products in the market. The function of RFID can fulfil this regulation as to record, track, and trace medication across the supply chain.

Counterfeit drugs are a growing threat in the United States. 40% of drugs and 80% of ingredient are imported from overseas where 30% of drugs in Asia, Africa and Latin America are confirmed counterfeit as estimated by The World Health Organization. Therefore, there is an urgent need for tracking of medications from the manufacturer to the end users in order to protect consumers from counterfeit drugs and reduce the possible revenue losses. The unique RFID tag, as one of the features of RFID, is unique for each item. Each item can be identified

on an individual basis and it is significantly harder to copy comparing to Barcode, so it helps a lot to reduce a counterfeit drug to travel all the way to its final destination.

Security Breaches

There is no question that RFID gives a great benefit to the pharmaceutical supply chain. However, it is vulnerable of being attacked like any other information system. The company categorizes security breaches using the "CIA[48] Principle", which are attacks on the three criteria, namely confidentiality, integrity and availability. For the size of the focal study company, this is a standard practice, simple but widely applicable security analysis. Attack of confidentiality means data has been disclosed to an unauthorized individual; Attack on integrity means the IT system or data has been destroyed or modified by an unauthorized entity; Attack on availability means either the system or data is not available when needed by a user. Each of the principles can lead to serious consequences. Therefore, an overview of CIA Principle allows an organization to determine quickly which threats are of importance to be countered and protected.

The company has an information system safety team to hack their own system, constantly evaluating the company's vulnerability in order to maintain in high-level security. After cases of spoofing, long-range reading, and rewriting information on the RFID tag, the information system safety team has identified the following as possible security breaches to the RFID system.

Viruses are one of the most common types of attacks against information systems. Even though most of the RFID passive tags have only a small memory capacity, virus is still a credible threat to RFID system, it has been reported that RFID tags can be used to transmit a computer virus as a medium.

For example, if an RFID tag that had been infected with a computer virus arrived in a distribution warehouse, the back-end servers in the warehouse could then be attacked by the SQL injection from that particular RFID virus which may reveal or destroy the data stored in the data base, threaten the security of the communication between the reader, tag and back-end database or even bring the entire RFID system down.

Consequently, it provides hackers plenty of opportunities to access the company's database and steal the data, which could include valuable or confidential information about the business

[48] CIA The Central Intelligence Agency of United States of America

like suppliers' contacts, costs or even disclosure of the info of patients or customers. If this information falls into the competitor's hand, corporate trade secrets can be exposed.

Spoofing is an attack on the communication between reader and tag. It occurs when a counterfeit tag impersonates as a valid tag and therefore gains its privileges. To masquerade a valid tag, attackers use some special emulating devices to spoof the RFID tags by reading and receiving the encrypted message or even sending out false information to the tag and reader.

Tag cloning is a kind of spoofing attacks where the attacker captures the date from a valid tag and creates a copy of the captured sample on a black tag. Therefore, it enables the attacker to read the tag's data from a cheap product, uploading the data into another tag that attached to a similar but expensive product. Therefore, if an attacker is an internal employee, who is familiar with the workflow in either the warehouse or the retail stores, he could purposely steal valuable drugs from the company. As a test of security, the information system safety team has stolen expensive kinds of medication such as Soliris and Elaprase, which could cost more than US$ 2000 for only a few millilitres.

As illustrated above, RFID data security is important. It may lead to a big loss or even a serious consequence. Hence, after identifying the threats by CIA principle, the company believes that it is critical to take certain protective measures to prevent those threads, and it may start from both technical and operational point of views.

When it comes to technical problem, it is always important to keep up with the latest technologies and trends. The more constant the company improve the security system technically, the earlier security vulnerabilities are identified, and solutions can be implemented earlier too.

One common way to ensure integrity for the attack from virus is to use anti-virus products. Virus attack has been demonstrated as the common attacks against information system, so there has already been some well-developed middle-ware to block anomalous bits from the tag, or to presents SQL injection detection tools to prevent the virus to infect the system thereby protecting the data from being destroyed or modified by an unauthorized entity.

Organization protects against attack on confidentiality like spoofing attack with encryption and access control. For example, users are required first to authenticate and then access is granted on their proven identity. A common way is to implement a data encryption and RFID authentication protocol that will increase the technology complexity and the cost needed for a successful attack.

After evaluating the solution for the technical issues, it is important to review from the operational point of view. The company reported in the focus group study that losses could be

caused through a variety of methods and by different reasons, it showed that internal staff pilferage is the largest contribute to loss for the company. Happened in Jan 2017, the pharmacy technician has just been caught stealing for more than US$ 12,000 in the prescription drugs at the place where she worked.

Employee theft could occur from simple merchandise theft by the staff, or collusion with external theft. The basic solution is to equip CCTV, motion sensors, or even an embedded security for security professionals to monitor retail outlets in 24 hours manner. These CCTVs are installed by security professionals to ensure no hiding spots for full coverage of theft events are recorded. In addition, a loss prevention program that focuses on operational control, including concepts of establishing procedures, policies and business practice to prevent the loss of inventory have been in place to help minimizing the risk of employees leaving work place with the stolen merchandise.

At management level, seminars and training sessions of change management have been frequently scheduled to share up to date information together with trading partners such as vendors, especially for global supply chain of pharmaceutical products where counterfeit products exists. The best company often manages change by educating suppliers and their staff about the benefits they will achieve, rather than just forcing them to follow instruction. Instruction manuals of how RFID is beneficial to the company is being explained, which educates supplier on how RFID implementation works in the company which may improve the effectiveness of the RFID system right from the start of the supply chain.

Focus Group Member UU3:

"For contractors we use, we have no idea of how our RFID tags being distributed are being tampered, and we have to use other systems to make sure they are used in the good hands."

– Focus group member

The case is for delivery truck that delivers pharmaceutical products to the warehouse of a pharmaceutical company, located inside a research lab. In the past, a security booth is used to validate every single truck going into the research lab. To improve this human operation, a second lane was opened beside the security booth, which has RFID readers to automatically read RFID tags of vehicles that are allowed to enter the research lab facility. The most notable benefit of the second lane is the vehicle waiting time to enter the research lab is being reduced, as vehicles are permitted to enter or exit the facility without human intervention. Instead of swiping an ID card or pushing passwords on keypads, one simply approaches the second lane and the automatic barring system would release the vehicle for entrance. RFID cards will be installed in vehicles, with a reading range of 5-7 meters. These cards will be fixed on vehicle

windshield, encoding the identity of these vehicles. In another word, The RFID cards are wireless vehicle license plates that will transfer the identity to the long-range reader just before the vehicle reaches the automatic barring system. In case an unauthorized vehicle has approached the automatic barring system, not only the bar will stay in its place, but also an audible alarm plus CCTV recording will lead to further security inspection performed by the security guards.

Security Breaches

A logistics company was given the RFID tag to enter the research lab facility. However, due to more flexible allocation of trucks, the logistics company cloned the RFID tag and therefore allowed it to easily enter the research lab for whichever truck it appointed. The cloning of the tag was not prohibited and there is no rules prohibiting the logistics company to do so.

As a result, the company adopted a more difficult to be cloned tag from another RFID hardware provider. Tags are changed from time to time and logistics companies or other parties are required to bring in the old tags to change for new ones. This method adopted the company's password changing protocol.

Knowing that it is possible to clone the tags, the company raised an issue that shall intruder wanted to access the research lab illegally as a trespasser. The intruder can clone a valid tag and access to the research laboratory illegally. As a precaution to this issue, an SMS is now being sent to the tag owner notifying that the vehicle has just passed through the security gate. This also serves as a vehicle security system of this research lab.

In addition, security manual were also being given to the tag owners to protect the tag while not driving the vehicle. For example, aluminium foil to wrap the tag while placed in the vehicle and security guard to keep vigilance and take note on suspicious persons entering the car park or vehicles entering the research lab have been documented in the standard operating procedure in the tag owners' manual security guard work handbook.

Finally, a solution that is proposed and will install in the automatic barring system is an imaging recognition system. The imaging recognition system automatically recognizes the vehicle that is approaching the security bar, and shall a different vehicle is found with the RFID tag, security guards were informed. Finally, in either successful or unsuccessful vehicle passing the bar, a photo will be taken and kept in the database.

Focus Group Member UU4:

"RFID systems do not provide enough security features. We added weight and CCTV system to record scanned item image when weight is different from scanned RFID tags in our POS"

– Focus group member

The focus group member UU4 is a jewellery retailer with a hired an unethical salesperson who is also the shopkeeper. Similar the other cases mentioned the focal company also uses RFID in jewellery tagging. A serial number tag is used and RFID scanners installed in the Point of Sale (POS) system would be able to display information regarding the piece of jewellery when it is being sold. Every night the shopkeeper has to report the jewellery sold to the company headquarters.

Security Breaches

The unethical staff was exchanging RFID tags of less expensive jewelleries to expensive items. With the knowledge of the operation and reporting by end of day, this exchanging of RFID tags would not work because a simple exchange the retail shop would be left with many mistagged jewelleries, which in turn would track down the unethical staff. The staff, while unethical, was smart to still be able to exchange the tags and purchase more expensive jewellery with a less expensive price. The staff first have a price of a rather expensive jewellery in mind, say A, and whenever a shopper ask for a similar line of product with a lower price, say B, the staff named the price of jewellery A instead. If the shopper believes that the jewellery price of A is too high for jewellery B and refuse to buy, the loss of sale would not be responsible by the staff but the storeowner. On the other hand, shall the jewellery B was being sold with the price of jewellery A, he would "purchase" the jewellery A with the price of jewellery B before the end of day where reports are sent, in cash, in order to avoid being traced. In theory, every single successful "purchase" will enable the staff to earn the amount of price A minus price B.

The act was caught, months after the staff left the company, when the printed receipts with the jewellery A purchase were brought back for cleaning and service with Jewellery B. The first time it was treated as simply an error, but after the third occurrence of similar mismatched invoices, investigation were started and found whenever a product mismatch invoice of jewellery A were caught, the mismatch invoice jewellery B will appear on the same date and a later time. However, the POS selling time difference could be up to 6 hours, and that it would be unreasonable to be justify the swap as a human error.

As a result, the POS was installed with a handheld RFID scanner before the incident, but now a stationed RFID scanner is attached. There is a specific tray for the reading zone, and a weight sensor is installed with the reading zone tray. All sales of jewellery now requires to be put on the tray for RFID scanning, and this is the only way for selling of products except the manager override for manual operation. The weight system automatically capture the weight of the jewellery being sold, and if there is any mismatch in weight information registered in the database, the POS will warn the storekeeper and the CCTV will send a still image to the

management. Apart for the need to weight every piece of jewellery and add such information to the database of the company, this solution is workable and since then there were no swapping of RFID tags unethically.

Focus Group Member UU5:

"RFID did not bring us any benefits as a medical practitioner. The RFID tag in injected needle and drug boxes caused us more problem than benefit it brings."

– Focus group member

Following the footsteps of various developed countries, Hong Kong announced on March 20, 2017 to run a waste levy system where user needs to pay waste management fees[49]. The master plan targets reduce waste by 40% in the year 2022.

The focal company is located in Hong Kong and has a waste management system run by the building, where different kinds of waste were charged differently for waste handling fees. In addition, medical wastes in Hong Kong, such as needle injections, are treated as toxic waste and special companies were employed to handle all these wastes with special fees, which is required by Hong Kong Law (Cap. 354) Waste Disposal Ordinance and Code of Practice for the Management of Clinical Waste[50].

The focal company wishes to avoid such fees and treat carton boxes of medical drugs as combustible waste instead of recycle materials, and boxes of needles, while not required by government to handle as toxic waste, to also be treated as combustible waste. The company is located in Central of Hong Kong, where tenants of lots of buildings were entirely medical clinics. The waste management team of the building started to use different colour bags for different wastes, with serial numbers on the waste strip wrap to indicate which tenant does the particular waste bag belongs to. RFID scanners were attached to a weigh system to calculate the weight of waste while the different kinds were processed by colour in sequence to indicate their waste properties.

Security Breaches

---

[49] Hong Kong Government News. 2017. *Waste Charging Details Announced*. [ONLINE] Available at: http://www.news.gov.hk/en/categories/environment/html/2017/03/20170320_152421.shtml. [Accessed 5 April 2018].

[50] Environmental Protection Department. 2018. *Code of Practice for the Management of Clinical Waste*. [ONLINE] Available at: http://www.epd.gov.hk/epd/clinicalwaste/file/doc06_en.pdf. [Accessed 4 April 2018].

The RFID scanner has picked up RFIDs from the medical carton boxes and needle boxes in the combustible waste sequence for this particular focal company. Initially was record error or RFID jam problem but later discovered the focal company treated recyclable waste as combustible waste, and was accused incorrectly for placing injected needles inside needle box in combustible waste instead of toxic waste. Although later it was found that the company did not violate any laws as the injected needle was not inside the needle box with needle manufacturer RFID, and there is no law in Hong Kong to prohibit treating recyclable waste as combustible waste. However, this is certainly a case of security breach in eavesdropping or even product information spying from waste in the uncontrollable area.

The solution was to place the right pieces of waste into the correct waste handling method. Needles to be put in needle box is also suggested as it fits the injected needle and although not required but it's a better way to protect the injected needle as virus might spread if contacted by human or animal. The company also set up a policy to cut the antenna part of the used RFID boxes before putting into waste system but this way to deactivate the tag is not proper. Other more proper way to deactivate the tag needs investment and was not economical friendly; nevertheless, a policy to destroy the tag is being implemented to protect privacy.

Focus Group Member UU6:

"By using RFID, exchanging RFID tagged Jewellery leads to exchanging prices and properties to them. The automation is good only if nobody intends to temper your RFID tags."

– Focus group member

The case focal company is same as the last case, and it is about unethical usage. An unethical staff member has relevant RFID knowledge, tried to change the tag information of RFID in order to lower value the jewellery price.

Security Breaches

The company used a re-writable RFID tag, and staffs are required to participate in writing information to the tag while attaching tags to jewellery products. The unethical staff member has a changed the RFID tag information in the evening after the store closes in CCTV blind spot of the shop. The accomplice purposely comes to the shop next day morning while the staff member is not in the shop, but instead a rather junior staff were taking care of the sales, tries to buy the piece of jewellery with a piece of RFID tag that is tagged with the wrong tag information. The selling was caught only after the sales have been completed, and it was found out as several similar incidents happened and the staff member were selling the jewellery in a second hand market.

As a result, cryptography measures are currently being used in the RFID tag to prohibit reading of the tag. Read Only tags were used in order to prohibit tag information to be modified to be swapped to tag jewellery. Every piece of jewellery now has a unique ID and once tagged jewellery is being sold the database would alert if the same number is scanned again. Finally this still possess a problem shall RFID hand held is being used in offline mode during shows and exhibitions, however, as the previous case suggests real time database update in transaction processing system should be required for full protection of theft.

Focus Group Member UU7:

"Cloning an RFID is easier than cloning our drug bottle, so tagging an RFID did not stop our drugs being counterfeited, and we still have to use an online server to record usage in order to protect our drugs being counterfeited."

– Focus group member

The case study focal company is a drug company that uses a special bottle to hold their liquid drug. Since the drug is an expensive drug, counterfeit products have always been a problem the drug company faced. In the past the company has tried to use laser label, then finally replaced by RFID since RFID are more difficult to counterfeit compared to laser labels. The company has put an RFID under the bottle cap in order to discourage counterfeit products.

Security Breaches

Security breaches happened when the sequence number of RFID are read by uncontrolled domains, For example, importers, packing supplier, distributor, hospital, and clinic, by RFID hand held scanner, drug counterfeit companies can also read this information off from the bottles and clone the RFID. The company then tried to use a technology that keeps the RFID inside the bottle layer, which is more difficult for the counterfeit company to manufacturer the bottle. This method worked for a while but finally the counterfeit company start to use genuine bottles to put counterfeit drugs. Indeed, the liquid is easy to counterfeit compared to a physical drug, the special bottle is difficult to counterfeit, and therefore, drug counterfeiting companies use used bottles to hold other edible liquid to counterfeit a drug.

The solution the company has used is an online server. Once an RFID label is being used, and read by the RFID handheld reader, the drug company requires the pharmaceutical practitioner, be it a hospital or medical clinic, to register the use of this RFID number. The solution works

since the end users will not use this particular drug. However, in cases of uncontrolled users also use this drug then this could create potential issues. At present, this problem is not tackled as even if the user has got a bottle it would be small in quantity making these used bottles difficult to be reused in a large scale unlike clinics and hospitals.

Focus Group Member UU8:

"RFID helped us in emergency anesthesia and narcotis medication control, if used with the right operation procedures."

– Focus group member

The focus group member is a hospital pharmacy with anesthesia and emergency medicine package such as narcotis. The company used a smart tray for drug supplement and distribution with advanced RFID technology to automate pharmaceutical kits and tray replenishments. The system can store and sort more than 150 items in a matter of seconds to provide detailed information about missing content, what has expired, and upcoming drug kits, pallets, solutions and packaging bags.

Furthermore, the system can perform automatic monitoring of the refrigerator and temperature control cabinet. An RFID-enabled controlled temperature cabinet with the ability to auto count whenever the cabinet door is closed and report number of RFID in the cabinet to a computer database. The pharmacy manager can quickly identify expired or recalled drugs by reading inventory updates remotely from cabinet and being notified of product shortage in order to avoid out of stock.

Safe operating room that stores and use of anesthesia drugs and narcotics is the heart of the system. The hospital used patented and proprietary RFID technology to automatically collect operational drug inventory data at the point of care without manual counting, paper recording, or item-level scanning. Providing secure access, uninterrupted real-time visibility and reliable usage metrics are critical to charge trapping verification. The use of narcotis drug is prohibited and is for persons who use drugs, the lower dosage assigned by medical physicist is for eventually rehabilitation of drug users back to normal. As narcotis itself is a drug, in the past, some drug users pretended to be narcotis patients to retrieve narcotis for their own use. In a hospital environment it was difficult for every medical practitioner to know every single patient, or check ID at every single stage. Indeed to some extent, it is difficult for a medical practitioner to confirm the person presented the ID is the person himself. The use of RFID prohibited the misidentification, once a patient has been assigned for narcotis an RFID wristband will be attached to the patient, and then in the operating room the patient's wristband

and the narcotis on the automated tray will both be scanned simultaneously, ensuring the patient's identity.

Security Breaches

RFID security breach reported was the wristband was detached and reapplied to another person who wanted the narcotis. Both persons – the donor of narcotis and the receiver – visit the hospital at the same time, and the after the donor received medical checkups and being assigned narcotis, the donor passes the RFID wristband to the receiver. The receiver then queues up for narcotis usage in the operating room. With the RFID checks the wristband and the matching automated tray, the narcotis are released to the receiver.

The solution for this is a policy being released that the RFID wristband must be attached by a hospital worker and then this wristband will be cut open by the hospital work on disposal, after the nacrotis have been consumed. In the middle of the process, say the donor would like to transfer the wristband to the receiver, the wristband was made by elastic plastic such that after removed it cannot be attached again, and the operating room are not allowed to release nacrotis to any person bringing in detached wristbands. Finally, the problem of RFID has been solved, further breaches but not to the RFID system was further reported. Donors have tried to take nacrotis out of the operating room, with either inside the donor's mouth or with other ways, however the number of incidents are minimal and also another policy of the narcotis for patients had to be consumed immediately have further solved this problem.

Focus Group Member OE1:

"We minimize information that are written to RFID in order to prevent information theft for counterfeiting drugs"

– Focus group member

The case study focal company OE1 is the same as case HE5, with another security breach in another focus group.

Security Breaches

A second security breach is the counterfeiting problem of this valuable drug. Counterfeiting was not a problem for the case study focal company before the company supplied the drug worldwide, and overseas drug manufacturers wants to penetrate in the Turkish market. Locally in Turkey at the time of the focus group discussion, the case study focal company was the only supplier of this kind of cancer treatment medicines in the Turkish market. After overseas drug

manufacturers entered the Turkish market, counterfeited drugs were reported to go through RFID scanner verification without problem. The drugs were equipped with RFIDs information gained from eavesdropping RFIDs on genuine drugs in overseas genuine operating environment. Since these drugs were not supposed to be sold in Turkey, there will be no duplication of RFIDs being scanned.

Current solution to this problem is to use encrypted RFID tag with minimal information. Not all details are written to the tag and indeed for the drug intake timing purpose, using an ID tag with check digits is all it requires.

Focus Group Member OE2:

"We were forced to use unorganized number to avoid long range reading our product information from competitors in public"

– Focus group member

The focus group member OE2 is a jewellery manufacturing and retailing company and uses RFID to transfer information such as tracking and tracing to inventory control software.

The company felt the need for robust tracking in the supply chain at any time and visibility solutions is the backbone of their business success. The case study target one of the biggest jewellery companies in Hong Kong and the RFID project also involves other companies in their jewellery supply chain. The case company is using the RFID Technology in their 1470 shops around the world, including exhibitions, private shows and warehouses in Hong Kong, mainland China, USA and Australia.

The use of the RFID technology helps the company to locate high value goods more quickly and improve inventory control, increase security levels in order to prevent counterfeiting during sale, loss and thievery. It also promises to enable new efficiencies in the supply chain by tracking goods end to end, monitoring the demand of specific items online anytime and anywhere, which may lead to a possible increase of revenue and support customers' sales process.

In the jewellery industry where each shop often include a big amount of high value items, inventory management can be a challenge, therefore, RFID application is commonly being used for the purpose of efficient inventory control through jewellery management system. Jewellery management system help to manage the tracking, distribution, sales and flow of the

jewellery items with an RFID tag from production across distribution to retail till the point of sale.

Every item in the Jewellery store is tagged with an RFID loop tag that provide the data to be read from hundreds or thousands of items in few estimated seconds. The RFID tag being used include a unique electronic chip that represent a unique identity number to capture the full details of the specific item by RFID Scanner that transfer the data back to the jewellery management system. The system enables sales to inventory the stocks of jewellery items in few estimated seconds by reducing the time of counting the items one by one.

Apart from the reduction of inventory time consumption, the RFID tags and the jewellery management system cuts inventory costs for the retailer and guards against theft by a special RFID tag with a limit of radio waves transaction, which activate the alarm once the item is away from the RFID reader.

The case study company applies the RFID Technology by using a computer management system installed in a computer, with RFID desktop and handheld readers. Every single pieces of jewellery are tagged with RFID tags with a unique number. The system is flexible to install in any display box even in exhibitions for temporary use, which reduces chance of theft and fraud while enhancing security.

Security Breaches

Security Breaches are critical issue that must be taken and considered seriously in order to ensure the security of valuable information especially when the focal company is a listed company. Security breaches identified are physical removal of tag by potential buyer when inspecting the jewellery item and the prevention of it is to use security sensors on the RFID tag, which turn on an Alarm that notifies about the removal immediately when the tag is out of a high proximity area. More simple solution is to use a strong bond or glue that would prevent the removal of the tag and to guide the staff to be aware of the issue and check the RFID tag on the item once the item is back to staff hands.

The case study company is also one of the top three companies in Mainland China selling jewelleries. Most shopping malls have all three branded shops exist and business competitors have been using long-range RFID reader with high gain antenna to read the tags and collect the supply chain information for business purposes. This commercial spying is addressed as the most common security concern among the use of RFID in this jewellery company. Information of in stock and out of stock items with sales history hacking helped the competitors understand the profit model of the case study company, and areas of competition.

The current solution is to keep the tag with a simple run number and all number should have no organization or any linkage to jewellery property. Previously the number on tag has representative digits on the diamond grading property on colour, cart, clarity, and gold purity information but then it was omitted.

Focus Group Member OE3:

"We use Shared Key Authentication to protect our RFID systems"

– Focus group member

Focus Group Member OE3 is a system integrator and has developed a new and comprehensive security system for use of RFID in the supply chain including pharmaceutical companies. RFID system security is highly regarded as a main security feature of the software, as the RFID tags can be eavesdropped at any point of the supply chain.

Security Breaches

Security breaches were documented by including RFID devices that can record the existence of RFID readers. The company calls these devices anti-RFID eavesdropper, and they were placed in the pharmaceutical goods to record eavesdropping cases, which most incidents are reported to happen in the associated domain during logistics transportation.

As a result, solution applied based on Shared key which included authentication, data encryption, and middle-ware based security policy were in place. The major problem this solution was to shield against unauthorized reading, eavesdropping, replay, and deceive of RFID signals.

The operation steps of Multi-authentication protocol based on the Shared key is followed:

Step1: Read and write device generate a random number R, and R will be stored in read/write device. Then send the label certification request (Query) and R to tag.

Step2: After tag receives the R, it generates a pseudo-random number NT and stores it. By operating, generates a cipher text S and sent it back to read/write device

Step3: After read/write device receives NT, S and R, it calculates G and sent them all to middle-ware.

Step4: Middle-ware sent the data to database

Step5: Database calculates IDT by using Hash operation and check the ID with IDT. If they are the same, it can pass the protocol.

After the tag and middle-ware check with each other, they can transmits data.

In order to ensure the safety of data during transiting, encryption of data in the RFID system is needed. When the tag sends data, it first sends shared key K to its own key generator, and generate a stream cipher sequence, then use stream cipher sequence information encrypted it and sends it to read and write device. After read and write device receives the data, it will also first send shared key K to its own key generator, generate sequences to decrypt stream cipher, and get the original information. Therefore, even if the communication channel between tags and to read/write is intercepted, the interceptor does not have the key sequence. In addition, whenever any read/write device transmits data to/from the labels, encryption and decryption shall be taken place in order to retrieve the original information.

Focus Group Member OE4:

"Eavesdropping are everywhere if you work with celebrities, luckily hardware solutions helped us to shield from such breaches."

– Focus group member

The focal company is a dermatology clinic in Hong Kong with its own brand dermatology product. Majority of clients being celebrities and an injection of Switzerland made needle could cost up to US$ 10,000.00. This company considers security, privacy, and authenticate drugs are top priority in the supply chain. All clients of this company are coded by customer number and even under inquiry they response only to codes. Sales of the company's drug are kept in top secret, and their need to secure and authenticate pharmaceutical products has been increasing along with the emerging counterfeit product market. The motivation to introduce counterfeit pharmaceutical products in the supply chain could be to gain rapid economic benefits or affecting the reputation of this dermatology clinic.

RFID is mainly used in this supply chain to deter counterfeiting attempts, and it is used in other domains. For example, efficient expiry date management, pharmaceutical tamper detection, and fraud detection and prevention. As RFID has the capability of capturing and relaying data,

which is what the industry is looking towards to improve quality, reduce costs, and most importantly improve patient safety.

The RFID lifecycle includes three main parts of chain operations in this supply chain

1. Manufacturing's plant

2. Manufacturing's distribution centre

3. The dermatology clinic

At a manufacturing plant, the tag is embedded with product description, lot number, batch number, and the expiration date. At the exit gate, the reader scans the tags to captures the product information, and records when and where the data capture took place. It sends the recorded date to a middleware and then to an application via PDA, laptop, or a desktop computer. Next, the plant ships the product to a manufacturer's distribution centre. When the product arrives, a reader records the date time and receiving location, at the manufacturer or distribution centre's entrance gate. When a notification of a purchase order from a wholesale distributor is received, the product is prepared for outbound shipment. A reader at the exit gate captures the date time and shipping location.

During the above supply chain process, all the product information is collected automatically and directly saved in the tags through RFID system. Even products are in motion, mobile devices can read condition and location-based information, feeding the cloud in real-time through the logistics process. This enables visibility, as well as making midcourse corrections to save products at risk, protecting the patient and the brand. In addition, it helps to achieve the goal of anti-counterfeit, quality improvement and cost saving, and makes the whole process more efficient.

In the final stage, when the dermatology clinic uses a drug or needle injection to the client, the clinic nurse uses handheld RFID scanner to make sure the correct drug is used with the correct client, with the correct dosage, and in the correct order.

Security Breaches

A security breach in RFID applications would leak valuable information about physical objects to unauthorized parties. Specially in this dermatology clinic where the clients are celebrities, a security breach is reported that newspaper reporters attacks the dermatology clinic RFID system by eavesdropping, and hacking into RFID computer handheld and server systems.

Hacker is always the main problem of uncontrolled parties leading to security breaches. Hackers can easily eavesdrop on the conversation between the tag and the electronic RFID

readers because of its principle of broadcasting information, and then manage to gain access to or tamper with information. In this dermatology clinic, this would mean information could lead to a report of a certain celebrities are using certain dermatology products which is an invasion of privacy with good profits.

The solution of the case would be to use sleeping and zombie tags. The sleeping mechanism is another type of physical solutions. This approach is performed by sending a "sleep" command including a password to the tag by the reader to make it temporarily inactive. This is almost same as the killing tag method which only difference is the sleeping tag can wake up and be activated as soon as it receives the command from the reader. Meanwhile, the tag can never be re-activated in the killing tag method. The sleeping tag approach offers an advantage to the user to switch the state of the tag between active and inactive. The problem of using this method is the existence of the possibility that the password used for controlling the tags might be overheard by an eavesdropping attack. Zombie tags, on the other tags are additional tags that are attached to a product for scanning purpose. For example, product serial numbers represent various dermatology drugs when scanned by RFID scanners since the scanner software query database for the dermatology drug information, by putting additional tags on the product, without relative information in the database, would return no data. Since more RFIDs can be scanned within a second, the zombie tags have no meaning and will be able to divert the hacker's attention from the real RFID tag that represent the particular drug. These zombie tags are attached to the drugs in manufacturing stage, and this is possible only because this dermatology clinic has their own brand, manufacturing, and logistics facilities.

Focus Group Member OE5:

"We use shielded drawers to safeguard our jewellery from competitors' eavesdropping."

– Focus group member

The case study focal company is a small jewellery retail kiosk that sells jewellery with different karatage of gold. Karat is the term used to measure the gold content or purity of the gold, the highest karatage is 24k gold, or called the pure gold, and there exists other lower karatages. The lower the number, the less pure the gold is. A piece of gold can be divided into 24 parts, shall a gold with no traces of any other metals, it is known as 999 gold for 99.9% or 9999 gold for 99.99%. 22K gold, on the other hand, had two parts of other metals put into the gold; it could be silver, zinc, nickel and other alloys. One can say that there are only 91.67 per cent is pure gold. A dull colour gold that has only 75% of gold with 25% of other metals like copper and silver is called 18K gold.

Such karatage is written inside the RFID tagged with jewellery on a label. The RFID information is used only when goods are received and in the stock taking process. Shall the piece of jewellery is being sold; this RFID label is immediately removed from the jewellery and kept in the jewellery retail kiosk drawer. This RFID is being read daily to crosscheck the sales of the day. The different karatage of gold being sold is the main determining factor of the jewellery sold in this kiosk, and the goods were consignment goods, which means the payment to vendor only take place after the jewellery is being sold, as confirmed by returning the RFID tag. Shall there is no sales, the jewellery kiosk can return the jewellery without paying the vendor.

Security Breaches

Security breach occurs for this information being leaked to unauthorized parties, say competitors for corporate espionage. In the same shopping mall there are few jewellery shops and this information is useful for them to market their products in relation to what is being sold in this small jewellery kiosk. This RFID information was read by long-range RFID readers eavesdropping.

Currently the solution for blocking such eavesdropping by installing metal drawers to protect the RFID tags. For products that are inside the kiosk for selling, they are protected by locked glass display cabinets, which are covered by cloths with aluminium foils when the kiosk closes. For daytime, it takes the storekeeper a vigilant eye to investigate suspicious persons with portable RFID readers. The owner of the shop recommended the jewellery vendor to include RSA blocker tag, which can be used to protect communication between tags and readers since RSA blocker tags responds positively to all unauthorized request from eavesdropping scanners thus blocks readers to read RFID tags nearby. However, this request was not granted from the jewellery vendor.

Focus Group Member OE6:

"As a sustainable express company, reusable RFID tags are mailed back to us from consignee with our pre-paid postage service, however, god knows what the RFID has gone through."

– Focus group member

The focus group member OE6 is one of the largest courier companies in the world. The company has an RFID application for enhancing pharmaceutical SCM. Pharmaceutical industry requires supply chain to deliver their life saving product to the correct place at the requested time in the right condition. Patient safety is the main goal in the supply chain of pharmaceutical products, and temperature monitoring plays a key role to guarantee product integrity. Avoiding temperature excursions during storage and transportation is essential to

guarantee product integrity, and visibility and transparency of supply chain are needed to meet the increasing demand from pharmaceutical regulators. Therefore temperature monitoring is one of the important parts of the pharmaceutical supply chain.

The focal company is a world leading courier company with service cover in more than 220 countries and territories worldwide. The RFID application the company uses for pharmaceutical supply chain, namely The Smart Sensor, can be used in air, sea, and land transport modes without restrictions. It is a semi-passive device based on UHF RFID technology, consisting of an EPC Gen 2 semi-passive UHF RFID inlay integrated with a battery-powered temperature logger, manufactured by the company CAEN RFID. The sensor continually captures temperature data at a predetermined time frequency, defaulted 15 minutes, and stores it until the tag is interrogated. As RFID has the ability to communicate without line of sight, temperature information can be read out any time, with handheld or stationed RFID reader without the opening the product package. For customers opt for the this service, the company applies the Smart Sensor to carton box level of the shipment, it could be mounted on the exterior of the box inside a courier pouch, or the shipper can request that the carton box to be opened and the sensor be placed inside for extra security. The Smart Sensor has a size of approximately twice the height and width of a credit card, and with a thickness similar to a standard credit card.

The Smart Sensor is linked to the company’s online platform, as well as to shipping details, including that product's destination address, waybill (a transportation bill) number, temperature requirements, and the product name. The Smart Sensor tag is read at least at four points: upon arrival at the first origin station, when the item leaves that station to be tendered to an airline, when it is received at the destination station located nearest the intended recipient, and when it is shipped from that site to the delivery address.

At each of these Smart Sensor reading stations, a tag's ID number and temperature recordings are captured and then forwarded via a wireless connection to the online platform database, where the data is analysed and stored. There is a software system that reads data off the online platform database and if it determines that the temperature readings have deviated from acceptable levels, it issues an alert to a Global Proactive Monitoring & Intervention Centre, which can work with the appropriate local Certified Life Sciences Station to forward a message to the shipping customer, as well as dispatch a staff member to address the problem.

If there are no deviations the data is simply stored in the 24/7 online platform in the cloud based computer system, securely stored up to 10 years in a data warehouse located in Prague, Czech Republic. At any time inspecting agencies and authorized drug users or medical practitioners can check the condition of the products at any time. Options to download reports of

temperature captured during transportation are also available, in various formats such as portable document format (.pdf) and excel spreadsheets (.xls/.xlsx).

At the last step of the operation, the consignee of the medical goods can use a mailing company, which is a sister company to the focal company, to send a postage pre-paid mail that includes the sensors to the company. The consignee can simply drop the envelope with the sensor inside at the nearest local post office drop box from the end-user location at destination back to the focal office in Germany. The focal company will erase the data inside the sensor and reuse the sensor, at present, the sensor is re-assigned to the same shipper who shipped the medical goods.

Security Breaches

The focal company reported security breaches happened when the Smart Sensor is sent back by consignee with the postage pre-paid envelopes. The reverse logistics process aimed to maximize the usage of the sensor to reduce cost and being environmental friendly. However, since the reverse logistics is not handled by the focal company but just by the local postal service, cases of loss of tag and eavesdropping were reported. As data inside the tag contains sensitive information, such as waybill number, which from the focal company web tracking system delivery time can be displayed, essentially some sensitive information were disclosed to intruders.

The solution is a re-design of postage pre-paid envelopes with RFID signal blocking materials has been implemented. With thin sheets of metal the envelope is shielded for protection from eavesdropping. However, this does not protect theft, which the issue of theft has reflected the case to the local mailing to handle.

Another security beaches was missing scan the sensor during the operation. A typical reason of missed scan is because of peak time sorting and staffs do not scan as required in their standard operating procedures. The solution of this is to apply long-range RFID readers instead of the use of handheld at certain checkpoint locations. This solution works well in most cases and apart from being a costly solution this has been installed in some courier checkpoints.

The combination of the state-of-the art RFID technology with temperature logger, with and the reverse logistics process resulted in a temperature monitoring solution that is on a cost scale up to 85% lower than other market leader solutions. Currently this temperature monitoring service, including the RFID loggers & reverse logistics process, is offered based on an innovative pricing model and calculated per shipment monitored but not price per device, allowing an extremely competitive price per shipment monitored. Key benefits of the solution includes patients safety by monitoring the temperature of the products across the pharmaceutical supply chain, manufacturers guarantee the product integrity and patient’s safety. Increase of customer

service is also achieved as pro-active notification if any incidence and activate agreed contingency plans to recover the shipment. It was also reported cost savings of 85% as compared to temperature monitoring offered by alternative solutions from the procurement management, data management and archiving savings, and environmentally friendly in the re-use of RFID loggers.

Intangible benefits also include the compliance of host of country-specific trade regulations, peace of mind of pharmaceutical manufacturers to have outsourced temperature management with a trusted logistics party while protecting product data integrity is required by legislative departments of some countries.

Focus Group Member OE7:

"Proprietary software key required to read any data from our RFID tags."

– Focus group member

The focus group member OE7 manufactures pharmaceutical sample cases and these cases carry toxic or medical samples where information must be correct and cannot be eavesdropped.

Security Breaches

A sample of virus or biochemical weapons can be utilized by terrorist for attacks and the financial and non-financial impact of this threat cannot be underestimated, and therefore, a state-of-the-art system avoiding eavesdropping must be used. The company refuses to report past security breaches count but admitted there were incidents of security breaches of eavesdropping happened in the associated domain during logistics transportation of "a highly infectious virus"

The solution is to use a tag that responses to the interrogating request only when the reader sends a right key. The information of the tag is also encrypted and can be read by authorized readers with the correct key.

Quick response is a big concern in this particular supply chain and the code system should not reduce the speed of supply chain. As the supply chain is operated by different parties, all the participants should have the right key and able to capture the information of the tag with authorization. Keys can be cracked by brute-force attack, even this method is considered has low effectiveness. From the development of supercomputers and other techniques, the keys are strong enough which contains 128 to 256 bits or 16 to 32 letters of Arabic numerals. The capacity of the RFID tags should be big enough to store the key and the product information.

A 512-bit UHF anti-metal tag was used, cost more than US1 dollar for each. The cost was reduced by having implemented the RFID tag recyclable in both pallet and container level instead of unit level. Customers do not receive such RFID tag with the product and therefore there is no consumable cost in this case.

Symmetric Key Algorithm (SKA) uses the cryptographic keys for both encryption and decryption of ciphered text. In this case, the reader and the tag both contain the same pre-set keys. When the tag receives a piece of data carried by the electromagnetic wave, the tags will decryption the data with the key. If the message is correct, the tag will send back the encrypted information to the reader. At last, the reader decrypts the information and read it. Since the key is strong enough, even the hacker captures the ciphered text; they are not able to understand what the exact message is.

Public Key Infrastructure (PKI) contains two different keys, which are the public key and private key. In the RFID system, the reader holds the public key and each tag holds a unique private key. After the message encrypted with the public key, the reader will broadcast the ciphered text. When the tag receives the ciphered text, the text will be decrypted by the private key. If the text can be read, the reader will be considered as an authorized reader, and the tag will sends back the product information.

Focus Group Member HA1:

"Software is the key of technology and our RFID products have security policy based on the RFID middleware programming."

– Focus group member

The focal company is a logistics company in United States where department of transport has laid down laws of drivers to drive a maximum of 10 hours after 8 consecutive hours off duty. In a normal day operation of distances of delivery is more than 10 hours of drive, the truck drivers were instructed to drive the entire truck to racks of trains and take rest in the logistics hub called relay terminals. The truck would then move by the train without the truck driver inside the truck, in order to save truck driving labour cost and to comply with department of transport law.

Security Breaches

The security breach exist when a hacker helped to change the serial number of the RFID reader ID of one trucker to another in order to have the trucker to work for the other trucker. While the

purpose of such breach is not in the scope of this study, the solution of such breach has to be kept confidential with only the principles reported.

Each reader unit has its unique reading and writing ID number. These privileges of these ID numbers, including usage, scope of accessing are all stored in a database, like a user management system. So when reader device needs to access middleware and in need of being identified legitimacy, it can be compared with access privilege data stored in the database.

In addition, the operator should also have identity authentication. It is necessary to register the ID of operator in logistics information system and the accessible reader ID for this particular operator. For example, every warehouse number and readers they can operate should be recorded in database.

For upper layers software of RFID applications, some middleware processing tag has secret information and privacy, so if someone wants to read these data, they must pass through certain authorization mechanism. So this upper layer software functionality is limited by the same set of user access rights to the data, which are achieved by this middleware.

This middleware does not only benefit security but also costs issue as it enables only basic data of items to be stored inside the RFID tag. Considering practical applications in the modern logistics systems, the label and the capacity of the read/write device, can be minimal in order to save costs.

Focus Group Member HA2:

"Our software has high standards of security, robustness, and high level of customer satisfaction due to our strict programming policies following the System Development Life Cycle Approach."

– Focus group member

An RFID system has been programmed by a software company. The software company provides software for the freight forwarders, a type of third party logistics companies that focuses in freight transportation. This software includes data from the purchase order from the buyer in a general trade, and from the data series of freight documents such as bills of lading are generated.

The purchase order information generally consists of the buying price of products and the quantity purchased. These are sensitive information as the seller's competitors can use this information to give more attractive quotations to the buyers.

Security Breaches

Professional hackers were reported performing back-end attacks for stealing such purchase order information. Stealing information from a freight forwarder has a higher return as multiple buyers' purchase orders are compromised while individually attacking buyer's system could steal only one single buyer's purchase order.

As a solution, the software company had carefully followed System Development Life Cycle (SDLC) in their software programming efforts, and the following RFID enabled security features have been in consideration since the beginning of the SDLC.

In the five stages of the SDLC, namely System Requirements, System Design, Data Encryption, Testing and Maintenance, extra effort were made compared to general software programming in order to provide additional security features for tackling RFID security threats.

In the system requirements stage, the software company has been aware of the following possible hacker attacks:

(1) Eavesdropping: Hacker intercepts data with any complaint reader for the correct tag family and frequency while a tag is being read by an unauthorized RFID reader.

(2) Man-in-the-middle (MIM) attack: Hacker interrupts the communication path and manipulates the information back and forth between RFID components.

(3) Denial of Service (DoS): Hacker use devices that actively broadcasts radio signals to block and disrupt the operation of any nearby RFID readers or make back-end machine or network resource unavailable to its intended users.

(4) Spoofing: Hacker captures the data from a valid tag, clone the data, and then creates a copy of the captured sample with a blank tag.

(5) Replay: Hacker intercepts the communication between a reader and a tag to capture a valid RFID signal. Later, this recorded signal is re-entered into the system when the hacker receives a query from the reader.

Therefore, in the system design stage, extra steps were placed in the design documents to deal with the hacker attacks listed above. These extra steps include RFID tag authentication, design transfer protocol, and data encryption.

The first step is tag authentication. Passive tags are weak in tamper resistance due to its limited hardware resources. However, passive RFID tags are the most widely adopted in supply chain industries due to its low cost. In order to strengthen the RFID system's resistance to hacking, it

is inevitable to improve the tag in hardware level. In this solution, the software company has adopted both Physically Unclonable Functions (PUF) circuit and Linear Feedback Shift Registers (LFSR) circuit. The solution includes implantation of the two circuits into each passive tag to ensure only the authenticated tags and readers can successfully communicate with each other.

Kulseng[51] described that PUF is a delay circuit and each circuit has its unique delay properties. Therefore, each tag's PUF will produce different output even they receive the same input. This uniqueness helps to verify the identity of tags. LFSR consists of shift registers and three XOR gates. The shift registers produce a long sequence of pseudo-random values, which will be masked by truly random values generated from XOR fates. The random values outputted by the LFSR are used to obscure the transmission between the tag and the reader. This physical design prevents spoofing attack, as hacker cannot imitate exactly the same output from PUF.

The second step is design transfer protocols. Mutual authentication protocol developed by Kulseng is adopted in the software solution. In brief, the tag sends its IDs, which will be updated in each read cycles rather than its identifier (ID) to a reader before authenticating the reader. Then, the reader will receive a unique greeting number (Gn) outputted from the PUF in the tag to authenticate the tag.

The mutual authentication protocols effectively resist to eavesdropping attack. In addition, the DoS attack by message blocking cannot affect the communication between readers and tags. Kulseng's protocol emphasized, "nothing adverse will happen if message 1, 2 or 3 is blocked or dropped". When message 4 is blocked, reader and tag can use the updated IDs sent from tag and the old Gn sent from reader to mutually authenticate messages from each other.

Thorough study has been done by Kulseng's study. However, the protocol is still vulnerable, as it does not provide resistance to MIM attack as required in the requirement stage. Under Kulseng's model, the protocol can still be tempered if the Reader sends the message 3 (ID+Gn) to hacker's device. This can happen if the hacker recorded the IDs being sent from a tag to reader and replay the IDs before the IDs changes. A third solution has been used by this software house, which is the data encryption.

The software house used data encryption to encrypt all the IDs in message 3. By doing so, the system's ability to defence replay attack is also tackled, as the intruder has no information about the IDs. In addition, an RFID reader which can store a number of hash keys for

---

[51] Kulseng, L., Yu, Z., Wei, Y., & Guan, Y. (2010, March). Lightweight mutual authentication and ownership transfer for RFID systems. In *INFOCOM, 2010 Proceedings IEEE* (pp. 1-5). IEEE.

encrypting tag ID and has the ability to rewrite the tag ID on the items that are decided to be installed in the supply chain facilities like warehouses, distribution centres and trucks. This action progressively improves data security by dynamically changing the data encryption but keeping the tag ID static.

The third stage of the SDLC, system implementation, is the stage concerns the development and integration of system. A twelve-step operation flow has been highlighted by the system architect of the software company:

1. Collect source data: Collecting data being stored into RFID Tag and relevant data, for example, the product information, EPC or ID assigned to items.

2. Database preparation: Design database schema based on the requirement of designated protocols. This has to fit the program and algorithm that will be designed in step 6.

3. Software evaluation and selection: Evaluate and select suitable software (middle-ware, programming tools, encryption software) based on the design of system.

4. Software purchase: Purchase the selected software.

5. Software installation: Installing the purchased software.

6. Program & algorithm development: Develop program and algorithm to generate data (e.g. IDs) required for protocol.

7. Software/ Program for generate data: Generate data required for protocol by program & algorithm developed in step 6.

8. Data encryption: Encrypting tag ID and tag information, which will be inputted to tags.

9. Hardware evaluation and selection: Evaluate and select suitable hardware (PUF, LFSR, readers and tags) based on the design of system.

10. Hardware purchase: Purchase the selected hardware.

11. Hardware installation Tag: PUF and LFSR implantation, set up of readers.

12. Loading data: Load the required data into tags and readers.

In the testing stage, system test and User Acceptance Tests (UAT) are conducted. The system test are conducted after the integrating all system components into a system. It aims to verify the proper functioning of the system. UAT is a black box penetration test is done, in the case of the software company, with no knowledge about the protocol used and RFID systems. This

software company hired a security expert who has hacking experience as the black box tester to simulate hacking into the system, with little or no information about both the RFID and software system is provided to the tester. It aims to test the system vulnerability without insider knowledge.

The final stage in the SDLC is maintenance, where in the case of software house regularly system check and updating are planned. Regular maintenance includes hardware, software and network safety check. In hardware check, middleware, readers and circuits insides the tags are repaired or replaced if physical damage is found. For disposing tags, a tag killer machine will be used prior to disposal to avoid leakage of information. In software check, system test and periodic penetration test are proposed to be conducted. In network safety check, virus scanning, firewall checking and improvement are proposed to be conducted.

All software produced by this company has followed this improved RFID security SDLC. There was no hacker attacks spotted after the SDLC is in place.

Focus Group Member HA3

"Instead of developing our own security system, we use standard Public Key Infrastructure systems to ensure RFID system security."

– Focus group member

The focal company is a software provider of a jewellery company with only one single shop where RFID lifecycle is relatively short as the retail shop is the only domain uses RFID. Whenever jewellery is received from the manufacturer it will be tagged with RFID paper label. Such paper label is removed whenever the jewellery is sold.

Security Breaches

Similar to other jewellery retailing RFID breaches discussed, this software company's software also experienced eavesdropping with unauthorized readers. While the purpose of these reading cannot be judged, the software company wanted to protect the RFID tags by limiting the readers used, and the company believes it is a sensible solution as the RFID tags and readers exist only in one single shop.

Public Key Infrastructure (PKI) can be used to tackle the hacker attack threat. According to the company's working principles of RFID technology, the company wanted to use a visiting

control system to insulate the readers without authentication, which is an RFID authentication based on PKI enabled anti-hacking system. According to the design principles and analysis of security demand of anti-counterfeiting system, an RFID anti-hacking system based on PKI authorization is built. PKI is a key management platform following encryption protocol standards, which mainly include certification authority, certification library, key creation, backup copy, and rerun, renew management system, certification revocation system and application interface system.

Anti-hacking system based on password technology is the core of this designed approach. There are two major components in this authentication system, the key management centre and the authentication key. The key management centre is responsible for key creation, interchanging, destroying, including the issuance of public key and protection of private key. There is a random number generator in key management centre and the keys are created randomly.

The authentication key is recorded in anti-hacking system. The anti-hacking system is responsible to authenticating for readers, which can be taken charge of by the logistics department in supply chain. After testing the validity of readers by anti-hacking system, the data information can be read.

In addition to the PKI, anonymous ID systems are used as well. A smart-tag method was used with rewritable memory as an improvement to traditional PKI methods. When the tags are installed with rewritable memory, the information in the tag will be rewritten by the reader after read to avoid the hacker attack. This method will cost the company more as because rewritable memory is needed to be installed in a tag. In addition, a method named “anonymous-ID scheme” is in place, which store an encrypted ID in the tag. After read, the tag will send the ID which is encrypted to the reader as response, and the server receives the encrypted ID from the reader, which passes to the server for decryption. Upon successful decryption, the server obtains the ID information of the tag and sends the information to the reader. The method prevents the consumer data to be attacked by hacker via encrypting the ID. Being able to track a consumer’s location is another problem; the encrypted ID has to be rewritten by reader more frequently the better. Also, the reader will create a new password to text ID with new encrypted ID, after that the reader will replace the old encrypted ID by using the new one. The disadvantage is that the reader needs to rewrite the encrypted ID after agreements from consumers; it means the reader cannot rewrite the tags ID without cooperation from consumers. The frequency of ID rewrote also represent the level of privacy protection that is affected by the consumer. For example, if an ID is rewritten once during a long period of time, the tag can be attacked by a hacker during the period.

As time could be a factor for hacker attack, this solution is not perfect. However, as the RFID lifecycle of this particular supply chain is shorter than the safe period of time, there is no threat for this security system being used in this particular supply chain and there were no RFID security breach incidents spotted after the system is in place.

11 References

Abdelkafi, Nizar, and Margherita Pero. "Supply chain innovation-driven business models: Exploratory analysis and implications for management." *Business Process Management Journal* 24, no. 2 (2018): 589-608.

Abernathy, Frederick H., John T. Dunlop, Janice H. Hammond, and David Weil. "Retailing and supply chains in the information age." *Technology in society* 22, no. 1 (2000): 5-31.

Abraham, D. W., E. W. Dereje, and C. I. Lim. "Fishbone diagram approach for improving the passing rate for basic engineering subjects." Enhancing Learning: Teaching and Learning Conference, 2001.

Academic Coaching and Writing LLC (2017). *Dissertation Literature Review | How to Write a Dissertation Literature Review* . [ONLINE] Available at: https://www.academiccoachingandwriting.org/dissertation-doctor/resources/writing-a-literature-review. [Accessed 30 October 2017].

Alavi, Maryam, and Patricia Carlson. "A review of MIS research and disciplinary development." *Journal of Management Information Systems* 8, no. 4 (1992): 45-62.
Heron, John. *Co-operative inquiry: Research into the human condition*. Sage, 1996.

Alfaro, Joaquin Garcia, Michel Barbeau, and Evangelos Kranakis. "Proactive threshold cryptosystem for EPC tags." *Ad hoc & sensor wireless networks* 12, no. 3-4 (2011): 187-208.

Ali, Moazzam, and Bakali Mukasa. "Contraception supply chain challenges: a review of evidence from low-and middle-income countries." *The European Journal of Contraception and Reproductive Health Care* 23 (2018): 100.

Almasizadeh, Jaafar, and Mohammad Abdollahi Azgomi. "Mean privacy: A metric for security of computer systems." *Computer Communications* 52 (2014): 47-59. Alonso, Jose Antonio, and M. Teresa Lamata. "Consistency in the analytic hierarchy process: a new approach." *International journal of uncertainty, fuzziness and knowledge-based systems* 14, no. 04 (2006): 445-459.

Alonso, Jose Antonio, and M. Teresa Lamata. "Consistency in the analytic hierarchy process: a new approach." *International journal of uncertainty, fuzziness and knowledge-based systems* 14, no. 04 (2006): 445-459.

Amaratunga, Dilanthi, David Baldry, Marjan Sarshar, and Rita Newton. "Quantitative and qualitative research in the built environment: application of "mixed" research approach." *Work study* 51, no. 1 (2002): 17-31.

American Society for Quality (2005). Fishbone diagram. [ONLINE] Available at: http://www.asq.org/learnabout-quality/cause-analysis-tools/overview/fishbone.html. [Accessed 4 September 2017].

Apiecionek, Łukasz, Jacek M. Czerniak, and Wojciech T. Dobrosielski. "Quality of services method as a DDoS protection tool." In *Intelligent Systems' 2014*, pp. 225-234. Springer, Cham, 2015.

Arthur, Jeffrey B. "Effects of human resource systems on manufacturing performance and turnover." *Academy of Management journal* 37, no. 3 (1994): 670-687.

Bacheldor, Beth. "Washington Hospital Center to quadruple its RFID expansion." *RFID Journal, http://www. rfidjournal. com/article/view/3009* (2007).

Baker, Sarah Elsie, Rosalind Edwards, and Mark Doidge. How many qualitative interviews is enough? Expert voices and early career reflections on sampling and cases in qualitative research. *National Centre for Research Methods, Southampton, UK.* [ONLINE] Available at: http://eprints.ncrm.ac.uk/2273/4/how_many_interviews.pdf [Accessed 27 April 2018].

Balanced Scorecard Institute (1995, May 3). Basic Tools for Process Improvement. [ONLINE] Available at: http://www.balancedscorecard.org/Portals/0/PDF/c-ediag.pdf [Accessed 4 September 2017].

Balanced Scorecard Institute (2007). Basic tools for process improvement, Module 5 – Cause and Effect diagram. [ONLINE] Available at: http://www.balancedscorecard.org/files/c-ediag.pdf [Accessed 4 September 2017].

Baumgartner, Hans, and Jan-Benedict EM Steenkamp. "Response styles in marketing research: A cross-national investigation." *Journal of marketing research* 38, no. 2 (2001): 143-156.

Behnam, Bahmankhah, and Helena Alvelos. "Exploring the potential of quality tools in tire retreading industry: A case study." *International Journal of Engineering Science and Technology (IJEST)* 3, no. 6 (2011): 5337-5345.

Bell, Bradford S., and Steve WJ Kozlowski. "Active learning: effects of core training design elements on self-regulatory processes, learning, and adaptability." *Journal of Applied psychology* 93, no. 2 (2008): 296.

Bell, Judith. *Doing Your Research Project: A guide for first-time researchers*. McGraw-Hill Education (UK), 2014.

Benbasat, Izak, and Robert W. Zmud. "The identity crisis within the IS discipline: Defining and communicating the discipline's core properties." *MIS quarterly* (2003): 183-194.

Benbasat, Izak, David K. Goldstein, and Melissa Mead. "The case research strategy in studies of information systems." *MIS quarterly* (1987): 369-386.

Bertino, Elisa, and Elena Ferrari. "Big data security and privacy." In *A Comprehensive Guide Through the Italian Database Research Over the Last 25 Years*, pp. 425-439. Springer, Cham, 2018.

Bhagwat, Rajesh O., and Dadarao N. Raut. "Impact assessment of supply chain constraints over performance of public distribution system." *International Journal of Indian Culture and Business Management* 16, no. 1 (2018): 19-38.

Biedermann, Sebastian, and Stefan Katzenbeisser. "Detecting computer worms in the cloud." In *Open Problems in Network Security*, pp. 43-54. Springer, Berlin, Heidelberg, 2012.

Bi, Fei, and Yi Mu. "Efficient RFID authentication scheme for supply chain applications." In *Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on*, pp. 583-588. IEEE, 2010.

Birdi, Kamal, Chris Clegg, Malcolm Patterson, Andrew Robinson, Chris B. Stride, Toby D. Wall, and Stephen J. Wood. "The impact of human resource and operational management practices on company productivity: A longitudinal study." *Personnel Psychology* 61, no. 3 (2008): 467-501.

Blackstone, Erwin A., Joseph P. Fuhr Jr, and Steve Pociask. "The health and economic effects of counterfeit drugs." *American health & drug benefits* 7, no. 4 (2014): 216.

Blanchard, D. "SCOR goes green." *Industry Week* 257, no. 5 (2008): 79.

Blume, Brian D., J. Kevin Ford, Timothy T. Baldwin, and Jason L. Huang. "Transfer of training: A meta-analytic review." *Journal of management* 36, no. 4 (2010): 1065-1105..

Bolstorff, Peter, and Robert Rosenbaum. *Supply Chain Excellence: A Handbook for Dramatic Improvement Using the SCOR Model. AMACOM Div American Mgmt Assn*. ISBN 0-8144-0730-7, 2003.

Bordage, Georges, and Beth Dawson. "Experimental study design and grant writing in eight steps and 28 questions." *Medical education* 37, no. 4 (2003): 376-385.

Bose, Tarun Kanti. "Application of fishbone analysis for evaluating supply chain and business process-a case study on the St James Hospital." *International Journal of Managing Value and Supply Chains (IJMVSC)* 3, no. 2 (2012): 17-24.

Boselie, Paul, Jaap Paauwe, and Paul Jansen. "Human resource management and performance: lessons from the Netherlands." *International Journal of Human Resource Management* 12, no. 7 (2001): 1107-1125.

BPMSG. AHP Priority Calculator [ONLINE] Available at: https://bpmsg.com/academic/ahp_calc.php. [Accessed 30 July 2016].

Bradley, Joseph. "Management based critical success factors in the implementation of Enterprise Resource Planning systems." *International Journal of Accounting Information Systems* 9, no. 3 (2008): 175-200.

BRANDMAN, BARRY. "Supply chain security: playing it safe: does your current asset-protection plan provide a false sense of security?." *Inbound Logistics* (2015). [ONLINE] Available at: http://www.inboundlogistics.com/cms/article/supply-chain-security-playing-it-safe. [Accessed 03 June 2018].

Braunscheidel, Michael J., and Nallan C. Suresh. "Cultivating Supply Chain Agility: Managerial Actions Derived from Established Antecedents." In *Supply Chain Risk Management*, pp. 289-309. Springer, Singapore, 2018.

Brødsgaard, Kjeld Erik. "China's 13th Five-Year Plan: A Draft Proposal." *The Copenhagen Journal of Asian Studies* 33, no. 2 (2016): 97-105.

Bruque, Sebastian, and Jose Moyano. "Organisational determinants of information technology adoption and implementation in SMEs: The case of family and cooperative firms." *Technovation* 27, no. 5 (2007): 241-253.

Bryman, Alan. "Integrating quantitative and qualitative research: how is it done?." *Qualitative research* 6, no. 1 (2006): 97-113.

Bryman, Alan, and Duncan Cramer. *Quantitative data analysis for social scientists*. Taylor & Frances/Routledge, 1990.

Bullet, No Silver. "Essence and accidents of software engineering, fp brooks." *IEEE Computer* 20, no. 4 (1987): 10-19.

Cai, Shaoying, Chunhua Su, Yingjiu Li, Robert Deng, and Tieyan Li. "Protecting and restraining the third party in RFID-enabled 3PL supply chains." In *International Conference on Information Systems Security*, pp. 246-260. Springer, Berlin, Heidelberg, 2010.edited by Somesh Jha and Anish Mathuria, (pp. 246-260).

Cai, Shaoying, Tieyan Li, Yingjiu Li, and Robert H. Deng. "Ensuring dual security modes in RFID-enabled supply chain systems." In *International Conference on Information Security Practice and Experience*, pp. 372-383. Springer, Berlin, Heidelberg, 2009.

Camp, Robert C. "Benchmarking: the search for industry best practices that lead to superior performance." In *Benchmarking: the search for industry best practices that lead to superior performance*. ASQC/Quality Resources, 1989.

Candy, Philip C. "Constructivism and the study of self-direction in adult learning." *Studies in the Education of Adults* 21, no. 2 (1989): 95-116. https://doi.org/10.1080/02660830.1989.11730524

Carbone, Anna. "Foods and Places: Comparing Different Supply Chains." *Agriculture* 8, no. 1 (2018): 6.

Carrer, T. *Carriage of Goods by Sea*. 1952.

Carr, Taylor. (2015). *Threat Vulnerabilities Life Sciences Companies Will Face This Year*. [ONLINE] Available at: http://www.securadyne.com/industry-pharmaceutical/threat-vulnerabilities-life-sciences-companies-will-face-this-year. [Accessed 30 June 2018]

Cassel, Mathieu, Hervé Piégay, and Jérôme Lavé. "Effects of transport and insertion of radio frequency identification (RFID) transponders on resistance and shape of natural and synthetic pebbles: applications for riverine and coastal bedload tracking." *Earth Surface Processes and Landforms* 42, no. 3 (2017): 399-413.

Cavinato, Joseph L. "A total cost/value model for supply chain competitiveness." *Journal of business logistics* 13, no. 2 (1992): 285.

Centobelli, Piera, Roberto Cerchione, Emilio Esposito, and Mario Raffa. "Digital Marketing in Small and Medium Enterprises: The Impact of Web-Based Technologies." *Advanced Science Letters* 22, no. 5-6 (2016): 1473-1476.

Cha, Shi-Cho. "Efficient method of achieving agreements between individuals and organizations about RFID privacy." *IEICE TRANSACTIONS on Information and Systems* 93, no. 7 (2010): 1866-1877.

Chang, Hyejung. "Evaluation framework for telemedicine using the logical framework approach and a fishbone diagram." *Healthcare informatics research* 21, no. 4 (2015): 230-238.

Chang, James I., and Cheng-Chung Lin. "A study of storage tank accidents." *Journal of loss prevention in the process industries* 19, no. 1 (2006): 51-59.

Chawla, Vipul, and Dong Sam Ha. "An overview of passive RFID." *IEEE Communications Magazine* 45, no. 9 (2007).

Chen, Cheng-Liang, and Wen-Cheng Lee. "Multi-objective optimization of multi-echelon supply chain networks with uncertain product demands and prices." *Computers & Chemical Engineering* 28, no. 6-7 (2004): 1131-1144.

Chen, Lianghan, Kevin Correll, Leon Telyaz, and Nicole E. Pivnick. "System and method of notifying user near point of sale location of available rewards at the point of sale location." U.S. Patent Application 10/147,100, filed December 4, 2018.

Chen, Li, He Ba, Wendi Heinzelman, and Andre Cote. "RFID range extension with low-power wireless edge devices." In *2013 International Conference on Computing, Networking and Communications (ICNC)*, pp. 524-528. IEEE, 2013.

Cheng, TC Edwin, and Tsan-Ming Choi, eds. *Innovative quick response programs in logistics and supply chain management*. Springer Science & Business Media, 2010.

Cheung, H. H., and S. H. Choi. "Implementation issues in RFID-based anti-counterfeiting systems." *Computers in Industry* 62, no. 7 (2011): 708-718.

Chien, Hung-Yu, and Chi-Sung Laih. "ECC-based lightweight authentication protocol with untraceability for low-cost RFID." *Journal of Parallel and Distributed Computing* 69, no. 10 (2009): 848-853.

China Briefing News (2018). The Pearl River Delta Greater Bay Area Integration Plan - China Briefing News. [ONLINE] Available at: http://www.china-briefing.com/news/2018/02/05/the-pearl-river-delta-greater-bay-area-integration-plan.html. [Accessed 27 May 2018].

China Knowledge (2010). China Online Knowledge Databank. [ONLINE] Available at: http://www.chinaknowledge.com/Databank/Default.aspx. [Accessed 21 September 2010].

Christopher, Martin, and Hau Lee. "Mitigating supply chain risk through improved confidence." *International journal of physical distribution & logistics management* 34, no. 5 (2004): 388-396.

Chung, Rih-Lung, Hui Ming Wee, Yen-Deng Huang, and Yung-Lung Cheng. "Supply Chain Inventory System Considering Production Postponement and Rework." *International Journal of Industrial Engineering: Theory, Applications and Practice*24, no. 5.

Ciocoiu, Carmen Nadia. *Managementul riscului: Teorii, practici, metodologii*. Editura ASE, 2008.

Cleven, Anne, Philipp Gubler, and Kai M. Hüner. "Design alternatives for the evaluation of design science research artifacts." In *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology*, p. 19. ACM, 2009.

CNET (2006). *Gone in 60 seconds--the high-tech version - CNET*. [ONLINE] Available at: https://www.cnet.com/news/gone-in-60-seconds-the-high-tech-version/. [Accessed 10 June 2018].

Colicchia, Claudia, and Fernanda Strozzi. "Supply chain risk management: a new methodology for a systematic literature review." *Supply Chain Management: An International Journal*17, no. 4 (2012): 403-418.

Colquitt, Jason A., Jeffrey A. LePine, and Raymond A. Noe. "Toward an integrative theory of training motivation: a meta-analytic path analysis of 20 years of research." *Journal of applied psychology* 85, no. 5 (2000): 678.

Colvey, S. (2009). What on earth is RFID? RFID features [ONLINE] Available at: http://www.vnunet.com/computeractive/features/2013911/earth-rfid. [Accessed 30 October 2011].

Compilation and Translation Bureau. *The 13th Five-Year Plan.* [ONLINE] Available at: http://en.ndrc.gov.cn/policyrelease/201612/P020161207645766966662.pdf [Accessed 13 December 2016].

Comunian, Roberta, and Lauren England. "The resilience of knowledge from industrial to creative clusters: the case of regional craft clusters in the West Midlands (UK)." In *Resilience, Crisis and Innovation Dynamics*. Edward Elgar Publishing, 2018.

Cooper, Donald R., Pamela S. Schindler, and Jianmin Sun. *Business research methods*. Vol. 9. New York: McGraw-Hill Irwin, 2006.

Council of Supply Chain Management Professionals (n.d.). Definition of Supply Chain Management. [ONLINE] Available at: www.cscmp.org. [Accessed 23 May 2018].

Creswell, John W. "Mapping the field of mixed methods research." (2009): 95-108.

d'Arcimoles, Charles-Henri. "Human resource policies and company performance: a quantitative approach using longitudinal data." *Organization studies* 18, no. 5 (1997): 857-874.

Dastmalchian, Ali, and Paul Blyton. "Organizational structure, human resource practices and industrial relations." *Personnel Review* 21, no. 1 (1992): 58-67.

Dauriz, Linda, Nathalie Remy, and Thomas Tochtermann. "A multifaceted future: The jewelry industry in 2020." *Retrieved on December* 4 (2014): 2014. [ONLINE] Available at: https://www.mckinsey.com/industries/retail/our-insights/a-multifaceted-future-the-jewelry-industry-in-2020. [Accessed 30 June 2018].

Davison, Robert M., Douglas R. Vogel, and Roger W. Harris. "The e-transformation of Western China." *Communications of the ACM* 48, no. 4 (2005): 62-67.

Delaney, John T., and Mark A. Huselid. "The impact of human resource management practices on perceptions of organizational performance." *Academy of Management journal* 39, no. 4 (1996): 949-969.

Detica (2018). *The Cost of Cyber Crime* [ONLINE] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf [Accessed 30 June 2018].

de Treville, Suzanne, Mikko Ketokivi, and Vinod R. Singhal. "Competitive manufacturing in a high-cost environment: Introduction to the special issue." (2017).

De Vita, Giuseppe, F. Bellatalla, and Giuseppe Iannaccone. "Ultra-low power PSK backscatter modulator for UHF and microwave RFID transponders." *Microelectronics Journal* 37, no. 7 (2006): 627-629.

Dey, Ian. *Qualitative data analysis: A user friendly guide for social scientists*. Routledge, 2003.

Dey, Prasanta Kumar. "Decision support system for inspection and maintenance: a case study of oil pipelines." *IEEE transactions on engineering management* 51, no. 1 (2004): 47-56.

Dhandapani, Dhanasekar. "Applying the Fishbone diagram and Pareto principle to Domino." *IBM Lotus technical library June* (2004).

Dictionary (2018). *The definition of bias*. [ONLINE] Available at: http://www.dictionary.com/browse/bias. [Accessed 26 Apr 2018].

Dodou, Dimitra, and Joost CF de Winter. "Social desirability is the same in offline, online, and paper surveys: A meta-analysis." *Computers in Human Behavior* 36 (2014): 487-495.

Dormann, Carsten F., Jane Elith, Sven Bacher, Carsten Buchmann, Gudrun Carl, Gabriel Carré, Jaime R. García Marquéz et al. "Collinearity: a review of methods to deal with it and a simulation study evaluating their performance." *Ecography* 36, no. 1 (2013): 27-46.

Doshi, J. A., J. D. Kamdar, S. Y. Jani, and S. J. Chaudhary. "Root Cause Analysis using Ishikawa diagram for reducing radiator rejection." *International Journal of Engineering Research and Applications* 2, no. 6 (2012): 684-689.

Duckstein, Lucien, and Serafim Opricovic. "Multiobjective optimization in river basin development." *Water resources research* 16, no. 1 (1980): 14-20.

El-Awamry, Ahmed, Maher Khaliel, Abdelfattah Fawky, Mohamed El-Hadidy, and Thomas Kaiser. "Novel notch modulation algorithm for enhancing the chipless RFID tags coding capacity." In *2015 IEEE International Conference on RFID (RFID)*, pp. 25-31. IEEE, 2015.

Eltrun (1993). International Logistics Paper [ONLINE] Available at: http://www.eltrun.gr/papers/International-Logistics-Paper.pdf. [Accessed 30 October 2011].

Engels, Daniel W., and Sanjay E. Sarma. "The reader collision problem." In *Systems, Man and Cybernetics, 2002 IEEE International Conference on*, vol. 3, pp. 6-pp. IEEE, 2002.

Enyinda, Chris I., and Denver Tolliver. "Taking counterfeits out of the pharmaceutical supply chain in Nigeria: Leveraging multilayer mitigation approach." *Journal of African Business*10, no. 2 (2009): 218-234.

EPC Express (2011). RFID Forecasts, Players and Opportunities 2011-2021., What Is RFID? [ONLINE] Available at: http://www.epcexpress.org/modules.php?name=Content&pa=showpage&pid=139. [Accessed 30 October 2011].

Evans, W. Randy, and Walter D. Davis. "High-performance work systems and organizational performance: The mediating role of internal social structure." *Journal of management* 31, no. 5 (2005): 758-775.

Fang, Junhui, Youci Liang, Ruojing Wang, and Yunfei Zhong. "Research on Process Parameters of Screen Printed RFID Tags." In *Applied Sciences in Graphic Communication and Packaging*, pp. 393-399. Springer, Singapore, 2018.

Fechner, Gustav Theodor. "Elemente der Psychophysik. Leipzig." *SN: Breitkopf* (1860).

FedEx. Jewellery shipping program. FedEx Declared Value Advantage. [ONLINE] Available at: https://www.fedex.com/content/dam/fedex/us-united-states/services/FedEx_Jewelry_Shipping_Program.pdf. [Accessed 02 July 2018].

Fettke, Peter, and Peter Loos. "Multiperspective evaluation of reference models–towards a framework." In *International Conference on Conceptual Modeling*, pp. 80-91. Springer, Berlin, Heidelberg, 2003.

Fielden, Jann M. "Grief as a transformative experience: Weaving through different lifeworlds after a loved one has completed suicide." *International Journal of Mental Health Nursing* 12, no. 1 (2003): 74-85.

Fink, Arlene. *How to design survey studies*. Vol. 6. Sage, 2003.

Finkenzeller, Klaus. "RFID handbook 2nd Edition." *Wilesy*(2003).

Fitzgerald, William. "Training versus development." *Training and Development* 46, no. 5 (1992): 81-84.

Flyvbjerg, Bent. "Five misunderstandings about case-study research." *Qualitative inquiry* 12, no. 2 (2006): 219-245.

Francis, Lishoy, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. "Potential misuse of NFC enabled mobile phones with embedded security elements as contactless attack platforms." In *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for*, pp. 1-8. IEEE, 2009.

Free Patents Online. Patents Search Online [ONLINE] Available at: http://www.freepatentsonline.com/result.html?query_txt=electronic+seal+RFID&sort=relevance&srch=top&search. [Accessed 20 October 2010].

Fui-Hoon Nah, Fiona, Janet Lee-Shang Lau, and Jinghua Kuang. "Critical factors for successful implementation of enterprise systems." *Business process management journal* 7, no. 3 (2001): 285-296.

Galliers, Robert D. "Strategic information systems planning: myths, reality and guidelines for successful implementation." *European Journal of Information Systems* 1, no. 1 (1991): 55-64.

Gall, Meredith Damien, Walter R. Borg, and Joyce P. Gall. *Educational research: An introduction*. Longman Publishing, 1996.

Gandino, Filippo, Bartolomeo Montrucchio, and Maurizio Rebaudengo. "A security protocol for RFID traceability." *International Journal of Communication Systems* 30, no. 6 (2017): e3109.

Ganesan, Shankar, Morris George, Sandy Jap, Robert W. Palmatier, and Barton Weitz. "Supply chain management and retailer performance: emerging trends, issues, and implications for research and practice." *Journal of Retailing*85, no. 1 (2009): 84-94.

Ganji Jamehshooran, Bijan, M. Shaharoun, and Habibah Norehan Haron. "Assessing supply chain performance through applying the SCOR model." *International Journal of Supply Chain Management* 4, no. 1 (2015).

Gartner. "*Gartner Says Worldwide RFID Revenue to Surpass $1.2 Billion in 2008*." 2003. Accessed April 2, 2018. https://www.gartner.com/newsroom/id/610807

Gawdzińska, K. "Application of the Pareto chart and Ishikawa diagram for the identification of major defects in metal composite castings." *Archives of Foundry Engineering* 11, no. 2 (2011): 23-28.

Gerber, Alan S., and Donald P. Green. "The effects of canvassing, telephone calls, and direct mail on voter turnout: A field experiment." *American political science review* 94, no. 3 (2000): 653-663.

Gill, Paul, Kate Stewart, Elizabeth Treasure, and Barbara Chadwick. "Methods of data collection in qualitative research: interviews and focus groups." *British dental journal* 204, no. 6 (2008): 291.

Glaser, Barney G., and Anselm L. Strauss. *Discovery of grounded theory: Strategies for qualitative research*. Routledge, 2017.

Google (2013). Good to know e-guide to staying safe and secure online [ONLINE] Available at: http://www.google.com/goodtoknow/online-safety/locking/. [Accessed 12 December 2015].

Greenleaf, Eric A. "Improving rating scale measures by detecting and correcting bias components in some response styles." *Journal of Marketing Research* 29, no. 2 (1992): 176.

Gregor, Shirley. "The nature of theory in information systems." *MIS quarterly* (2006): 611-642.

Grimm, Curtis M. "The practice of supply chain management: where theory and application converge." *Transportation Journal* 43, no. 2 (2004): 59.

GS1. EPCGlobal | GS1. [ONLINE] Available at: https://www.gs1.org/EPCGlobal. [Accessed 17 May 2018].

Guo, Ken H. "Security-related behavior in using information systems in the workplace: A review and synthesis." *Computers & Security* 32 (2013): 242-251.

Hall, Bronwyn H., and Beethika Khan. *Adoption of new technology*. No. w9730. National bureau of economic research, 2003.

Hancke, Gerhard P. "Practical eavesdropping and skimming attacks on high-frequency RFID tokens." *Journal of Computer Security* 19, no. 2 (2011): 259-288.

Handfield, Robert B., and Ernest L. Nichols. *Supply chain redesign: Transforming supply chains into integrated value systems*. Ft Press, 2002.

Harel, Gedaliahui H., and Shay S. Tzafrir. "The effect of human resource management practices on the perceptions of organizational and market performance of the firm." *Human Resource Management: Published in Cooperation with the School of Business Administration, The University of Michigan and in alliance with the Society of Human Resources Management* 38, no. 3 (1999): 185-199.

Harrison, Mark, Duncan McFarlane, Ajith Kumar Parlikad, and Chien Yaw Wong. "Information management in the product lifecycle-the role of networked RFID." In *Industrial Informatics, 2004. INDIN'04. 2004 2nd IEEE International Conference on*, pp. 507-512. IEEE, 2004.

Hart, Chris. "Hart, Chris, Doing a Literature Review: Releasing the Social Science Research Imagination. London: Sage, 1998." (1998).

Haas, Rainer, and Oliver Meixner. "An illustrated guide to the analytic hierarchy process." *Vienna: University of Natural Resources and Applied Life Sciences* (2005).

Hasan, Bassam. "Effectiveness of computer training: The role of multilevel computer self-efficacy." *Journal of Organizational and End User Computing (JOEUC)* 18, no. 1 (2006): 50-68.

Hashim, H. Z., K. A. A. Rahman, H. Alli, and R. A. A. R. Effendi. "Design economic evolution in the jewellery industry through design process." *Journal of Fundamental and Applied Sciences* 10, no. 4S (2018): 773-782.

Healthcare Distribution Management Associations (2009). The Role of Distributors in the Us Healthcare Industry, Arlington VA: Center for Healthcare Supply Chain Research.

Heinrich, Claus. "RFID and Beyond." *Growing Your Business through Real World Awareness* (2005).

Hekmatpanah, Masoud. "The application of cause and effect diagram in the oil industry in Iran: The case of four liter oil canning process of Sepahan Oil Company." *African Journal of Business Management* 5, no. 26 (2011): 10900-10907.

Hennessey Jr, Joseph P. "A comparison of the Weibull and Rayleigh distributions for estimating wind power potential." *Wind Engineering* (1978): 156-164.

Hevner, Alan R., Salvatore T. March, Jinsoo Park, and Sudha Ram. "Design science in information systems research." *Management Information Systems Quarterly* 28, no. 1 (2004)

Holste Cliff ." *Logistics News: The New Age Of Security Awareness*." 2013 Accessed January 25, 2019. http://www.scdigest.com/experts/Holste_13-05-29.php?cid=7089

Hong Kong Trade Development Council Research. PRD Economic Profile [ONLINE] Available at: http://china-trade-research.hktdc.com/business-news/article/Facts-and-Figures/PRD-Economic-Profile/ff/en/1/1X000000/1X06BW84.htm, [Accessed 27 September 2018].

Hong-Ying, Sun. "The application of barcode technology in logistics and warehouse management." In *Education Technology and Computer Science, 2009. ETCS'09. First International Workshop on*, vol. 3, pp. 732-735. IEEE, 2009.

Horkheimer, Max. "Traditionelle und kritische Theorie." *Zeitschrift für Sozialforschung* 6, no. 2 (1937): 245-294.

Hsiao, Rong-Shue, Chun-Hao Kao, Tian-Xiang Chen, and Jui-Lun Chen. "A passive RFID-based location system for personnel and asset monitoring." *Technology and Health Care*Preprint (2018): 1-6.

Huang, George Q., Y. F. Zhang, and P. Y. Jiang. "RFID-based wireless manufacturing for real-time management of job shop WIP inventories." *The International Journal of Advanced Manufacturing Technology* 36, no. 7-8 (2008): 752-764.

Hugos, Michael H. *Essentials of supply chain management*. John Wiley & Sons, 2018.
Hult, G. Tomas M., Christopher W. Craighead, and David J. Ketchen, Jr. "Risk uncertainty and supply chain decisions: a real options perspective." *Decision Sciences* 41, no. 3 (2010): 435-458.

Huo, Fei, Patrick Mitran, and Guang Gong. "Analysis and validation of active eavesdropping attacks in passive FHSS RFID systems." *IEEE Transactions on Information Forensics and Security* 11, no. 7 (2016): 1528-1541.

Hwang, Ching-Lai, and Kwangsun Yoon. "Methods for multiple attribute decision making." In *Multiple attribute decision making*, pp. 58-191. Springer, Berlin, Heidelberg, 1981.

Hwang, Ching-Lai, Young-Jou Lai, and Ting-Yun Liu. "A new approach for multiple objective decision making." *Computers & operations research* 20, no. 8 (1993): 889-899.

IBS. Mini Case Studies, *Case Study in Business, Management* [ONLINE] Available at: http://www.icmrindia.org/casestudies/Mini%20Case%20Studies.htm. [Accessed 12 August 2018].

IDTechEx. "*RFID Forecasts, Players and Opportunities 2018-2028: IDTechEx*." 2018. Accessed January 25, 2018. https://www.idtechex.com/research/reports/rfid-forecasts-players-and-opportunities-2018-2028-000642.asp.

Ilie, Gheorghe, and Carmen Nadia Ciocoiu. "Application of fishbone diagram to determine the risk of an event with multiple causes." *Management Research and Practice* 2, no. 1 (2010): 1-20.

Introna, Lucas D. "Privacy and the computer: why we need privacy in the information society." *Metaphilosophy* 28, no. 3 (1997): 259-275.

Ishida, Masanori, Shigeru Sekiguchi, Kouki Hayashi, Shin Nakamatsu, and Ryuutarou Hosoi. "RFID tag search method, non-transitory storage medium storing RFID tag search program, and RFID tag search device." U.S. Patent 9,551,774, issued January 24, 2017.
Jackson, Susan E., and Randell S. Schuler. "Understanding human resource management in the context of organizations and their environments." *Annual review of psychology* 46, no. 1 (1995): 237-264.
Jamieson, Susan. "Likert scales: how to (ab) use them." *Medical education* 38, no. 12 (2004): 1217-1218.

Janesick, Valerie J. "The choreography of qualitative research design." *Handbook of qualitative research.* (2000): 379-399.

Jedermann, Reiner, Luis Ruiz-Garcia, and Walter Lang. "Spatial temperature profiling by semi-passive RFID loggers for perishable food transportation." *Computers and Electronics in Agriculture* 65, no. 2 (2009): 145-154.

Jiang, Jingjing (2004). Wal-Mart's China inventory to hit US$18b this year, China Business Week. [ONLINE] Available at: http://www.chinadaily.com.cn/english/doc/2004-11/29/content_395728.htm. [Accessed 21 September 2010].

Jones, David, and Shirley Gregor. "The anatomy of a design theory." *Journal of the Association for Information Systems* 8, no. 5 (2007): 1.

Juels, Ari. "RFID security and privacy: A research survey." *IEEE journal on selected areas in communications* 24, no. 2 (2006): 381-394.

Juran, Joseph M., and A. Blanford Godfrey. "Juran's quality handbook 5th ed." (1999).

Kalleberg, Arne L., and James W. Moody. "Human resource management and organizational performance." *American Behavioral Scientist* 37, no. 7 (1994): 948-962.

Kaminska, Olena & Foulsham, Tom (2013). Understanding Sources of Social Desirability Bias in Different Modes: Evidence from Eye-tracking. [ONLINE] Available at: https://www.iser.essex.ac.uk/research/publications/working-papers/iser/2013-04.pdf [Accessed 12 December 2015].

Kaplan, Bonnie, and Dennis Duchon. "Combining qualitative and quantitative methods in information systems research: a case study." *MIS quarterly* (1988): 571-586.

Karapetrovic, Stanislav, and E. S. Rosenbloom. "A quality control approach to consistency paradoxes in AHP." *European Journal of Operational Research* 119, no. 3 (1999): 704-718.

Karlsson, Julia. "Mini cases vs. Full length case studies: advantages and disadvantages." (2016).

Kartoglu, Umit, and Julie Milstien. "Tools and approaches to ensure quality of vaccines throughout the cold chain." *Expert review of vaccines* 13, no. 7 (2014): 843-854.

Katsuki, T. "Crisis: The Advanced Malware." *Internet security threat report-2013., Symantec Corporation* 18 (2012).

Kelly, Eileen P., and G. Scott Erickson. "RFID tags: commercial applications v. privacy rights." *Industrial Management & Data Systems* 105, no. 6 (2005): 703-713.

Khan, Edwin C., and Yunfei Ma. "RFID device, methods and applications." U.S. Patent 9,645,234, issued May 9, 2017.

Kilcarr, S. "Tips for thwarting cargo theft." *American Trucker, December* 30 (2015).

Kim, Dong Seong, Taek-Hyun Shin, and Jong Sou Park. "A security framework in RFID multi-domain system." In *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on*, pp. 1227-1234. IEEE, 2007.

Kim, Hee-Woong, and Atreyi Kankanhalli. "Investigating user resistance to information systems implementation: A status quo bias perspective." *MIS quarterly* (2009): 567-582.

Komac, Marko. "A landslide susceptibility model using the analytical hierarchy process method and multivariate statistics in perialpine Slovenia." *Geomorphology* 74, no. 1-4 (2006): 17-28.

Korpela, Jukka, Antti Lehmusvaara, and Markku Tuominen. "An analytic approach to supply chain development." *International Journal of Production Economics* 71, no. 1-3 (2001): 145-155.

Kourouthanassis, Panos, Leda Koukara, Chris Lazaris, and Kostas Thiveos. "Grocery Supply-Chain Management: MyGROCER innovative business and technology

framework1." *the e-Business Center, Athens University of Economics & Business, Athens, Greece* (2001): 5-9.

Krieger, Murray. "Ekphrasis the Illusion of the Natural Sign." (1991).

Krosnick, Jon A. "Survey research." *Annual review of psychology* 50, no. 1 (1999): 537-567.
Kumar, Sameer, Brooke B. Kadow, and Melissa K. Lamkin. "Challenges with the introduction of radio-frequency identification systems into a manufacturer's supply chain–a pilot study." *Enterprise Information Systems* 5, no. 2 (2011): 235-253.

Kumar, Sameer, Erin Dieveney, and Aaron Dieveney. "Reverse logistic process control measures for the pharmaceutical industry supply chain." *International Journal of Productivity and Performance Management* 58, no. 2 (2009): 188-204.

Kumru, Ozan S., Sangeeta B. Joshi, Dawn E. Smith, C. Russell Middaugh, Ted Prusik, and David B. Volkin. "Vaccine instability in the cold chain: mechanisms, analysis and formulation strategies." *Biologicals* 42, no. 5 (2014): 237-259.

Kwiesielewicz, Miroslaw, and Ewa Van Uden. "Inconsistent and contradictory judgements in pairwise comparison method in the AHP." *Computers & Operations Research* 31, no. 5 (2004): 713-719.

Ladyshewsky, Richard K. "A strategic approach for integrating theory to practice in leadership development." *Leadership & Organization Development Journal* 28, no. 5 (2007): 426-443.

Lahiri, Sandip. *RFID sourcebook*. IBM press, 2005.

Landt, Jeremy. "The history of RFID." *IEEE potentials* 24, no. 4 (2005): 8-11.

Lao, S. I., K. L. Choy, G. T. S. Ho, Y. C. Tsim, and N. S. H. Chung. "Determination of the success factors in supply chain networks: a Hong Kong-based manufacturer's perspective." *Measuring business excellence* 15, no. 1 (2011): 34-48.

Laumanns, Marco, and Stefan Woerner. "Multi-echelon Supply Chain Optimization: Methods and Application Examples." In *Optimization and Decision Support Systems for Supply Chains*, pp. 131-138. Springer, Cham, 2017.

Lee, Allen S. "A scientific methodology for MIS case studies." *MIS quarterly* (1989): 33-50.

Lee, Hau, and Seungjin Whang. "Decentralized multi-echelon supply chains: Incentives and information." *Management science* 45, no. 5 (1999): 633-640.

Lee, Hau L., and Seungjin Whang. "Higher supply chain security with lower cost: Lessons from total quality management." *International Journal of production economics*96, no. 3 (2005): 289-300.
Lee, Hau L., Venkata Padmanabhan, and Seungjin Whang. "The bullwhip effect in supply chains." *Sloan management review* 38 (1997): 93-102.

Lee, Newton. "Cyber attacks, prevention, and countermeasures." In *Counterterrorism and Cybersecurity*, pp. 249-286. Springer, Cham, 2015.

Lee, Yong Ki, Lejla Batina, and Ingrid Verbauwhede. "Privacy challenges in RFID systems." In *The Internet of Things*, pp. 397-407. Springer, New York, NY, 2010.

Lehtonen, Mikko, Daniel Ostojic, Alexander Ilic, and Florian Michahelles. "Securing RFID systems by detecting tag cloning." In *International Conference on Pervasive Computing*, pp. 291-308. Springer, Berlin, Heidelberg, 2009.

Lehtonen, Mikko O., Florian Michahelles, and Elgar Fleisch. "Trust and security in RFID-based product authentication systems." *IEEE Systems Journal* 1, no. 2 (2007): 129-144.

Levin, Richard C. "Appropriability, R&D spending, and technological performance." *The American Economic Review*78, no. 2 (1988): 424-428.

Lewis. RFID is becoming a significant business driver. RFID Article [ONLINE] Available at: http://www.rfidtoday.co.uk/articles/rfid_rfidforum.html. [Accessed 30 October 2011].

Life, Researching Social. "Qualitative data analysis." (1994).

Li, Jianxin, Bo Li, Tianyu Wo, Chunming Hu, Jinpeng Huai, Lu Liu, and K. P. Lam. "CyberGuarder: A virtualization security assurance architecture for green cloud computing." *Future Generation Computer Systems* 28, no. 2 (2012): 379-390.

Li, Nan, and Burcin Becerik-Gerber. "Life-cycle approach for implementing RFID technology in construction: Learning from academic and industry use cases." *Journal of Construction Engineering and Management* 137, no. 12 (2011): 1089-1098.

Li, Si-ming. "The Pearl River Delta: the Fifth Asian Little Dragon?." *Hong Kong, Macau, and the Pearl River Delta: A Geographical Survey* (2009): 210-235.

Liu, Alex X., and LeRoy A. Bailey. "PAP: A privacy and authentication protocol for passive RFID tags." *Computer Communications* 32, no. 7-10 (2009): 1194-1199.

Liu, Jun. "Development of Regional Logistics Along the One Belt and One Road." In *Contemporary Logistics in China*, pp. 77-101. Springer, Singapore, 2016.

Liu, Leian, Zhiqiang Chen, Ling Yang, Yi Lu, and Hongjiang Wang. "Research on the security issues of RFID-based supply chain." In *E-Business and E-Government (ICEE), 2010 International Conference on*, pp. 3267-3270. IEEE, 2010.

LPM. *Precious Cargo: Tiffany's Supply Chain Security* [ONLINE] Available at: http://lossprevention media.com/insider/supply-chain-security/precious-cargo-tiffanys-supply-chain-network/. [Accessed 30 June 2018].

Louis, Joseph, and Phillip S. Dunston. "Integrating IoT into operational workflows for real-time and automated decision-making in repetitive construction operations." *Automation in Construction* 94 (2018): 317-327.

Luo, Zongwei, B. P. Yen, Zhining Tan, and Zhicheng Ni. "Value analysis framework for RFID technology adoption in retailers in China." *Communications of the Association for Information Systems* (2008).

Lynch, James P., and John P. Jarvis. "Missing data and imputation in the uniform crime reports and the effects on national estimates." *Journal of Contemporary Criminal Justice*24, no. 1 (2008): 69-85.

Lyons, Kevin (2017). *Six Golden Rules for Defining Good Research Objectives* [ONLINE] Available at: https://www.lipmanhearne.com/how-to-define-good-research-objectives/. [Accessed 31 May 2018].

Madu, Christian N., ed. *Handbook of total quality management*. Springer Science & Business Media, 2012.

Mahinderjit-Singh, Manmeet, and Xue Li. "Trust in RFID-enabled supply-chain management." *International Journal of Security and Networks* 5, no. 2-3 (2010): 96-105.

Makridakis, Spyros, Steven C. Wheelwright, and Rob J. Hyndman. *Forecasting methods and applications*. John wiley & sons, 2008.

Malhotra, N., and J. Shaw Hall. "M. and Oppenheim, P.(2008), Essentials of Marketing Research: An Applied Orientation."

Mandhare, Supriya, Dr AK Sen, and Rajkumar Shende. "A Proposal on Protecting Data Leakages In Cloud Computing." *International Journal of Computer Engineering and Technology* 6, no. 2 (2015).

March, Salvatore T., and Gerald F. Smith. "Design and natural science research on information technology." *Decision support systems* 15, no. 4 (1995): 251-266.

March, Salvatore T., and Veda C. Storey. "Design science in the information systems discipline: an introduction to the special issue on design science research." *MIS quarterly*(2008): 725-730.

Marnerides, Angelos K., Michael R. Watson, Noorulhassan Shirazi, Andreas Mauthe, and David Hutchison. "Malware analysis in cloud computing: Network and system characteristics." In *Globecom Workshops (GC Wkshps), 2013 IEEE*, pp. 482-487. IEEE, 2013.

Marshall, Bryan, Peter Cardon, Amit Poddar, and Renee Fontenot. "Does sample size matter in qualitative research?: A review of qualitative interviews in IS research." *Journal of Computer Information Systems* 54, no. 1 (2013): 11-22.

Mason, Mark. "Sample size and saturation in PhD studies using qualitative interviews." In *Forum qualitative Sozialforschung/Forum: qualitative social research*, vol. 11, no. 3. 2010.

Maxwell, Joseph A. *Qualitative research design: An interactive approach*. Vol. 41. Sage publications, 2012.

McCullagh, Declan, and Story last modified January. "RFID tags: Big Brother in small packages." (2003).

McDowell, Christopher S. "Frangible RFID tag and method of producing same." U.S. Patent 9,626,620, issued April 18, 2017.

Meade, Laura, and Joseph Sarkis. "Strategic analysis of logistics and supply chain management systems using the analytical network process1." *Transportation Research Part E: Logistics and Transportation Review* 34, no. 3 (1998): 201-215.

Merriam, Sharan B. *Qualitative Research and Case Study Applications in Education. Revised and Expanded from" Case Study Research in Education."*. Jossey-Bass Publishers, 350 Sansome St, San Francisco, CA 94104, 1998.

Merriam-Webster. Bias | *Definition of Bias by Merriam-Webster*. [ONLINE] Available at: http://www.merriam-webster.com/dictionary/bias. [Accessed 26 April 2018].

Merriam-Webster. Security| *Definition of Security by Merriam-Webster*. [ONLINE] Available at: http://www.merriam-webster.com/dictionary/security. [Accessed 26 November 2019].

Merriam-Webster. Privacy| *Definition of Privacy by Merriam-Webster*. [ONLINE] Available at: https://www.merriam-webster.com/dictionary/privacy. [Accessed 26 November 2019].

Mick, David Glen. "Are studies of dark side variables confounded by socially desirable responding? The case of materialism." *Journal of consumer research* 23, no. 2 (1996): 106-119.

Miles, Matthew B., A. Michael Huberman, Michael A. Huberman, and Michael Huberman. *Qualitative data analysis: An expanded sourcebook*. sage, 1994.

Min, Hokey. "Location analysis of international consolidation terminals using the analytic hierarchy process." *Journal of Business Logistics* 15, no. 2 (1994): 25.

Mishra, Bimal Kumar, and Samir Kumar Pandey. "Dynamic model of worm propagation in computer network." *Applied mathematical modelling* 38, no. 7-8 (2014): 2173-2179.

Molnar, David, and David Wagner. "Privacy and security in library RFID: Issues, practices, and architectures." In *Proceedings of the 11th ACM conference on Computer and communications security*, pp. 210-219. ACM, 2004.

Moreno, Pedro Vizcaino. "Elements to Evaluate the Security of the Containerized Supply Chain." PhD diss., Universitat Politècnica de Catalunya. Escola Tècnica Superior d'Enginyeria Industrial de Barcelona. Escola Tècnica Superior d'Enginyeria Industrial de Barcelona. Mobilitat, 2010 (Enginyeria en Organització Industrial), 2010.

Morse, Janice M. "The significance of saturation." (1995): 147-149.

MTrack (2010). Tracker GPS GSM RF Self Powered | Best Award Winning Tracker [ONLINE] Available at: http://www.mtrackonline.co.uk. [Accessed 20 October 2010].

Mullis, Joe, Steve Gonzalez, and Emily Olanoff. "Non-transferable radio frequency identification label or tag." U.S. Patent 9,552,541, issued January 24, 2017.

Murphy, Richard S. "Property rights in personal information: An economic defense of privacy." In *Privacy*, pp. 43-79. Routledge, 2017.

Muzellec, Laurent, and Eamonn O'Raghallaigh. "Mobile technology and its impact on the consumer decision-making journey: how brands can capture the mobile-driven "Ubiquitous" moment of truth." *Journal of Advertising Research* 58, no. 1 (2018): 12-15.

Myers, Michael D. "Qualitative research in information systems." *Management Information Systems Quarterly* 21, no. 2 (1997): 241-242.

Nair, Prashant R., and S. P. Anbuudayasankar. "Tackling Supply Chain Management Through High-Performance Computing: Opportunities and Challenges." In *Silicon Photonics & High Performance Computing*, pp. 1-7. Springer, Singapore, 2018.

Narayana, Sushmita A., Rupesh Kumar Pati, and Prem Vrat. "Managerial research on the pharmaceutical supply chain–A critical review and some insights for future directions." *Journal of Purchasing and Supply Management* 20, no. 1 (2014): 18-40.

Nguyen, Dung H., Sander de Leeuw, and Wout EH Dullaert. "Consumer behaviour and order fulfilment in online retailing: a systematic review." *International Journal of Management Reviews* 20, no. 2 (2018): 255-276.

Nickerson, Raymond S. "Confirmation bias: A ubiquitous phenomenon in many guises." *Review of general psychology*2, no. 2 (1998): 175.

Nicolaou, Andreas I. "Quality of postimplementation review for enterprise resource planning systems." *International Journal of Accounting Information Systems* 5, no. 1 (2004): 25-49.

Noe, Raymond A., Michael J. Tews, and Alison McConnell Dachner. "Learner engagement: A new perspective for enhancing our understanding of learner motivation and workplace learning." *Academy of Management Annals* 4, no. 1 (2010): 279-315.

Novikov, Alexander M., and Dmitry A. Novikov. *Research methodology: From philosophy of science to research design*. CRC Press, 2013.

O'Conner, Mary Catherine (2006). Gillette Fuses RFID With Product Launch, RFID Journal [ONLINE] Available at: http://www.rfidjournal.com/article/articleview/2222/1/1/. [Accessed 20 October 2010].

Octopus (2010). Octopus Card Limited – Our History. [ONLINE] Available at: http://www.octopus.com.hk/about-us/corporate-profile/our-history/en/index.html. [Accessed 20 October 2010].
O'donovan, Denis. "Rating extremity: pathology or meaningfulness?." *Psychological Review* 72, no. 5 (1965): 358.

Ohkubo, Miyako, Koutarou Suzuki, and Shingo Kinoshita. "RFID privacy issues and technical challenges." *Communications of the ACM* 48, no. 9 (2005): 66-71.

Oki, Kiyohiro (2016). What is a Bad Research Question? *Akamon Management Review*, 15(10), 509-522.

Olson Hope. "Quantitative "versus" qualitative research: The wrong question." May 8, 1995. Accessed March 5, 2003. http://www.ualberta.ca/dept/slis/cais/olson.htm

Opricovic, Serafim, and Gwo-Hshiung Tzeng. "Compromise solution by MCDM methods: A comparative analysis of VIKOR and TOPSIS." *European journal of operational research* 156, no. 2 (2004): 445-455.

Orlikowski, Wanda J., and C. Suzanne Iacono. "Research commentary: Desperately seeking the "IT" in IT research—A call to theorizing the IT artifact." *Information systems research*12, no. 2 (2001): 121-134.

Orlikowski, Wanda J., and Jack J. Baroudi. "Studying information technology in organizations: Research approaches and assumptions." *Information systems research* 2, no. 1 (1991): 1-28.

Osaka, Kyosuke, Tsuyoshi Takagi, Kenichi Yamazaki, and Osamu Takahashi. "An efficient and secure RFID security method with ownership transfer." In *RFID security*, pp. 147-176. Springer, Boston, MA, 2008.

Otto, James R., and Q. B. Chung. "A framework for cyber-enhanced retailing: Integrating e-commerce retailing with brick-and-mortar retailing." *Electronic Markets* 10, no. 3 (2000): 185-191..

Pannucci, Christopher J., and Edwin G. Wilkins. "Identifying and avoiding bias in research." *Plastic and reconstructive surgery* 126, no. 2 (2010): 619.

Pardal, Miguel L., Mark Harrison, Sanjay Sarma, and José Alves Marques. "Expressive RFID data access policies for the Pharmaceuticals supply chain." In *RFID (RFID), 2013 IEEE International Conference on*, pp. 199-206. IEEE, 2013.

Parent, William A. "Privacy, morality, and the law." In *Privacy*, pp. 105-124. Routledge, 2017.

Paret, Dominique. *RFID and contactless smart card applications*. John Wiley & Sons, 2005.

Partovi, Fariborz Y. "Determining what to benchmark: an analytic hierarchy process approach." *International Journal of Operations & Production Management* 14, no. 6 (1994): 25-39.

Pather, Shaun, and Dan Remenyi. "Some of the philosophical issues underpinning research in information systems: from positivism to critical realism." In *Proceedings of the 2004 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries*, pp. 141-146. South African Institute for Computer Scientists and Information Technologists, 2004.

Peiris, K. Dharini Amitha, Jin Jung, and R. Brent Gallupe. "Building and evaluating ESET: A tool for assessing the support given by an enterprise system to supply chain management." *Decision Support Systems* 77 (2015): 41-54.

Peretz, Hilla, and Zehava Rosenblatt. "The role of societal cultural practices in organizational investment in training: A comparative study in 21 countries." *Journal of Cross-Cultural Psychology* 42, no. 5 (2011): 817-831.

Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., & Ribagorda, A. (2006, September). RFID systems: A survey on security threats and proposed solutions. In *IFIP*

international conference on personal wireless communications (pp. 159-170). Springer, Berlin, Heidelberg.

Pervan, Graham P. "The measurement of GSS effectiveness: A meta-analysis of the literature and recommendations for future GSS research." In *HICSS (4)*, pp. 562-571. 1994.

Petronio, Sandra. *Boundaries of privacy: Dialectics of disclosure*. Suny Press, 2012.

Pfeiffer, Daniel, and Bjorn Niehaves. "Evaluation of conceptual models-a structuralist approach." *ECIS 2005 Proceedings*(2005): 43.

Pfeiffer, J. "Seven practices of successful organizations." *California Management Review* 40, no. 2 (1998): 96-124.

Pharmaceutical Commerce (May 16, 2017). Pharmaceutical cold chain logistics is a $13.4-billion global industry [ONLINE] Available at: http://pharmaceuticalcommerce.com/supply-chain-logistics/pharmaceutical-cold-chain-logistics-13-4-billion-global-industry/. [Accessed 15 June 2017].

Phillips, Denis Charles, and Nicholas C. Burbules. *Postpositivism and educational research*. Rowman & Littlefield, 2000.

Phillips, Ted, Tom Karygiannis, and Rick Kuhn. "Security standards for the RFID market." *IEEE Security & Privacy* 3, no. 6 (2005): 85-89.

Piikivi, Lauri. "Wireless communication device providing a contactless interface for a smart card reader." U.S. Patent 6,776,339, issued August 17, 2004.

Piramuthu, Selwyn, and Robin Doss. "On sensor-based solutions for simultaneous presence of multiple RFID tags." *Decision Support Systems* 95 (2017): 102-109.

Pirkey, W. (2015, May 6). Personal Interview.

Podsakoff, Philip M., Scott B. MacKenzie, Jeong-Yeon Lee, and Nathan P. Podsakoff. "Common method biases in behavioral research: A critical review of the literature and recommended remedies." *Journal of applied psychology* 88, no. 5 (2003): 879.

Poirier, Charles C., and Duncan McCollum. *RFID strategic implementation and ROI: a practical roadmap to success*. J. Ross Publishing, 2006.

Poll Everywhere. [ONLINE] Available at: https://pollev.com/ [Accessed 17 July 2016].

Poluha, Rolf G. *Application of the SCOR model in supply chain management*. Cambria Press, 2007.

Pourghasemi, Hamid Reza, Biswajeet Pradhan, and Candan Gokceoglu. "Application of fuzzy logic and analytical hierarchy process (AHP) to landslide susceptibility mapping at Haraz watershed, Iran." *Natural hazards* 63, no. 2 (2012): 965-996.

Pries-Heje, Jan, Richard Baskerville, and John R. Venable. "Strategies for Design Science Research Evaluation." In *ECIS*, pp. 255-266. 2008.

Qu, Xiuli, LaKausha T. Simpson, and Paul Stanfield. "A model for quantifying the value of RFID-enabled equipment tracking in hospitals." *Advanced Engineering Informatics* 25, no. 1 (2011): 23-31.

Rabin, Matthew, and Joel L. Schrag. "First impressions matter: A model of confirmatory bias." *The Quarterly Journal of Economics* 114, no. 1 (1999): 37-82.

Rachels, James. "Why privacy is important." In *Privacy*, pp. 11-21. Routledge, 2017.

Raju, P. V. S. N., and Pritee Parwekar. "DNA encryption based dual server password authentication." In *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014*, pp. 29-37. Springer, Cham, 2015.
Ramanathan, Ramakrishnan, Usha Ramanathan, and Lok Wan Lorraine Ko. "Adoption of RFID technologies in UK logistics: Moderating roles of size, barcode experience and government support." *Expert Systems with Applications* 41, no. 1 (2014): 230-236.

Raven, Gregory A., Jason Harrigan, Rene Martinez, Pavel Nikitin, Shashidhar Ramamurthy, David William Gilpin, and Stephen Kelly. "RFID tag with anti-tamper assembly." U.S. Patent 9,542,637, issued January 10, 2017.
Responsible Jewellery Council (n.d.). [ONLINE] Available at: http://www.responsiblejewellery.com. [Accessed 18 January 2017].

RFID Journal (n.d.) FAQ [ONLINE] Available at: www.rfidjournal.com/faq/16. [Accessed 18 January 2017].

RFID Today (n.d.) RFID compliance problems. [ONLINE] Available at: http://www.rfidtoday.co.uk/articles/rfid_compliance.htm. [Accessed 30 October 2011].

RFID Tribe. "*Where the World's RFID Community Shares Ideas"* 2005. Accessed January 21, 2012. http://www.RFIDTribe.org.

RFID Update. The Potential for RFID in Pharmaceuticals. [ONLINE] Available at: http://www.rfidupdate.com/articles/index.php?id=1195. [Accessed 25 July 2018].

Richardson, Dena. "Increasing Supply Chain Security: The Requirement for RFID Technology on Containerized Cargo [graduate project]." (2017).

Rieback, Melanie R., Bruno Crispo, and Andrew S. Tanenbaum. "RFID Guardian: A battery-powered mobile device for RFID privacy management." In *Australasian Conference on Information Security and Privacy*, pp. 184-194. Springer, Berlin, Heidelberg, 2005.

Riley, Michael and Walcott, John. (2018). *China-Based Hacking of 760 Companies Shows Cyber Cold War - Bloomberg*. [ONLINE] Available at: https://www.bloomberg.com/news/articles/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war. [Accessed 30 June 2018].

Rittel, H. W. J., and M. M. Webber. "Planning problems are wicked problems. N. Cross (Ed.). Developments in Design Methodology (pp. 135-144)." (1984).

Rodríguez, Ricardo J. "Evolution and characterization of point-of-sale RAM scraping malware." *Journal of Computer Virology and Hacking Techniques* 13, no. 3 (2017): 179-192.

Rosenbaum, Paul R., and Donald B. Rubin. "Reducing bias in observational studies using subclassification on the propensity score." *Journal of the American statistical Association* 79, no. 387 (1984): 516-524.

Rosenbloom, Joshua L. "Academic Appointments." *Journal of Human Resources* 34, no. 3 (1999): 449-74.

Rotter, P. (2008). A framework for assessing RFID system security and privacy risks. *IEEE Pervasive Computing*, (2), 70-77.

Ruhm, Karl H. (2004). Cause and Effect Diagram, Internet Portal Measurement Science and Technology. [ONLINE] Available at: http://www.mmm.ethz.ch/dok01/d0000538.pdf

[Accessed 4 September 2017].

Russell, James S., James R. Terborg, and Mary L. Powers. "Organizational performance and organizational level training and support." *Personnel psychology* 38, no. 4 (1985): 849-863.

Saaty, Thomas. "The analytical hierarchy process (AHP)." (1980). New York, USA: McGraw Hill

Saaty, Thomas L. "An exposition of the AHP in reply to the paper "remarks on the analytic hierarchy process"." *Management science* 36, no. 3 (1990): 259-268.

Saaty, Thomas L. "Decision making with the analytic hierarchy process." *International journal of services sciences* 1, no. 1 (2008): 83-98.

Saaty, Thomas L. "Priority setting in complex problems." *IEEE Transactions on Engineering Management* 3 (1983): 140-155.

Saaty, Thomas Lorie, and Luis Gonzalez Vargas. *Prediction, projection, and forecasting: applications of the analytic hierarchy process in economics, finance, politics, games, and sports*. Kluwer Academic Pub, 1991.

Sarma, Sanjay E., Stephen A. Weis, and Daniel W. Engels. "RFID systems and security and privacy implications." In *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 454-469. Springer, Berlin, Heidelberg, 2002.
Sarniak, Rebecca (2017). *Nine types of research bias and how to avoid them | Quirks.com*. [ONLINE] Available at: https://www.quirks.com/articles/9-types-of-research-bias-and-how-to-avoid-them. [Accessed 30 October 2017].

Saunders, Mark, Philip Lewis, and Adrian Thornhill. *Research methods for business students*. Pearson education, 2009.

Scherhäufl, Martin, Markus Pichler, and Andreas Stelzer. "UHF RFID localization based on phase evaluation of passive tag arrays." *IEEE Transactions on Instrumentation and Measurement* 64, no. 4 (2015): 913-922.

Schipmann, Christin, and Matin Qaim. "Supply chain differentiation, contract agriculture, and farmers' marketing preferences: The case of sweet pepper in Thailand." *Food Policy* 36, no. 5 (2011): 667-677.

Schmitt, Amanda J., and Mahender Singh. "A quantitative analysis of disruption risk in a multi-echelon supply chain." *International Journal of Production Economics* 139, no. 1 (2012): 22-32.

Security Magazine (2015). Cargo Theft Declines in 2014 Average Value Increases, [ONLINE] Available at: https://www.securitymagazine.com/articles/86214-cargo-theft-declines-in-2014-average-value-increases. [Accessed 03 June 2018].

Security Park (2010). SecurityPark.Net. [ONLINE] Available at: http://www.securitypark.co.uk/security_article263553.html. [Accessed 20 October 2010].

Sell, Supply Produce Distribute. "Introduction to supply chain management." (1999).

Sevkli, Mehmet, S. C. Lenny Koh, Selim Zaim, Mehmet Demirbag, and Ekrem Tatoglu. "Hybrid analytical hierarchy process model for supplier selection." *Industrial Management & Data Systems* 108, no. 1 (2008): 122-142.

Shahin, Ashraf A. "Polymorphic worms collection in cloud computing." *arXiv preprint arXiv:1409.1654* (2014).

Shin, Kwang Cheol, Seung Bo Park, and Geun Sik Jo. "Enhanced TDMA based anti-collision algorithm with a dynamic frame size adjustment strategy for mobile RFID readers." *Sensors* 9, no. 2 (2009): 845-858.

Siau, Keng, and Matti Rossi. "Evaluation techniques for systems analysis and design modelling methods–a review and comparative analysis." *Information Systems Journal* 21, no. 3 (2011): 249-268.

Siewiorek, Daniel, and Robert Swarz. *Reliable Computer Systems: Design and Evaluatuion*. Digital Press, 2017.

Silberschneider, Roman, Thomas Korak, and Michael Hutter. "Access without permission: A practical RFID relay attack." In *Proc. 21st Austrian Workshop Microelectronics*, vol. 10, pp. 59-64. 2013.

Simchi-Levi, David, Philip Kaminsky, Edith Simchi-Levi, and Ravi Shankar. *Designing and managing the supply chain: concepts, strategies and case studies*. Tata McGraw-Hill Education, 2008.

Simon, H. A. "The science of design." *The Sciences of the Artificial* (1981): 129-60.

Simon, Herbert A. *The sciences of the artificial*. MIT press, 1996.

Sorensen, Herb. *Inside the mind of the shopper: The science of retailing*. FT Press, 2016.

Stahl, Bernd Carsten, and Carole Brooke. "The contribution of critical is research." *Communications of the ACM* 51, no. 3 (2008): 51-55.

Stake, Robert E. *The art of case study research*. Sage, 1995.

Stake, Robert E. *Multiple case study analysis*. Guilford Press, 2013.

Statista. Largest Jewellery Markets by Country. [ONLINE] Available at: https://www.statista.com/statistics/718856/largest-jewelry-markets-by-country/. [Accessed 03 July 2018].

Stewart, David W., and Prem N. Shamdasani. *Focus groups: Theory and practice*. Vol. 20. Sage publications, 2014.

Stewin, Patrick, and Iurii Bystrov. "Understanding DMA malware." In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pp. 21-41. Springer, Berlin, Heidelberg, 2012.

Stübing, Hagen. *Multilayered security and privacy protection in Car-to-X networks: solutions from application down to physical layer*. Springer Science & Business Media, 2013.

Su, Hsin-Lung, Hong-Sheng Huang, and Sung-Lin Chen. "An ellipse-shaped with slanted slot circularly polarized monopole antenna for UHF RFID readers." In *Antennas and Propagation & USNC/URSI National Radio Science Meeting, 2017 IEEE International Symposium on*, pp. 2443-2444. IEEE, 2017.

Suneetha, S., and B. Megharaj. "Elements of Japanese Value Delivery Process in Providing Customer Value-with Special Focus on Jewellery Customers of Hyderabad & Secunderabad." *International Journal of Research in Finance and Marketing* 6, no. 10 (2016): 111-124.

Supply Chain Council (2008). SCOR 9.0 Overview Booklet

Supply Chain Council (2011). [ONLINE] Available at: http://supply-chain.org/. [Accessed 15 February 2011].

Swaminathan, Jayashankar M., Stephen F. Smith, and Norman M. Sadeh. "Modeling supply chain dynamics: A multiagent approach." *Decision sciences* 29, no. 3 (1998): 607-632.
Swedberg, Claire. (Jun 05, 2006) Wal-Mart Canada Plans Its First RFID Pilot. *RFID Journal.* [ONLINE] Available at: http://www.rfidjournal.com/article/articleview/2390/ [Accessed 30 October 2011].

Sweeney, Latanya. "k-anonymity: A model for protecting privacy." *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10, no. 05 (2002): 557-570.

Symantec (2013). Internet security threat report 2013 [Moutain View, USA].

Taghaboni-Dutta, Fataneh, and Betty Velthouse. "RFID technology is revolutionary: who should be involved in this game of tag?." *academy of Management perspectives* 20, no. 4 (2006): 65-78.

Tague, N. R. "The quality toolbox, 2nd edn., American Society for Quality." (2005).

TeskaLabs. "*Understanding the Importance and Value of Backend Security · TeskaLabs Blog."* 2016 Accessed January 22, 2018. https://teskalabs.com/blog/backend-security-importance.
The Council of Logistics Management. "*Logistics Definition"* 2018 Accessed January 25, 2018. http://www.clm1.org/.

The Economist. "Li & Fung: Optimising Supply Chain for Other Companies" May 31, 2001. Accessed April 2, 2018.
http://bear.warrington.ufl.edu/kraft/MLI26C653/docs/08_LiAndFung.pdf

The Law Dictionary. "*Black's Law Dictionary - Free Online Legal Dictionary"* 2018 Accessed January 25, 2018. http://www.Thelawdictionary.org.

The United States Department of Defense. 2010. *U.S. Department of Defense Vulnerability*. [ONLINE] Available at: https://www.defense.gov/. [Accessed 25 January 2018].

Thomas, Kenneth W., and Betty A. Velthouse. "Cognitive elements of empowerment: An “interpretive” model of intrinsic task motivation." *Academy of management review* 15, no. 4 (1990): 666-681.

Thompson, Dennis M. "Using AHP to allocate contract incentives." *AACE International Transactions* 1994 (1994): DCL7-1.

Thompson, Edmund R. "Clustering of foreign direct investment and enhanced technology transfer: evidence from Hong Kong garment firms in China." *World Development* 30, no. 5 (2002): 873-889.

Thurstone, Louis L. "A law of comparative judgment." *Psychological review* 34, no. 4 (1927): 273.

Toulmin, Stephen E. *The uses of argument*. Cambridge university press, 2003.

Tsai, Janice Y., Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. "The effect of online privacy information on purchasing behavior: An experimental study." *Information Systems Research* 22, no. 2 (2011): 254-268.

Tsiakis, Panagiotis, Nilay Shah, and Constantinos C. Pantelides. "Design of multi-echelon supply chain networks under demand uncertainty." *Industrial & Engineering Chemistry Research* 40, no. 16 (2001): 3585-3604.

Turati, Pietro, Nicola Pedroni, and Enrico Zio. "Knowledge‐driven System Simulation for Scenario Analysis in Risk Assessment." *Knowledge in Risk Assessment and Management* (2018): 165-219.

Turban, Efraim, Jon Outland, David King, Jae Kyu Lee, Ting-Peng Liang, and Deborrah C. Turban. "Order Fulfillment Along the Supply Chain in e-Commerce." In *Electronic Commerce 2018*, pp. 501-534. Springer, Cham, 2018.

Tu, Yuju, and Selwyn Piramuthu. "Lightweight non-distance-bounding means to address RFID relay attacks." *Decision Support Systems* 102 (2017): 12-21.

Umble, Elisabeth J., Ronald R. Haft, and M. Michael Umble. "Enterprise resource planning: Implementation procedures and critical success factors." *European journal of operational research* 146, no. 2 (2003): 241-257.

U.S. Air Force Software Protection Initiative. (2010). The Three Tenents of Cyber Security, [ONLINE] Available at: http://www.spi.dod.mil/tenets.htm, [Accessed 24 October 2010)].

Ustundag, Alp, and Mehmet Tanyas. "The impacts of radio frequency identification (RFID) technology on supply chain costs." *Transportation Research Part E: Logistics and Transportation Review* 45, no. 1 (2009): 29-38.

Van Den Haag, Ernest. "On privacy." In *Privacy and Personality*, pp. 149-168. Routledge, 2017.

Van Eemeren, Frans H., Rob Grootendorst, and Frans Hendrik Eemeren. *A systematic theory of argumentation: The pragma-dialectical approach*. Vol. 14. Cambridge University Press, 2004.

Vaney, Neelam, Abhinav Dixit, Tandra Ghosh, Ravi Gupta, and M. S. Bhatia. "Habituation of event related potentials: a tool for assessment of cognition in headache patients."

Vargas, Luis G. "An overview of the analytic hierarchy process and its applications." *European journal of operational research*48, no. 1 (1990): 2-8.

Vassallo, Carmine, Sebastiano Panichella, Fabio Palomba, Sebastian Proksch, Andy Zaidman, and Harald C. Gall. "Context is king: The developer perspective on the usage of static analysis tools." In *2018 IEEE 25th International Conference on Software Analysis, Evolution and Reengineering (SANER)*, pp. 38-49. IEEE, 2018.

Venable, John. "The role of theory and theorising in design science research." In *Proceedings of the 1st International Conference on Design Science in Information Systems and Technology (DESRIST 2006)*, pp. 1-18. 2006.

Venable, John R. "Design science research post hevner et al.: criteria, standards, guidelines, and expectations." In *International Conference on Design Science Research in Information Systems*, pp. 109-123. Springer, Berlin, Heidelberg, 2010.

Venkatesh, Viswanath, Michael G. Morris, Gordon B. Davis, and Fred D. Davis. "User acceptance of information technology: Toward a unified view." *MIS quarterly* (2003): 425-478.

Veyrat, Pierre (2016). Business process improvement. [ONLINE] Available at: https://www.heflo.com/blog/process-optimization/business-process-improvement-definition/ [Accessed 04 May 2018].

Veyrat, Pierre (2017). Employee Termination Process. [ONLINE] Available at: https://www.heflo.com/blog/hr/employee-termination-process-flow-chart/ [Accessed 04 May 2018].

Voss, C. Tsikriktsis. "N. & Frohlich, M." *Case research in operations management* 22, no. 2 (2002): 195-219.

Walls, Joseph G., George R. Widmeyer, and Omar A. El Sawy. "Building an information system design theory for vigilant EIS." *Information systems research* 3, no. 1 (1992): 36-59.

Walsham, Geoff. "Interpretive case studies in IS research: nature and method." *European Journal of information systems*4, no. 2 (1995): 74-81.

Wang, Ge, Samuel H. Huang, and John P. Dismukes. "Product-driven supply chain selection using integrated multi-criteria decision-making methodology." *International journal of production economics* 91, no. 1 (2004): 1-15.

Wang, Liang, Tao Gu, Xianping Tao, and Jian Lu. "Toward a wearable RFID system for real-time activity recognition using radio patterns." *IEEE Transactions on Mobile Computing* 16, no. 1 (2017): 228-242.

Wang, S-J., W-L. Wang, C-T. Huang, and S-C. Chen. "Improving inventory effectiveness in RFID-enabled global supply chain with Grey forecasting model." *The Journal of Strategic Information Systems* 20, no. 3 (2011): 307-322.

Ward, Mark (15 March 2006). Viruses leap to smart radio tags. [ONLINE] Available at: http://news.bbc.co.uk/2/hi/technology/4810576.stm [Accessed 30 October 2011)].

Warren, Carol, and Barbara Laslett. "Privacy and secrecy: A conceptual comparison." *Journal of Social Issues* 33, no. 3 (1977): 43-51.

Watson, Greg. "The legacy of Ishikawa." *Quality Progress* 37, no. 4 (2004): 54.

Watson, Michael R., Angelos K. Marnerides, Andreas Mauthe, and David Hutchison. "Towards a distributed, self-organising approach to malware detection in cloud computing." In *International Workshop on Self-Organizing Systems*, pp. 182-185. Springer, Berlin, Heidelberg, 2013.

Weber, Ron. "Toward a theory of artifacts: a paradigmatic base for information systems research." *Journal of Information Systems* 1, no. 2 (1987): 3-19.

Wei, Fu, and Ma Jianguo. "Erratum: Study of the passive microwave RFID tag range using distance‐dependent reflection coefficient over multipath channel." *Microwave and Optical Technology Letters* 51, no. 12 (2009): 3029-3029.

Wei, Fu, and Ma Jianguo. "Study of the passive microwave RFID tag range using distance‐dependent reflection coefficient over multipath channel." *Microwave and Optical Technology Letters* 51, no. 10 (2009): 2266-2268.

Weir, Bruce S. *Genetic data analysis. Methods for discrete population genetic data*. Sinauer Associates, Inc. Publishers, 1990.

Westin, Alan F., and Oscar M. Ruebhausen. *Privacy and freedom*. Vol. 1. New York: Atheneum, 1967.

Westin, Alan F. "Privacy and freedom, atheneum." *New York* 7 (1967).
Whang, Seungjin. "Timing of RFID adoption in a supply chain." *Management Science* 56, no. 2 (2010): 343-355.

White, Andrew A., Seth W. Wright, Roberto Blanco, Brent Lemonds, Janice Sisco, Sandy Bledsoe, Cindy Irwin, Jennifer Isenhour, and James W. Pichert. "Cause‐and‐effect analysis of risk management files to assess patient care in the emergency department." *Academic Emergency Medicine* 11, no. 10 (2004): 1035-1041.

Williams, Jeffrey, and Arshan Dabirsiaghi. "Method and system of attack detection and protection in computer systems." U.S. Patent Application 15/294,728, filed May 18, 2017.

Wong, Kam Cheong. "Using an Ishikawa diagram as a tool to assist memory and retrieval of relevant medical cases from the medical literature." (2011): 120.

Wonglimpiyarat, Jarunee. "The pursuit of original equipment manufacturer strategy: insights from an Asian country." *R&D Management* 48, no. 2 (2018): 243-252.

Workman, Daniel. (2018). China's Top Trading Partners, World's Top Exports. [ONLINE] Available at: http://www.worldstopexports.com/chinas-top-import-partners/. [Accessed 04 June 2018].

World Atlas. Countries with the Biggest Global Pharmaceutical Markets in the World [ONLINE] Available at: https://www.worldatlas.com/articles/countries-with-the-biggest-global-pharmaceutical-markets-in-the-world.html. [Accessed 03 July 2018].

Wreden. From OEM to OBM: Crossing The Chasm. [ONLINE] Available at: www.fusionbrand.com. [Accessed 21 September 2010].

Wueest, Candid. "Security for virtualization: finding the right balance." *Kaspersky Lab* (2012).

Xinhua (2015). Proposals of the Central Committee of the Communist Party of China on the 13th Five-Year Plan for National Economic and Social Development, adopted by the Fifth Plenary Session of the 18th Central Committee of the CCP, 29 October 2015. [ONLINE] Available at: http://news.xinhuanet.com/fortune/2015-11/03/c_1117027676.htm. [Accessed 2 December 2015].

Yin, Robert K. "Case Study Research. Design and Methods,(2. utg.)." (1994).

Yoon, Kwangsun. "A reconciliation among discrete compromise solutions." *Journal of the Operational Research Society* 38, no. 3 (1987): 277-286.

Yu, Fang, Yongsheng Yang, and Daofang Chang. "A Complex Negotiation Model for Multi-Echelon Supply Chain Networks." *IEEE Transactions on Engineering Management* (2018).

Yu, Po-Lung. "A class of solutions for group decision problems." *Management Science* 19, no. 8 (1973): 936-946.

Zalud, Bill. (Apr 01, 2016) The Daily Challenges of Supply Chain Security. *Security Solutions for Enabling and Assuring Business* [ONLINE] Available at: https://www.securitymagazine.com/articles/87010-the-daily-challenges-of-supply-chain-security. [Accessed 03 June 2016].

Zeleny, Milan, and James L. Cochrane. *Multiple criteria decision making*. University of South Carolina Press, 1973.

Zhang, Li, Song Wang, Fachao Li, Hong Wang, Li Wang, and Wenan Tan. "A few measures for ensuring supply chain quality." *International Journal of Production Research* 49, no. 1 (2011): 87-97.

Zhao, Chun Hua, Jin Zhang, Xian You Zhong, Jia Zeng, and Shi Jun Chen. "analysis of accident safety risk of tower crane based on fishbone diagram and the Analytic Hierarchy Process." In *Applied Mechanics and Materials*, vol. 127, pp. 139-143. Trans Tech Publications, 2012.

Zheng, Lijuan, Yujuan Xue, Linhao Zhang, and Rui Zhang. "Mutual Authentication Protocol for RFID Based on ECC." In *Computational Science and Engineering (CSE) and Embedded and Ubiquitous Computing (EUC), 2017 IEEE International Conference on*, vol. 2, pp. 320-323. IEEE, 2017.

Zumsteg, Philip, and Huyu Qu. "Reading RFID tags in defined spatial locations." U.S. Patent 9,892,289, issued February 13, 2018.