Increasing Supply Chain Security:
The Requirement for RFID Technology on Containerized Cargo

By

Dena Richardson

Submitted in partial fulfillment of the requirements for the degree of

Master of Marine Management

at

Dalhousie University

Halifax, Nova Scotia

April 2017

Contents

List of Figures

List of Abbreviations

Article Number Association (ANA)

Authorized Economic Operators (AEOs)

Canada Border Services Agency (CBSA)

Canadian Marine Transportation Security Regulations (MTSR)

Cargo transport units (CTU)

Container Control program (CCP)

Customs-Trade Partnership against Terrorism (C-TPAT)

European Article Numbering (EAN)

International Civil Aviation Organization (ICAO)

International Criminal Police Organization (INTERPOL)

International Maritime Organization (IMO)

International Organization for Standardization (ISO)

International Ship and Port Facility Security Code (ISPS)

Machine Readable Travel Document (MRTD)

Non-Intrusive Inspection (NII)

Partners in Protection (PIP)

Radio Frequency Identification (RFID)

Return on Investment (ROI)

International Convention for the Safety of Life at Sea (SOLAS), 1974 (SOLAS)

United Nations Economic Commission for Europe (UNECE)

United States Department of Defense (USDOD)

World Customs Organization (WCO)

Containerized Twenty Foot Equivalent (TEU)

Acknowledgements

I would like to thank my supervisor, Dr. Moira L. McConnell, Professor Emerita (Law) for her support, guidance and patience throughout this past year. The expertise provided was crucial to the development of this Graduate Project. I would also like to say thank you to Eric Macham for agreeing to be the second reader. Also, it is necessary to thank Jessica Macintosh for her help in editing the final version of this Graduate Project.

To my colleagues at Transport Canada and the Canadian Coast Guard, thank you for your support and continuous understanding, particularly during semesters spent running between the classroom and the office. Thank you also, for often taking the time to offer me feedback and encouragement when it was much needed.

It is also very important for me to take the time to acknowledge Becky Field. Becky, in my opinion, is the reason the Marine Affairs Program is a success. Her determination, strong nudging, and countless 'talks' pushed me to continue my studies to reach this milestone. I will be forever grateful.

Most importantly, there are no words to express the gratitude I have for my family. Mom and Dad, thank you for coming to my rescue more times than I can count, knowing that I could rely on you to help care for Jack while I spent hours in the basement writing papers, alleviated most of the guilt. Additionally, I would like to recognize the love and support of my husband John. Thank you for your constant encouragement, support and love. Finally, I have to thank my little boy, Jack. I know it wasn't always easy, but I hope one day you will truly understand how much you inspired me to start and finish this journey.

Abstract

International shipping or transportation of goods, other than bulk cargo, such as petroleum products or LNG, is carried out almost entirely using cargo containers and through various modes including surface and marine. Establishing supply chain security of these containers through the various modes is essential to protecting not only the cargo that being shipped and the transportation systems involved but also the wider public security. Even though measures have been introduced to increase the level of protection in place to promote cargo and supply chain security, tampering and pilferage still take place. The potential for tampering with cargo in containers puts industry, the marine transportation system and the public at risk. Currently shippers using containers for international transportation employ various methods to ensure security of containers including “seals” however there is no single or universal standard employed. The use of Radio Frequency Identification (RFID) seals is a proven security feature that has already been put into use by various industries globally. This study suggests that RFID technology can be incorporated into the container seals to strengthen supply chain security and by extension the marine transportation system and provide greater protection to the public. Further, the technology has the potential to aid industry both logistically and financially by improving efficiencies associated with the tracking and monitoring of containerized cargo. The success of such implementation is entirely dependent on the ability of organizations and industry to work together to ensure a robust framework and policy design.

Keywords: Radio Frequency Identification, RFID, Container, Seal, Cargo, Supply Chain, Security, Customs, Trade, Globalization, Shipping, Stakeholder engagement, Logistics, Maritime, Regulations, International Maritime Organization, IMO, International Standards Organization, ISO, Active, Passive, Marine Transportation Security.

Chapter One

1.1 Introduction

International transport of goods is carried out almost entirely by means of container shipment through various modes including surface and marine. This research focuses mainly on the marine transportation mode and legislation that is specific to maritime security and trade.

Establishing supply chain security through the various modes is essential to protecting not only the cargo being shipped and the transportation systems involved but also the public. The use of containers for the covert international movement and importation of explosives, migrants, incendiaries, weapons or contraband at any point in shipping could potentially cause extreme harm if gone undetected. As noted above this project focuses mainly on the marine mode of transportation but it also outlines how the shipment of cargo via this mode is multimodal and interconnected with others.

The Canadian Marine Transportation Security Regulations (MTSR)[1] and the International Ship and Port Facility Security Code (ISPS)[2] both contain sections that are devoted entirely to the handling of cargo. The MTSR and the ISPS code both indicate that security measures have to be in place for both vessels and facilities that should prevent the tampering of cargo. However, neither the MTSR nor the ISPS code is prescriptive in detailing how this is to be facilitated. A container seal is one method that is used to assist in the prevention and detection of tampering. It should be noted that

[1] For more information on the MTSR, see http://laws-lois.justice.gc.ca/eng/regulations/SOR-2004-144/

[2] For more information on the ISPS Code, see http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

there are some methods and accepted practices in place that will be further examined in this project but it is important to highlight that there is no internationally accepted standard for container seals.

Even though mechanical[3] container seals have been used for many years, to date, an international standard has not been accepted. This lack of a standard has been recognized and noted by many entities, including the International Maritime Organization (IMO), as a vulnerability to supply chain security. This project examines the feasibility and utility in adopting or developing an international standard for container seals, and in particular an ISO standard employing the use of Radio Frequency Identification (RFID) seals, to strengthen supply chain security and by extension the marine transportation system. This project will also demonstrate how the use of RFID technology can benefit industry both logistically and financially by improving efficiencies associated with the tracking and monitoring of containerized cargo.

This project will also examine various organizations that have regional and national arrangements with Canada in order to further understand how Canada could implement an ISO standard that requires the use of RFID technology.

A basic internet search of the phrase “shipping container seal” will immediately produce hundreds of results that lead to companies who sell various types, makes and models of container seals that can be used on cargo transport units (CTU) that is, containers.

[3] A mechanical seal is a device marked with a unique identifier and usually designed for a single use, which is externally affixed to the container doors and designed to evidence tampering or intrusion through the doors of a container and to secure closed doors of a container. Depending on its design and construction, the seal provides varying degrees of resistance to an intentional or unintentional attempt to open it or to enter the freight container through the container doors. Seals need to be designed and constructed so that tamper attempts create and leave evidence of that tampering. All grades and types of seals require inspection to indicate whether tampering has occurred or entry has been attempted. Retrieved from: https://www.iso.org/obp/ui/#iso:std:iso:17712:ed-2:v1:en

This is ultimately the problem. The existence of so many products makes it nearly impossible to establish a standard method of detection of tampering. This problem has been recognized by industry and government for some time but even more so since the events of September 11th, 2001 in the United States. The 9/11 attacks triggered the IMO to develop the ISPS code under the auspices of the International Convention for the Safety of Life at Sea, 1974 (SOLAS) to be used to increase global maritime security. With the onset of the ISPS code, cargo handling and security, which are essential to world trade, were prioritized, and many measures have been put in place since to assist in supply chain security. The exception is an international legal standard for container seals.

The anticipated findings of this project may afford industry, regulators and other officials an opportunity to implement a security related technical standard for a seal that could assist in the prevention and detection of tampering with containers in coordination with other efforts for the purpose of protecting cargo, the integrity of the transportation system and the public and by keeping a large vulnerability from being exploited all whilst improving industry efficiencies that may provide financial gains.

1.2 Multimodal Shipment of Containerized Cargo

Throughout the course of history, cargo has been shipped internationally by various modes and methods. The development of crates, pallets and vessel holds created a method to transport goods more efficiently, however the increase in the volume of goods coupled with the lack of a standard means of shipment presented logistical difficulties and time constraints that inevitably created additional costs to the shippers

and in turn, to the consumer. Research indicates that the requirement for a standard in shipping became increasingly apparent to not only provide consistency, but to improve overall efficiencies related to the industry. This requirement for a standard led to the development of the Containerized Twenty Foot Equivalent (TEU) which is the basis for standard cargo container measurement.

The TEU is an inexact unit of cargo often used to describe the capacity of container ships and container terminals. It is based on the volume of a 20 foot long intermodal container, a standard sized metal box which can be easily transferred between different modes of transportation, such as ships, trains and trucks.[4] The introduction of the TEU has undoubtedly impacted the evolution of intermodal cargo shipment. Unfortunately, the standard TEU design has not evolved to make security a primary goal.

It is without question, that containerization has had the largest impact on intermodal transportation by increasing efficiencies and lowering transportation costs. It is also remarkable that shipping by means of a standard container essentially means that cargo can be shipped virtually everywhere from anywhere in the world. “In spite of serious reservations about its potential when it was introduced in the 1960s, no other technical improvement has contributed more to the process of globalization than the container” ([1]Rodrigue & Notteboom, 2009,). Industry has adapted to accept this standard to allow for the effective multimodal transhipment of goods from basically any location in to world to another.

[4] For more information on the twenty-foot equivalent unit (TEU), see http://www.businessdictionary.com/definition/twenty-foot-equivalent-unit-TEU.html

Figure 1 TEU Container. (Source: http://www.dimensionsinfo.com/wp-content/uploads/2010/01/20ft-Container.jpg)

Multimodal freight transportation is defined as the transportation of goods by a sequence of at least two different modes of transportation (UNECE, 2009). In most cases, containerized cargo is generally shipped by at least three methods of transportation from its point of origin to its final destination. This includes trucks, container ships and trains. A transportation chain is basically partitioned into three segments: pre-haul (or first mile for the pickup process), long-haul (door-to-door transit of containers), and end-haul (or last mile for the delivery process). In most cases, the pre-haul and end-haul transportation is carried out via road, but for the long-haul transportation, road, rail, air and water modes can be considered (SteadieSeifi et al., 2014).

It is fair to state that globalization and world wide access to information and products has contributed significantly to the increase in consumer demand, and by extension, multimodal transshipment of cargo and goods. New markets, coupled with the onset of

more trade agreements coincide with new shipping routes, canal expansions and super post Panamax sized container vessels. The rate of multimodal transhipment of freight increases annually by about fifteen percent. In 2010 about 45.8% of total freight transportation in European Union countries were transported via road, 36.9% via sea, around 10.2% via rail, and 3.8% via inland waterways (SteadieSeifi et al., 2014).

Canada has also witnessed considerable increases in the amount of containerized cargo being exported, in recent years. The tonnage and volume of international container traffic handled at Canadian ports rose in 2011. “While the tonnage rose 5.1% to 40.6Mt from 38.7Mt, the volume of containers increased marginally by 0.8% to 4.6 million TEUs from 4.5 million TEUs in 2010. The main driver behind the overall growth was increased two-way trade with China. The largest increases in both the tonnage (up 1.0Mt) and volume (up 63,738 TEUs) of international containerized cargo were registered at the port of Prince Rupert. However, Port Metro Vancouver continues to handle the majority (53%) of the country's international containerized cargo tonnage”. (Statistics Canada, 2015)

It is important to note, that even though measures have been introduced to increase the protection in place to promote cargo and supply chain security, tampering and pilferage still take place that put industry, the marine transportation system and the public at risk. As shipping becomes increasing prevalent in a world where trade has minimal boundaries as a result of globalization, industry continues to produce ships of monumental sizes to increase cargo capacity. “Shipping lines have significantly increased average vessel sizes from around 4500 TEU in 2000 to over 7500 TEU in early 2010” (Ducruet & Notteboom, 2012, p. 4). To provide context, Post-Panamax

vessels, developed to transit through the updated Panama Canal, will have a carrying capacity of approximately 12,000 TEU[5] and Super Post-Panamax vessel are currently under design.

In recognizing the substantial increase in cargo and limited capacity of individuals to inspect and verify the contents of each, it is suggested that that larger volumes of cargo increase the potential for error in delivery as well as the risk of theft or cargo tampering. Succinct standards and practices should be developed to ensure that industry is capable of protecting the cargo and the transportation mediums employed for shipment.

1.3 Supply Chain Security

Supply chains are not often linear. There are many stakeholders that both directly and indirectly involved ensuring that products reach their final destination. When considering the supply chain of containerized cargo it is essential to recognize that there can be many different modes of transport and layers of security involved. In order to understand the concept of supply chain security, it is first important to discuss what defines a supply chain as it relates to the shipment of containerized cargo to better understand the relationship between stakeholders and the potential for exploiting vulnerabilities. "A supply chain encompasses all activities associated with the flow and movement of goods, services, and related information from the point of origin to the point of consumption ([35] Murphy and Wood, 2008). The supply chain is complex and involves many actors. It is largely an international system encompassing many entities including suppliers, manufacturers, ocean carriers, freight forwarders, logistics service

[5] Propulsion Trends in Container Vessels. Table 1, Page 9. Retrieved from: http://www.mandieselturbo.com/files/news/filesof4672/5510-0040-01ppr_low.pdf

providers, customs, and buyers. Obviously, container shipping is an integral component of the supply chain and is responsible for handling and carrying cargo across the ocean. It links consigners and consignees as well as connects all entities in the supply chain (Closs and McGarrell, 2004; Willis and Ortiz, 2004; Lee and Song, 2010). The security of container shipping supply chain "invariably affects overall supply chain security performance". (Yang and Wei, 2013, p.75)

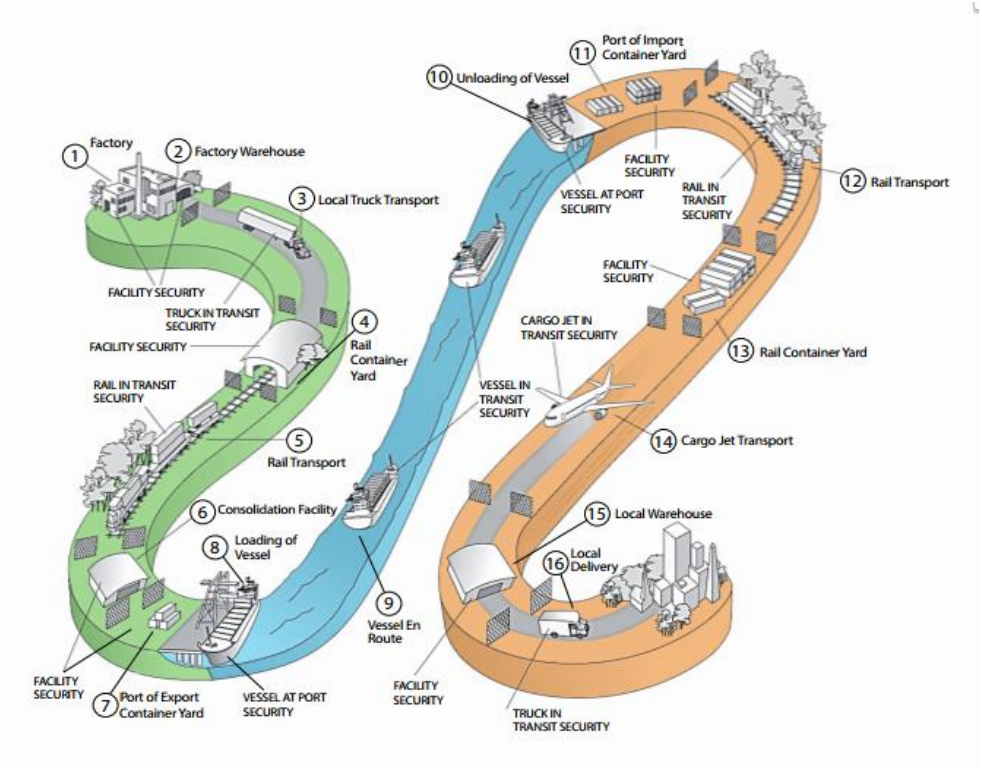

Figure 2 The supply Chain. (Source: US Customs and Border Protection, 2017)

Supply chain security consists of the procedures and instruments implemented by industry and governments to enhance the security of the supply chain as goods move from their place or origin to their final destination. Supply chain security is normally a layered approach whereby physical security features coupled with approved security procedures are strategically put in place throughout the chain to mitigate the

vulnerabilities and to assist with the deterrence and detection of security incidents, breaches and/or threats that have the potential to cause harm to the cargo, individuals or the transportation system. These strategies are often supported by various policies and legislation, many of which will be discussed throughout this project.

It is often stated that a chain is only as strong as its weakest link. The same principle applies to supply chain security. "The global system relies upon an interconnected web of transportation infrastructure and pathways, information technology, and cyber and energy networks. While these interdependencies promote economic activity they also serve to propagate risk across a wide geographic area or industry that arises from a local or regional disruption" (Government of the United States, 2012, p. 2). It is imperative that supply chain security evolves to ensure that it is sufficient to address and withstand ever changing threats that may be introduced.

Establishing supply chain security through the various modes is essential to protecting not only the cargo being shipped but also to protecting the interests of carriers and transportation systems. The ISPS code and associated regulations in Canada such as the MTSR, contain sections that are devoted entirely to the secure handling of cargo, but do not provide for prescriptive methods in which to prevent the tampering of cargo. A container seal is one method that is used to assist in the prevention and detection of tampering, but there is no internationally accepted standard in place. The following section of this project will examine recommendations, standards and initiatives that have been put in place to assist with supply chain security with specific focus of the protection of containerized cargo by use of seals.

1.4 The Issue

It has been a long accepted practice to place a mechanical seal on a container at the point of origin once the packing of the container is complete. The seal identification, often a combination or series of letters and numbers, is recorded on the cargo manifest and other shipping documentation that is provided to the shipper and the place of destination. This is also intended to provide ease of identification of the cargo container. Additionally, many shipping companies have procedures in place that ensure the container number must correspond with the seal number to further ensure the integrity of the contents. It is important to point out however, that if a seal is broken, many shippers require only that the incident is recorded and that the new seal information is updated on the cargo documentation accordingly.

It is also important to note that it has become increasingly easy to produce exact replicas of a seal. The ISPS code and associated regulations suggest that marine facility and vessel operators routinely check containerized cargo for evidence of tampering, with particular attention to the container seal. Replacing a mechanical seal with an exact copy of the seal would most likely not provide evidence of tampering.

In theory, a container of cargo may travel from one continent to another and by various means of transport. A mechanical seal does not provide any information about the details of the journey; as Rizzo et al. (2010) note, “the possibility to physically tamper with the seal during the long journey periods in which containers are not controlled, makes this solution highly vulnerable and ineffective…even when the tampering attempt is detected, a mechanical seal cannot provide information regarding the time and the

place in which the infraction took place" (p 846). This study will explore the use of a RFID can provide an improved method to ensuring an additional layer of security that would at the very least deter attempts to access the cargo by increasing the likelihood of determining the point of access.

1.5 Methodology

This project examines container seal standards and practices currently in place, as well as alternative technologies that have been tested and recognized as methods that can effectively and efficiently increase supply chain security across all modes, with concentration on the globally regulated marine mode in particular. A review of the literature as set out above and also later has been conducted with emphasis placed on the discussions about evolving RFID technology in use for container seals and by other industries.

Sources have been selected in Chapter 2 to establish the importance of regulatory bodies and organizations that strongly influence the containerized shipment of cargo and that also have national and regional agreements in place with Canada. The third chapter of this project reviews the ISO standards in use with an emphasis on the advantages and vulnerabilities of each. The literature reviewed and referenced in Chapter 3 also provides information regarding the motivation for industry to adopt an ISO RFID Standard as well as sources that argue against the implantation for financial reasons. Further, in addition to considering possible the Canadian implementation of a RFID seal as a technical standard for container seals, Chapter 4 of this project also

highlights a case study to draw attention to the successful global transition to RFID technology in an equally challenging industry, aviation security.

Chapter Two

The following chapter examines a number of global organizations that on varying levels are influential to world trade and associated security arrangements. The organizations in the chapter will be referenced frequently in this project. Significantly, greater attention is given to North American organizations that have been instrumental in defining industry standards. The organizations discussed in the chapter and throughout this project have contributed significantly to the development and use of RFID technology.

2.1 Regulatory entities and Organizations

Cargo pilferage and tampering have been well documented for centuries, (Johnston, 2006, p.515) as are the actions taken by marine insurers and underwriters to indemnify and protect the interests of shippers. It has been in recent years only, that there have been significant initiatives from governments and international bodies to impose regulations upon industry that require specific procedures to aid in the protection of marine transportation and associated goods. As previously mentioned, this project will mainly examine and concentrate on organizations that have regional and national arrangements relative to Canada

The shipping industry, particularly as it relates to the shipment of containerized cargo is subject to a high degree of regulation and oversight at an international level. There are various regulatory bodies and global organizations that have worked very closely in recent years to develop and establish recommendations based on best practices to

increase supply chain security while effectively and efficiently maintaining transport of cargo. The following entities are being discussed in this project to highlight the combined work of government and industry and to draw attention to the current initiatives that are in place.

2.2 International Maritime Organization (IMO)

The IMO's main task has been to develop and maintain a comprehensive regulatory framework for shipping and its remit today includes safety, environmental concerns, legal matters, technical co-operation, maritime security and the efficiency of shipping (Mapplebeck, 2009).

The events of 9/11 in the United States of America (USA) marked a shift in an influential government's approach to marine security. Even though the numbers of maritime related security incidents were limited, the IMO was tasked to develop a code to support the creation of security procedures that would protect property and life against attacks and enhance the detection of explosives, incendiary devices or weapons that could be used to cause significant disruptions to marine transportation. The IMO responded with the International Ship and Port Facility Security (ISPS) Code[6] that came into force July 1, 2004. Current to 2009, the measures of the ISPS Code apply to 159 States, the combined merchant fleets of which constitute over 99 % of the gross tonnage of the world's merchant fleet and the number of port facilities involved is in excess of 10,000 (Mapplebeck, 2009). It is important to note that the ISPS Code is largely non-prescriptive in that vessels and facilities are left to develop procedures that meet the

[6] See http://www.imo.org/ourwork/security/instruments/pages/ispscode.aspx for more details.

requirements of the code in a matter that is suitable to their operations. The ISPS Code does not dictate specific requirements; rather the task of ensuring that industry satisfies the requirements is the responsibility of national regulatory bodies and classification societies or Recognized Organizations (ROs) of signatory countries. Further, since ISPS was adopted through the IMO Tacit acceptance procedure, it should be understood that some countries ratified SOLAS but did not expressly agree to ISPS.[7]

The lack of specific instruction in the ISPS Code places the onus on industry to develop and adopt policies and procedures that can be implemented to satisfy the requirements of the code and to address or mitigate vulnerabilities that may exist within their operations. This is evident in the realm of supply chain security, particularly with the varied use of container seals and associated security procedures. It is important to note that resolution nine of the SOLAS Convention recognized the intermodal and international nature of containerized cargo and the need to ensure security throughout the supply chain. As a result, the World Customs Organization (WCO) was asked to develop measures to enhance the supply chain security which ultimately led to the (WCO) and United Nations Office on Drug and Crime (UNODC) jointly led Container Control Program (CCP)[8]and in turn, the WCO *Safe Framework of Standards (*SAFE)[9] that include a Seal Integrity Program, to be discussed in greater depth in this project.

2.3 World Customs Organization (WCO)

[7] IMO Status of Treaties:
http://www.imo.org/en/About/Conventions/StatusOfConventions/Documents/Status%20of%20Treaties.pdf
[8] For more information on the Container Control Program, see
https://www.unodc.org/unodc/en/drug-trafficking/horizontal-initiatives.html
[9] For more information on the WCO Safe Framework of Standards, see
http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/~/media/55F00628A9F94827B58ECA90C0F84F7F.ashx

The WCO[10] is an independent intergovernmental body whose mission is to enhance the effectiveness and efficiency of customs administrations. It represents 180 customs administrations globally, including Canada, which collectively processes approximately 98% of world trade.

In partnership with the UNODC, the WCO launched the CCP in 2003 (one year prior to the entry into force of the ISPS Code). This initiative was put in place because it was recognized that "seaports are notoriously difficult - and at times dangerous - places to work. Law enforcement structures are often hampered by a lack of resources, inter-agency mistrust, complex port processes and systems, and other factors which are purposefully exploited by criminal organizations. This situation poses a very real and serious threat to the security of the international trade supply chain, which is so important to sustainable development" (WCO, 2015).

The CCP is designed to assist governments in developing controls to assist in the identification of high risk containers. In particular, the CCP emphasizes the importance of interagency cooperation for the design and implementation of controls, inspection and enforcement.

The WCO is also responsible for the implementation of the *SAFE program that* was put in place in 2005 as a means to increase international supply chain security. It was designed to "to secure the movement of global trade in a way that does not impede but, on the contrary, facilitates the movement of that trade" (WCO, 2007, p.2). As detailed in the framework, "it is an unacceptable and an unnecessary burden to inspect every

[10] For more information on the WCO, see http://www.wcoomd.org/en.aspx

shipment. In fact, doing so would bring global trade to a halt" (WCO, 2007, p2). It is for this reason that the framework focuses on capacity building and the need for customs administrations to use automated systems and succinct procedures to assist in the identification of higher risk cargos.

In particular, the framework stresses the value and importance of employing various types of technology throughout the transit of cargo. For instance, the framework notes many standards that require the use of modern technology. Standard three indicates "non-intrusive inspection (NII) equipment and radiation detection equipment should be available and used for conducting inspections, where available and in accordance with risk assessment. The standard emphasizes that such equipment is necessary to inspect high-risk containers or cargo quickly, without disrupting the flow of legitimate trade" (WCO, 2007, p.8). Further, standard six notes that "the customs administration should require advance electronic information on cargo and container shipments in time for adequate risk assessment to take place" (WCO, 2007, p.8). It is also important to note as it relates to sealing containers, that the framework suggests that "Customs should facilitate the voluntary use of technologies to assist in ensuring the integrity of the container along the supply chain" (WCO, 2007, p.10).

On numerous occasions the WCO- SAFE program makes reference to the importance of ensuring the use of a high security container seal and the requirement to check it for tampering throughout the entire transit. It is fair to state that a great deal of emphasis is placed on the requirement for a mechanical seal on containers to assist with supply chain security; yet, it is also fair to state that the mechanical seal is perhaps one of the greatest vulnerabilities in the entire process. It may be for this reason that SAFE also

highlights that, “Customs administrations should encourage and facilitate, through appropriate incremental incentives, the voluntary use by Authorized Economic Operators (AEOs) of more advanced technologies beyond mechanical sealing for establishing and monitoring container and cargo integrity, as well as reporting unauthorized interference with container and cargo” (WCO, 2007, p. 33).

2.4 Customs-Trade Partnership against Terrorism (C-TPAT)

C-TPAT[11] was created in 2001 and was designed mainly to elicit the voluntary participation of the shipping industry to implement measures that would increase cargo and supply chain security, particularly as it relates to the multi-modal transshipment of containerized cargo. As of 2016, “more than 11,400 certified partners spanning the gamut of the trade community have been accepted into the program” (US Department of Homeland Security, 2017).

“The Security and Accountability for Every Port Act of 2006 provided a statutory framework for the C-TPAT program and imposed strict program oversight requirements” (US Department of Homeland Security, 2017). The C-TPAT initiative operates under the principal of mutual recognition in that it “seeks to develop cooperative container transport security relationships between the US Government and the organizations in a container transport chain (e.g. importers, terminal operators, carriers, etc.)” (Thibault et al., 2006), and “the benefits associated with C-TPAT participation are faster cargo clearance and fewer inspections at US ports” (Venus Lun et al, 2008, p.30).

[11] For more information on C-TPAT, see https://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-partnership-against-terrorism

C-TPAT's security criteria states that "…a high security seal must be affixed to all loaded containers bound for the U.S. All seals must meet or exceed the current ISO 17712 standards for high security seals" (US Customs and Border Protection, 2014, p.2). The current ISO standard does not require the use of RFID technology on seals. It is also important to note that the 2014 C-TPAT bulletin, *Compliance with ISO's 17712 Standards for High Security,* acknowledges that the high security seal is also vulnerable to tampering and in fact suggests that industry must also be aware that the documentation associated with the authentication of high security seals may also be subject to fraudulence and should therefore be further scrutinized before accepted.

2.5 Partners in Protection (PIP)

In Canada, the Canada Border Services Agency (CBSA), also a member of the WCO, has implemented the *Partners in Protection (PIP[12])* program that is very much aligned with the C-TPAT program of the U.S. The programs are similar to ensure adherence to the *Beyond the Border Action Plan.* Under the *Beyond the Border Action Plan*, Canada and the U.S. continue to develop a common approach for our Trusted Trader programs that aligns requirements, enhances member benefits, and facilitates the cross-border movement of commercial goods (Canada Border Services Agency, 2014).

As indicated by CBSA (2014), "Partners in Protection (PIP) is a cooperative program between private industry and the CBSA aimed at enhancing border and trade chain security. This voluntary program has no membership fee. It is designed to streamline and make border processes more efficient for low-risk, pre-approved businesses

[12] For more information on PIP, see http://www.cbsa-asfc.gc.ca/security-securite/pip-pep/menu-eng.html

recognized as trusted traders". The PIP program is also centered on mutual recognition of policies and procedures that have been agreed upon to ensure that best practices and standards are applied to assist with protecting the integrity of the supply chain.

The PIP program also clearly outlines requirements for sealing containerized cargo, in particular, cargo sealing guidelines for PIP members. It is important to point out that the guidelines, in addition to providing procedures for seal application, change-out and intrusion detection, also require that the ISO standard seals used by PIP members must meet or exceed the current PAS/ISO 17712 standards for high security, the same standard required by C-TPAT. The ISO and C-TPAT will be further discussed in this chapter. The guideline further notes that "such seals have been manufactured with strong metal materials with the intent to delay intrusion and generally require the use of bolt or cable cutters to be removed".[13] It is important to note that the guideline acknowledges that the 17712 standard may only *delay* entry into the container. It is also noteworthy that there are numerous instructional videos available online that provide techniques that allow for the successful removal of such seals in one minute or less. Many of the procedures that are outlined in the guideline produced by PIP are very stringent as well as valuable; they could easily be applied to the use of RFID seals to further increase the integrity of the controls in place to ensure supply chain security.

The entities and initiatives referenced above are all interconnected. They have fostered working relationships that have led to some very positive changes related to supply chain security in recent years. There are also some very obvious similarities and parallels that have developed between Canada and the United States, as detailed by

[13] http://www.cbsa.lgc.ca/security-securite/pip-pep/seals-scelles-eng.html

PIP and C-PAT. How these similarities can be leveraged to implement the standardized use of RFID seals will be discussed later in this project. It is important to understand that industry has a high degree of participation and influence on many of the above mentioned players and initiatives and as such, their level of engagement is paramount when considering new and potentially more expensive alternatives to the mechanical seal to increase supply chain security.

2.6 International Civil Aviation Organization (ICAO)

The International Civil Aviation Organization (ICAO) is a United Nations specialized agency established in 1944 to manage the administration and governance of the Convention on International Civil Aviation (ICAO, 2017).

In 1974, ICAO generated provisions for international aviation security under the auspices of the Chicago Convention, much like the IMO produced the ISPS code under the auspices of the SOLAS Convention. The ICAO provisions originally included guidance material and information for member states to assist with the implementation of international security measures. According to McConnell (2016), “in December 2002 the IMO held a Diplomatic Conference on Maritime Security and moved to adopt stringent requirements for security practices for ships and for port areas in the form of amendments to one of the most ratified of its maritime Conventions…the ICAO also took action to further develop its technical standards to ensure more secure passports and other travel documents” (McConnell, 2016 p. 20).

Most recently, and as discussed later in this project, ICAO has been involved in leading efforts to enhance the security of travel documents and to improve the training of

security personnel. Travel document security is being addressed by the *Machine Readable Travel Document (MRTD)* program[14]. Under this initiative, the ICAO has assisted significantly in the development of a worldwide standard for machine readable passports that incorporates the use of RFID technology. This project will include a section that will highlight the challenges and successes of the MRTD program and demonstrate how the critical components of the program can be applied to an initiative that incorporates the use of RFID technology on container seals.

2.7 International Organization for Standardization (ISO)

The ISO is an independent, non-governmental international organization with a membership of 163 national standard bodies (ISO, 2017). The ISO is designed to bring together experts of various fields to share knowledge that is used to develop voluntary industry standards that "support innovation and provide solutions to global challenges" (ISO, 2017).

In particular, the ISO has established many technical committees that are assembled based on the level and area of expertise required for the development and oversight of a given standard.

The ISO technical committee 104 concerning the security of freight containers "has worked on the design of the container doors, its bolts, and hinges to improve security features" (Min and Park, 2007, p. 47). Additionally, technical committee 104 has put in place a specific workforce responsible for the development of container seals, including electronic seals. As mentioned earlier in section 2.5, to date, the most widely

[14] For more information on the MRTD, Doc 9303, see http://www.icao.int/publications/Documents/9303_p1_cons_en.pdf

recommended, used and accepted high security seal is mechanical and adheres to the ISO 17712 standard. It should be noted, however, that the technical committee 104 has also developed the ISO 18185 standard for electronic seals that incorporates the use of RFID technology. Although, to date this standard has not been largely accepted or used by industry.

The ISO has been and continues to be instrumental in providing expertise and recommendations. As noted earlier, organizations such as the WCO, C-TPAT and PIP require industry, to use at a minimum the ISO standard 17712 for mechanical seals on containerized cargo. This project discusses in greater detail how such organizations should consider amending their requirements to include this ISO standard 18185 for electronic seals.

In conclusion, the international, regional and national organizations and programs that have been discussed in this chapter continue to interact on a regular basis to implement standards and requirements that serve to incorporate technological advances that can improve supply chain security and enhance global participation.

Chapter 3 l highlights the current requirements, new initiatives and the roles that the previously discussed organizations and programs have played with respect to international implementation.

Chapter Three

The use of container seals is by no means to be considered a new means of protecting cargo as a result of a post 9/11 security climate. In fact, quite the opposite is true. For

about as long as humans have been transporting goods, seals have been put in place to help ensure or indicate integrity of the sealed object. Stamp seals were first used at least 7000 years ago, becoming especially popular in Middle Eastern and Aegean civilizations of the 2nd and 3rd millenniums BC (Gibson and Briggs, 1977; Collon, 1987). Cylinder seals were invented around 3500 BC and were in widespread use from 3000 to 500 BC (Collon, 1987; Collon, 1990). Both types of seals were also found in the "New World" (Enciso, 1953). Wax or resin eventually replaced clay as the preferred sealing material in the 1st millennium AD, with lead seals coming into use by the 4th century AD (Vikan and Nesbitt, 1980; Johnston, Martinez and Garcia, 2001, p. 2). Tamper indicating seals from the earliest civilizations to the present day standards all have one thing in common, their vulnerabilities are often exploited and therefore the design must always be improved upon.

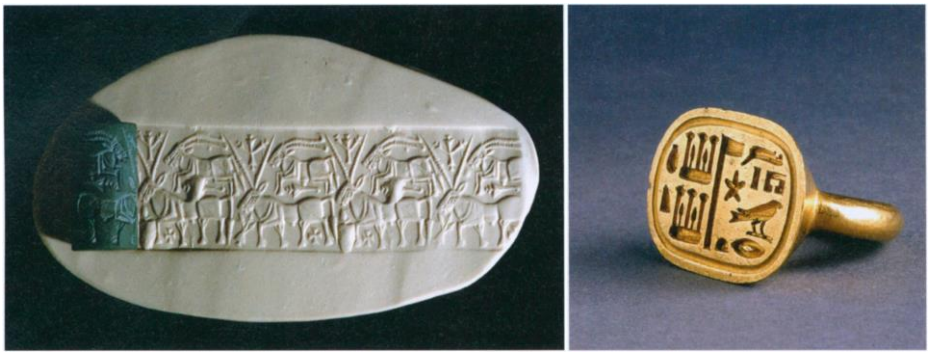

Figure 3 Ancient Seals (Johnston, Martinez and Garcia, 2001, p. 516)

3.1 The Use and Purpose of Container Seals

The following sections of this chapter set out the details of two specific types of container seals that can be used to increase cargo security: Mechanical seals and

electronic (e-seals) that incorporate RFID technology. According to Rizzo et al. (2010), “a seal is a device that is applied to one or both of the container doors and that has to be broken in order to gain access to the inside of the container…a seal also carries evidence of its own identity to ensure that the seal itself has not been replaced”. (p. 847). In broad terms, manual cargo seals have long been part of good security practice even though they are principally put in use for liability reasons. In considering emerging threats and the availability of advanced technologies there is value in considering the use of electronic or RFID seals. The RFID seal is a relatively new initiative that has the potential for increased cargo security benefits.

3.2 Mechanical Container Seal – ISO Standard

While there is no legally binding international agreement or convention relating to container seals, as mentioned in Chapter 2, countries such as Canada and the United States (both members of the WCO) require shippers, at a minimum, to use ISO Standard 17712 compliant seals on containers both leaving and entering the country.

Figure 4 ISO Standard 17712 – High Security Mechanical Bolt Seal. (Source: US Customs and Border Protection, 2014).

The WCO, by means of the SAF E program 2012, recommends, at a minimum, the use of a high security mechanical seal as prescribed in ISO) 17712. As detailed by the ISO 17712 Standard, the high security seal can be easily opened with a pair of bolt cutters. It is perhaps for this reason that the WCO SAFE further recommends the use of technologies to assist in ensuring the integrity of the container along the supply chain.

According to the C-TPAT Bulletin, "this standard defines three types of classes of seal strength or barrier capacity: "I" for indicative; "S" for Security; and "H" for High Security. C-TPAT requires the use of "H" class seals". (US Customs and Border Protection, 2014, p.1) In Canada, PIP also requires the use of "H" class seals (Canada Border Services, 2015).

3.2.1 Manual Container Seal – Various Concepts of a Standard

Even though various national customs agencies who are also members of the WCO require at a minimum the use of the ISO Standard 17712 compliant seals, it is important to point out that in this case, the concept of 'standard' may be considered somewhat misleading. The fact that a seal may meet or is compliant with the ISO Standard does not mean that seals are uniform and come in a specific size or shape. The ISO Standard establishes mandatory features of a compliant seal but allows for various formats, so container seals can vary extensively. For example, the PIP seal requirements note that seals that meet the standard are "generally" in the form of bolt or cable seals. According to PIP[15], examples of mechanical seals include:

[15] For more information on CBSA Cargo Sealing Guidelines for PIP Members, see http://www.cbsa-asfc.gc.ca/security-securite/pip-pep/seals-scelles-eng.html

- High-security bolt seal - A seal consisting of a metal rod, threaded or unthreaded, flexible or rigid, with a formed head and secured with a separate locking mechanism.
- High-security cable seal - A seal consisting of a cable and a locking mechanism. On a one-piece seal, the locking or seizing mechanism is permanently attached to one end of the cable. A two-piece cable seal has a separate locking mechanism that slips onto the cable or prefabricated cable end.
- High-security padlock - A reusable lock that can only be opened with a combination code or key. Note that high-security padlocks may only be used for multiple domestic pickups (i.e. less-than-truckload – LTL) where other cargo is added to an existing load enroute" (CBSA, 2015).

Given the various types and forms of mechanical seals available, that meet the requirements of the ISO Standard 17712, it is not unreasonable to conclude that it may be difficult for responsible individuals to detect tampering or replicas.

3.3 The Electronic RFID Seal

Radio frequency identification or RFID is put into practical use throughout the world on a daily basis. The technology is present in personal banking cards, passports, microchips on pets, hospital bracelets and a myriad of other applications by various types of industries globally. There are two types of RFID technology; active and passive. Each of these will be discussed in this section in greater detail and will provide a greater understanding of this technology and how it can be applied for use to increase supply chain security of containerized cargo.

There have been many policies and practices developed to assist with the physical security and integrity of containerized cargo. However, mechanical seals alone may not be adequate to address the continuing issues related to container security. Instances of "seals being broken, goods dumped or exchanged and a substitute imitation seal fixed" are still occurring. A mechanical seal cannot detect or provide an alert of when tampering takes place, nor can it provide additional detail regarding the time or place in which a tampering attempt may have occurred. This critical information can be obtained with the use of RFID technology embedded into seals that provide added security features, including the capacity to read, store and transmit information regarding cargo integrity.

Figure 5: Sample RFID Seal and Associated Reader.

http://www.isopas17712.com/

It is understood that a container may pass through various modes of transportation before it reaches the final destination. Current practices provide little to no information regarding the container once the contents have been sealed inside.

> A reliable account of the full history of the container is a key element of a secure transport chain. The ability to check--at any time or place--where, when and by whom a container was loaded, sealed, transported, transshipped and any other event that occurred in its trajectory is a vital part of security. To achieve such traceability a combination of technical solutions such as seals, radio frequency identification devices (RFIDs) and information systems needs to be deployed. They also need to be accessible by different parties in different parts of the world. This requires performance and interoperability standards and data sharing among industry, local and national or international authorities".
>
> (Dalhman et al, 2005 p. 17)

In practice, an RFID electronic seal possesses features that include "the possibility to certify that it has been closed correctly and can save in the internal memory the time of closure and identity of the operator who performed the installation. Furthermore, with RFID technology a new way of inspecting the seal becomes possible: in fact, in many applications it is the seal itself that performs a self-diagnosis and communicates its state to the inspector. This way the possibility of human error is greatly reduced, and the quality of inspections depend less on the inspector's skills and experience than before. (Rizzo et al, 2010, p. 847).

It should be noted that RFID technology is not new. "It was developed in the 1970s and is capable of using radio waves to automatically identify people or objects (Mehrjerdi, 2010, p. 282). Even though the technology has existed since the 1970s, RFID was not regularly used until much later. "The 1990s saw the acceptance of RFID as an important enabler in supply chain management, which spurred a further series of standardization activities. A milestone came in 1996 with the standardization of RFID as a data carrier by the Article Number Association (ANA) and European Article Numbering (EAN) groups. In 1999, EAN International, and the Uniform Code Council (UCC) of the United States, now both known as GS1, adopted a UHF frequency band for RFID and established the Auto-ID Center at the Massachusetts Institute of Technology." (Chawla and Ha, 2007, p. 11). Globally, industry continues to be more reliant upon digital methods of information storage and sharing. Of note, RFID technology has already been employed in the shipping industry by some manufactures and companies. It is recognized that "the advanced data-capture capabilities of Radio Frequency Identification (RFID) technology, coupled with unique product information coming from different data sources, open up many new possibilities for the efficient management of supply chain processes and decision support (Dmakopoulou et al., 2014, p. 191).

The main objectives of the RFID seal are to "satisfy the increasing need for high security and, at the same time, to be extremely competitive from an economical point of view" (Rizzo et al, 2011, p. 846). Although the acronym RFID is used often as it relates to seals, it should be noted that there are two very distinct technologies used, passive and active. In general, "passive seals are short range, low cost and disposable. Active seals are more sophisticated, have internal batteries and thus have longer range and

greater functionality. They can detect tampering when it occurs and at the time of events" (Siror et al, 2011, p. 191). In other words, "while both use radio frequency energy to communicate between a tag and a reader, the method of powering the tag is different. Active RFID uses an internal power source (battery) within the tag to continuously power the tag and its RF communication circuitry, whereas passive RFID relies on RF energy transferred from the reader to the tag to power the tag" (Whitepaper page 1). It should also be noted that a hybrid of the technology exists whereby a combination of the active and passive RFID has also been put in place.

The type of technology or seal required depends largely upon the security requirements and transit time of the cargo. Both passive and active seals provide a level of security for all modes of transport, but provide different levels of capability. "Passive RFID security solutions are good for applications where simple tamper detection is sufficient, the exact time of a tampering event is not important, and concern about sophisticated thieves attempting to "spoof" the seal are minimal. Because Passive RFID tags cannot be powered while the cargo is in transit, they cannot continuously monitor the presence and status of the cargo seal. They can only report if the seal appears intact at the next read point. Active RFID, on the other hand, can continuously monitor the seal status, detecting minute variations in the seal position or integrity and implementing sophisticated anti-spoofing techniques. Immediately upon detection of a problem, the date and time and event code can be logged in the tag's memory, providing a complete audit trail of all events during the shipment" (whitepaper page 4).

It is important to also draw attention to the fact that no matter which system is employed, "a supporting information technology infrastructure is needed to track the

status of every seal at all times. The complexity of this infrastructure is increased greatly by the geographically distributed nature of container shipping" (Rizzo et al, 2011, p. 847) The possible systems that could be used are beyond the scope of this project but it is understood and acknowledged that system implementation, given the varying technological capacities and limitations of some countries could serve as an hindrance to the adoption of an RFID standard.

3.4 ISO Standard 18185

It is important to draw attention to the fact that even though many organizations recommend or require the use of ISO 17712 standard for high security mechanical seals, the ISO has nearly completed a standard for electronic seals, ISO 18185(ISO, 2007). Currently ISO18185 consists of the following parts, under the general title Freight containers— Electronic seals (ISO, 2006):

- ISO 18185-1, Freight containers – Electronic seals –Part 1: Communication protocol *ƒ*
- ISO 18185-2, Freight containers – Electronic seals –Part 2: Application requirements *ƒ*
- ISO 18185-3, Freight containers – Electronic seals –Part 3: Environmental characteristics *ƒ*
- ISO 18185-4, Freight containers – Electronic seals –Part 4: Data protection *ƒ*
- ISO 18185-6, Freight containers – Electronic seals –Part 6: Messages sets for transfer between seal reader and host computer *ƒ*
- ISO 18185-7, Freight containers – Electronic seals –Part 7: Physical layer

The ISO Technical Committee 104 has discussed various approaches to the use of electronic seals that have led to the development of the ISO developed standard 18185 for the use of electronic seals. The ISO 18185 requires conformance with ISO Standard 17712. In other words, any electronic seal that is manufactured to meet the requirements of ISO 18185 must be done in such a way as to contain the physical properties of a high security mechanical seal as outlined in ISO 17712 and previously discussed in this paper.

"The ISO 18185 Part 1 standard is an international standard that provides a system for the unique identification and presentation of information about freight container electronic seals. It is used in conjunction with the other parts of ISO 18185 such as Part 4 that specifies data protection and Part 7 that specifies the physical layer protocol" (Dontharaju, 2004, p. 16).

The ISO 18185 standard may not be suitable for industry adoption as it is currently written, for two main reasons. To date, there are "no global standards for frequencies and technical specification for electronic seals. The International Standards Organization's (ISO) Technical Committee 104 is trying to specify data protection technology, and as a result, ISO 18185-4 Gen 1 was released in August 31, 2005. However, the ISO 18185-4 Gen 1 did not satisfy requirements of data protection and device authentication for eSeals" (Daschkovska, 2008, p.16). Further, the standard mainly provides for the use of passive seals that are disposable. As indicated by part one of the Standard, "ISO 18185-1:2007 specifies a read-only, non-reusable freight container seal identification system, with an associated system for verifying the accuracy of use, having a seal status identification system, a battery status indicator, a

unique seal identifier including the identification of the manufacturer, seal (tag) type (ISO, 2007). It is unlikely like industry would be willing to invest in RFID technology that cannot be reused as a means of offset the higher cost. To date, these characteristics are not conducive to active seals that may be better suited for the purpose of increasing supply chain security by logging tampering events as well as providing information regarding container location. It is important to note however that, "all major international trading countries including Japan and China have approved active RFID products operating at 433 MHz that are based on ISO 18000-7 standards. The global Radio Frequency (RF) community is moving to authorise the common High Frequency (HF), Ultra High Frequency (UHF) and microwave frequencies to enable RFID usage around the world (Mundo Maritimo, 2007).

3.4.1The Argument for the use of RFID Technology

The supply chain is complex and dynamic. "Global supply chains are hyper-connected models of efficiency and risk. The global import/export market exceeds US$6 trillion, with 15 million containers continually being transported on 46,000 vessels through 4000 global ports. Each link and node in the supply chain is subject to a variety of threats from fraud to terrorism (Siror et al., 2011, p. 796). In 2012, Canada's four largest container ports, Vancouver, Montreal, Prince Rupert and Halifax handled approximately five million TEUs and are still seeing annual growth. [16] This is nearly an average of fourteen thousand containers a day imported into Canada. In theory, that should also

[16] http://www.joc.com/port-news/international-ports/port-metro-vancouver/canada%E2%80%99s-big-4-container-ports-put-focus-infrastructure_20130902.html

mean fourteen thousand high-security mechanical seals should be affixed, checked, and inspected. It is safe to assume that this is a very large undertaking, particularly when you take into consideration that this checking is largely dependent on the human factor.

As required by the ISPS Code, port facilities and vessels are required to implement approved procedures that include monitoring and checking containerized cargo to detect any evidence of tampering. Marine facilities normally have designated individuals who are assigned these are various other security related responsibilities; and “while under great pressure to maintain security, port operators are penalized for supply chain interruptions” (Siror et al., 2011, p. 796). The checking of TEUs as previously mentioned is largely dependent on the individual at a marine facility or a ship who is responsible to check a container against the associated documentation for a number of things, including seal integrity, evidence of tampering and authentication against a standard. Individuals tasked with this responsibility generally do not receive high wages in many places of the world. Further, the level of training provided to assist with the checking of the seals varies greatly, even if provided beyond on the job training. Taking this into consideration along with the fact that seals can be easily replicated, removed or replaced with minimal effort, the ISO standard does not require seals to look the same. Also taking into consideration the sheer volume of TEUs that are shipped, it is not unreasonable to suggest that the use of mechanical seals as an added layer of security to the supply chain may not be adequate to address the emerging security threats. “The looming challenges of the future make it vital for port administrations to consider

intelligent handling methods. Manual and semi-manual methods [sic] (of goods) are totally inadequate in dealing with the current challenges" (Siror et al., 2011, p. 796).

Evolving technologies, such as the RFID seal have the capacity to improve the ability to secure the supply chain and provide a level of confidence in the integrity of the TEUs while travelling from the origin to the destination.

3.5 RFID Technology in Practice

In 2003, the Strategic Council of Security Technology[17] initiated a pilot test of electronic seals whereby a total of 818 containers were affixed with RFID seals. In this project, all electronic seals automatically reported their identification and security status to both fixed and handheld readers designed to transmit the information as required. The cost benefit of using the RFID seals at the time was negligible at approximately thirty dollars (USD) per container. It is reasonable to assume that those margins would be significantly higher today given the lower costs associated the technology involved. It is important to highlight that during the time of the study, "about eleven percent of the entire tested containers gave a tamper alert to the port authority" (Min and Park, 2007, p. 54)

The popularity of RFID technology continues to grow annually as the cost of manufacturing decreases and efficiencies improve. "RFID was an $8.9 billion global industry in 2014" (Zelbst and Sower, Chapter 2, 2016). Notably, various companies and government agencies have recently begun to report the benefits of RFID use,

[17] https://www.fraserinstitute.org/sites/default/files/NetworkCentricSecurity.pdf

particularly as it relates to supply chain management. The benefits to supply chain management can easily be translated into benefits to supply chain security.

The company Proctor and Gamble, for example, a major supplier of Walmart, has recently indicated that they have found "significant benefits in helping streamline processes, shipping and speeding the movement of their products to distribution centers" (Zelbst and Sower, Chapter 2, 2016).

The shipping company CHEP[18] founded in Australia is another well-known provider of pallet and container pooling services and also a user of RFID technology. The company uses RFID "to track 150000 foldable large containers (FLCs) throughout Europe" (Zelbst and Sower, Chapter 7, 2016). The use of RFID has earned the company various awards related to supply chain security and has provided accountability and improved inspection data for their containers that are valued at approximately $200 USD apiece (CHEP, 2014).

It is also important to point out that government agencies also rely on RFID technology to assist with maintaining cargo security. The United States Department of Defense (US DOD) used RFID supply chain management to track and maintain the security of shipments entering war zones of Iraq and Afghanistan" (Zelbst and Sower, Chapter 2, 2016).

There is no doubt that RFID technology can be used in many ways to improve efficiencies and provide valuable information and data regarding the shipment of cargo.

[18] For more information on CHEP, see https://solutions.chep.com/choose

The same technology can congruently provide real time information regarding the integrity of container seals and by extension, the container.

3.6 Existing and Documented Vulnerabilities with ISO Standard 17712

The underlying issue or vulnerability associated with the use of the ISO Standard 17712 is not the quality of the mechanical seal so much as it is the sole reliance upon an individual tasked with the responsibility of inspection to detect and report tampering. Further, the possibility exists that an individual may be persuaded to surreptitiously remove a seal and exchange it with another in order to maliciously introduce prohibited items into a container for transport.

The ISO Standard 17712 requires that mechanical seals have specific features to ensure that tampering can be identified. “Examples of tamper evidence include a change in the colour of the material, in surface texture, cracks, indentations, or abrasions. Tamper evident indicators are recognizable by normal examination under the usual circumstances prevailing in practice without technical aids (such as a magnifying glass or microscope)” (ISO, 2017). It is difficult to determine what constitutes ‘usual conditions’, as containers are exposed to various physical and environmental elements. Large gantry cranes are used to load and unload containers on and off ships respectively. From the dock, it may be transferred to a specific location at a facility where it may rest for a period of time until it is removed by truck or train or another vessel. Many container facilities operate on a twenty-four hour basis and often in adverse weather conditions with varied lighting. On vessels, containers are most often secured to an open deck where mariners are exposed to seas, weather and other

physical elements. It may be difficult to detect indications of tampering as prescribed above under such circumstances. It has been demonstrated that RFID technology has the ability “to operate well in a variety of visually and environmentally challenging conditions such as snow, ice, fog, paint, grime, inside containers, in vehicles, warehouses and ports” (Siror, 2011, p. 796).

The main advantages of the ISO Standard 17712 to industry are its relatively low cost and disposability. The mechanical seal is however, very easily counterfeited. The replication of seals has become increasingly prevalent as used parts are readily available as mechanical seals are intended for one time use and are most often not securely disposed of after use (Johnston, 2006, p. 521). Furthermore, individuals tasked with seal inspection, more commonly referred to as ‘checkers’ in the marine domain, are rarely given examples of genuine seals for reference, which may allow reasonably accurate forgeries to go unnoticed (Johnston, 2006, p. 517).

As documented in the WCO’s Container Analysis Report (2008), containers are subject to invasion for the purpose of introducing illicit substances. This is achieved in part by the use of replicated seals. “Very often a new seal duplicating the number of the original seal (see Figure 6) assigned to the container, and noted on the commercial documents, is attached to one of the bags carrying the contraband. When the contraband reaches the country of destination or transhipment port, the local conspirator breaks the original seal, opens the door, retrieves the contraband, closes the door, and affixes the duplicate seal to the container. No legitimate cargo is stolen and the original seal number is on the container. In some cases the original broken seal is “repaired” and reaffixed on to the doors of the container” (WCO, 2008). Additionally, the WCO

Container Analysis discusses four known possible opportunities for the introduction of malicious or illicit items into containers:

1. During the loading of the goods at the premises of the shipper: conspiracy of local employees of the shipper;

2. During the transport from the premises of the shipper to the port of loading: conspiracy of the transport company and/or driver;

3. On the terminal in the port of loading: conspiracy of: local port workers: employees who know the routing of the container (the contraband must arrive in the right port of destination) and the location of the container on the terminal;

4. On the vessel during the voyage: conspiracy of crewmember(s). This scenario is only possible when the container is accessible on the vessel.

Of note, three of the four circumstances noted above would require the removal of the mechanical seal which can easily be carried out by the use of a pair of standard bolt cutters by any individual who is strong enough to do so. Additionally the same vulnerabilities exist for the retrieval of contraband from containers at the port of discharge and final destination. The application of a replicated seal would not prompt a documentation change indicating that the seal had been changed.

Figure 6: Replicated Container Seals (WCO, 2008)

Source:http://www.mcmullinpublishers.com/downloads/OMDrcEN08.pdf

It should not be concluded that an RFID seal would provide an end to seal tampering. It can be assumed however that the use of such technology would however deter and limit the number of successful attempts as perpetrators become aware that the technology has the capability of providing indicators as to when and where the tampering has been attempted.

Chapter Four

There are numerous challenges associated with the global implementation of RFID technology. These challenges however, are not insurmountable. As demonstrated in the following case study, the advantages of the technology were recognized recently by the ICAO and a plan was successfully implemented to incorporate RFID technology, including chip readers, into electronic passports. The following case study is presented to draw attention to the similarities related to the technical and stakeholder engagement

challenges. Additionally, the following case study demonstrates how a similar framework could be developed for the implementation of RFID container seals particularly as it relates to the criticality of stakeholder engagement and industry buy-in. Finally, this chapter will also highlight the vulnerabilities associated with the existing ISO 17712 standard.

4.1 Case Study/ Comparison

The ICAO has a mandate to develop and maintain civil aviation standards, including standards related to the format and inspection of travel (passports etc) and other documents. The standard now in place is mainly referred to as the electronic passport or ePassport that incorporates the use of RFID and biometric technology for the secure protection of personal information of individuals.

> "In 2004, the Assembly of ICAO affirmed that cooperative work on specifications to strengthen the security and integrity of travel documents should be pursued by the Organization as a matter of high priority. In addition to the International Organization for Standardization (ISO), consultants to the TAG/MRTD include the International Air Transport Association (IATA), the Airports Council International (ACI), and the International Criminal Police Organization (INTERPOL). In 2005, the then 188 Member States of ICAO approved a new Standard that all States must begin issuing machine readable passports in accordance with Doc 9303 no later than the year 2010" (ICAO, 2015).

It was largely recognized by the ICAO there were many benefits of implementing such a standard, including, the ability to facilitate and secure passenger processing at border control points as well as enable global interoperability (Cuthbertson, 2010). The ICAO conducted extensive outreach and engaged with international stakeholders to market the benefits of the ePassport which in turn contributed to the 'buy-in' of member countries. It should be noted however that this initiative also experienced many challenges for the success of the program could be recognized. In particular, interoperability of member countries is highly dependent upon the technical capabilities of member countries. "In order for widespread deployment to occur, more vendors will need to reach similar performance levels with increased accuracy and detection rates" (Kumar et al., 2012, p.19). Further, "electronic passport rollout plans continue to move forward, but some countries continue to lag behind. Certainly, the ongoing debate over how best to protect data stored on the RFID tags may be preventing some nations from moving forward" (Kumar et al., 2012, p. 19.) It is not unreasonable to assume that the introduction of an RFID Container Seal Standard may face similar challenges.

It is important to note that the ISO played a significant role in the successful implementation of the ePassport. "The technical specifications sections of Doc 9303 have received the endorsement of the ISO as ISO Standard 7501. Such endorsement is made possible by means of a liaison mechanism through which manufacturers of travel documents, readers and other technologies provide technical and engineering advice to the TAG/MRTD under the auspices of ISO. Through this working relationship, the ICAO specifications have achieved, and are expected to continue to receive, the status of worldwide standards by means of a simplified procedure within ISO" (ICAO, 2015, p. 3).

Of particular note, the ISO standard in place with the ICAO provides the ability to introduce new specifications and subsequent approval for amendments to the standard.

Current to 2015, approximately 350 countries were producing electronic passports in accordance with ICAO standards, including Canada who introduced ePassports in 2014.

4.2 Analysis: Motivation for Industry to accept a Standard

It is difficult to dispute that stakeholder engagement and 'buy in' is critical to the success of any initiative where multiple players are involved, as proven in the case study above. The same holds true for the implementation of active RFID seal technology on containerized cargo. It is evident that the largest impediment to the adoption of the RFID seal is the cost, not only for the seal but for the associated infrastructure required such the RFID readers and the communication equipment. "Stakeholders have had little motivation until recently to implement additional security measures in the highly competitive container transport market" (Daschkovska, 2015, p. 38). However, as the costs for the technology continue to decrease, reusable seals are being designed and the benefits of the technology become increasingly evident and documented, it is now perhaps more important than ever before to present options to industry in a way that cannot only demonstrate the opportunity for increased security but also the potential to optimize business practices in such a way that industry can actually see the return on investment.

Reduced number of examinations and access to simplified procedures

Initiatives and programs such as C-TPAT and PIP have successfully implemented compliance as an opportunity. By meeting the requirements of the voluntary program, industry receives a reduced number of examinations and inspections as well as access to simplified procedures. Additionally, companies that meet the requirements also have an enhanced reputation of being low risk and therefore may in turn see an increase in business.

Incorporating the use of RFID seals may serve to further demonstrate a companies' investment in supply chain security. There may also be an opportunity for programs such as C-TPAT and PIP to require the use of such technology and in turn, provide access to additional streamlined processes to companies who participate. Further, the use of RFID Seal technology "may optimize logistics and generate improved efficiencies and delivery times of containerized cargo. To ensure that shipments are delivered on time to the right place at a low cost, it is most desirable that technology be used to track the status of container flows and support the associated information interchange in a container transport chain to enhance security for the cargo movement" (Lun et al 2008, p. 22). "The benefits according to a study conducted in a manufacturing industry revealed that lost containers could be reduced by 3%, container search times by up-to 75%, reduction of strays and errors by 95%, fewer production downtimes due to lack of containers and an increase in container circulation rate by 5%. A separate study undertaken by the same author revealed that 60% savings could be achieved by use of the solution and Return On Investment (ROI) of 10.4 months achieved" (Siror et al., 2010, p. 192). It should also be considered that future developments of the RFID seal are being designed to include the ability to incorporate electronic data regarding the

container contents in place of shipping documents. This could reduce costs and human error associated with information transfer.

Cost of RFID seals can be offset with operating efficiencies and insurance benefits

The costs of RFID seals can also be offset with operating efficiencies and insurance benefits. "The usage of the electronic cargo information in container e-seal can improve the container logistics processes by speed up the container passes thought the container transhipment nodes (port terminals), prevention and control of unauthorized access or theft of the container contains, provide the information for the companies and authorities about container location as well as getting automate monitoring and tracking of the containers, avoid typically errors during issuing or receiving of goods" (Daschkovska, 2015, p. 69).

Multi-modal transportation involves many players from the time packing at the point of origin to the final destination. "As many as 20 different companies have to coordinate the operations of more than 25 documents with approximately 200 data elements for only one international shipment in the global container network" (Kreowski et al, 2008, p. 459). Given the large number of actors and the distance travelled over many modes, current security regimes make it hard to determine, where in the supply chain tampering or theft may occur. This issue may contribute to shipping companies having to engage in unnecessary litigation and insurance claims that may otherwise have been avoided with the implementation of an RFID seal. An investment in supply chain security by means of RFID technology not only improves tracking and monitoring, but also shipment visibility and standards of care. "Shippers and carriers that are developing

"standards of care" for how to handle and protect shipments certainly will benefit from avoiding freight loss and damage. But they also will benefit from reduction in claims administration and lower insurance premiums" (Rice and Caniato, 2003, p. 30). Each year, there are several lawsuits that are entered into to determine to what extent, if any, shipping companies are liable for the theft or damage to cargo. As it relates to multi-modal transportation of goods, shipping companies are often faced with the burden of proof in demonstrating that the damage or theft has occurred on a separate leg of the cargo's journey. This lends to significant investigation and litigation costs that could possibly be avoided with the implementation of RFID seals. The following provides two such examples whereby the use of RFID seal technology may have prevented the need to engage in litigation.

Hauhaea v Laurabada Shipping Services Ltd [2005][19]

The plaintiff arranged with the defendant company to ship goods on two occasions. On both occasions a portion of the shipment was not received by the plaintiff and recorded as lost. The plaintiff sought to recover for these losses on the contract of carriage contained in the Bill of Lading. The complainant argued that the goods were not lost before loading or after discharge from the ship.

Decision: Claim dismissed.

Held: Clause 6 of the Bill of Lading expressly limits the liability of the defendant to losses incurred during the time that the goods were on the ship. As such the onus is on the plaintiff to prove that the loss occurred during the period from when the goods were

[19] Hauhaea v Laurabada Shipping Services Ltd [2005]. Retrieved from : http://www.paclii.org/maritime-law/case-summaries-sea-carriage/

loaded to the time the goods were discharged as per the Sea Carriage of Goods Act 1951. The plaintiff failed to discharge the onus.

Although the plaintiff in this case failed to transfer the burden of proof to the shipper in this instance, it is still recognized that the case may have not even been necessary if it could have been easily determined where the theft of cargo resulted. Such a determination could possibly be made with use of an electronic seal.

Alcoa, Inc. v. CP Ships (UK) Ltd., 2007 ONCA 686[20]

The Plaintiff contracted with the first Defendant for the carriage of a cargo of aluminum from Massena, New York to Italy. The first Defendant had an arrangement with the second Defendant for the performance of the inland portion of the carriage from Massena to Montreal. It was intended that the first Defendant would then complete the carriage by sea from Montreal. However, during the course of the inland transit the container was stolen when left unattended by the truck driver. The main issue in the case was whether the Defendants were entitled to limit their liability for the loss pursuant to the terms of the first Defendant's standard bill of lading. The Plaintiff argued that a document entitled Straight Form Bill of Lading had been issued when the cargo was picked up by the second Defendant and that this bill of lading, which contained no limitation clauses, governed. The trial Judge held, however, that this bill of lading was a mere acknowledgement of receipt. The trial Judge noted that on four prior occasions the Plaintiff had shipped goods with the first Defendant and that on each occasion the Defendant had issued its standard form bill of lading. Based on this prior practice, the

[20] Alcoa, Inc. v. CP Ships (UK) Ltd., 2007 ONCA 686. Retrieved from: http://www.admiraltylaw.com/summary.php?case_id=272

trial Judge held it was this bill of lading which governed even though it had not been issued at the time of the loss. The trial Judge next considered the Himalaya clause and the multi-modal clause in the bill of lading and concluded that they applied to the benefit of both Defendants. Finally, the trial Judge considered and rejected an argument that there had been a fundamental breach by the Defendants, noting that there was nothing deliberate about the conduct of the Defendants that would warrant denying them the protection of the limitation clause. In result, the Plaintiff was awarded $4,000 being the limitation amount in the bill of lading.

On appeal, the Ontario Court of Appeal held that the trial Judge had applied the wrong limitation provision. Specifically, the bill of lading provided various limits depending on where the transport occurred. The trial Judge applied the limitation for “Multi-Modal Transport outside the United States where COGSA is not contractually applicable”. The Court of Appeal said the appropriate clause was the one dealing with multi-modal transport in Europe or within a state other than the United States. This provision gave a higher limit of $65,000.

A provision for the use of an electronic seal incorporated into the contract of carriage for multi-modal transport could possibly serve to relieve the shipper of any liability for loss or damage to goods that can be proven to have occurred on a mode of transport other than marine.

Direct economic impact of Container theft

As containerized trade continues to grow, supply chain security plays an important role in the world economy. “The risk of theft, especially if the goods have a black market

value, is very real. Worldwide, the direct cost of cargo theft is estimated at about US $50 billion per year, with an indirect cost many times higher" (Kreowski et al, 2008, p. 464). Containers are most vulnerable when they are being loaded and unloaded to different modes of transport. The added layer of security provided by the RFID seal may serve as a deterrent to any entity that may be conspiring to commit theft. It should also be considered that in addition to the potential economic impact, companies who are impacted by pilferage and theft also face the risk of having their reputation negatively affected. "Electronic seals with their track-and-trace ability, not only ensure the container supply chain, but also gain supply chain efficiency from automatically tracking containers…damage to intangible assets and the contingent losses which could arise in cases where e-seals are not used are even greater" (Kreowski et al, 2008, p. 464). It should also be taken into consideration that "pilferage from the container or theft may lead to the loss of sensitive information or intellectual properties" (Kreowski et al, 2008, p. 464). The anti-tamper and alerting protection provided by RFID seal technology has the potential to be invaluable to industry in this regard.

Streamlining Port Facility Operations for Improved Efficiencies

The integration of RFID seal technology into port facility operational procedures may not only increase security but also optimize business practices providing a return on investment. As the number of containers being imported and exported via port facilities increases, operators are being met with growing pressure to provide efficient and cost-effective services that also meet specific security standards. "Terminals are faced with more and more containers to be handled in short time at low cost…therefore, they are forced to enlarge handling capacities and strive to achieve gains in productivity"

(Kreowski et al, 2008, p. 464). The ability of port operators to meet such high demands also speaks to their ability to remain competitive. The incorporation of RFID technology into regular port operations for handling containerized cargo can allow for demands to be met in a secure and efficient manner.

Stakeholder engagement will be necessary to demonstrate the benefits that can be recognized by the incorporation of RFID seal technology. “In order to gain their support for such efforts, as well as to assure that these efforts are realistic and effective, industry should be consulted and brought into the process at an early stage” (Dalhman et al., 2005 p. 24).

It is fair to state that the current standard required for use by such entities as C-TPAT and PIP could be greatly improved upon by incorporating the use of available RFID technology. The implementation however, will be no easy task and will require the combined efforts of industry and government working together to build a framework and associated policies that provide for the gradual positive change. The maritime industry, in particular, is globally regulated and handles large volumes of containerized cargo daily. Countries that are signatory to the IMO have adopted conventions and developed legislation that provides for regulations that are accepted as a global standard on maritime issues that relate to safety and security. Further, industry in order to comply with such regulations and by extension, to remain competitive, are very involved in contributing to the development of regulations and policies that provide for safe and secure shipping in a global market. The following chapter provides recommendations how existing organizations, law makers and industry can work together to leverage the use of RFID technology in container seals.

Chapter 5

It is important to note that the following recommendations provided will require intensive and transparent outreach and engagement to ensure that industry is provided ample time to participate in the process of formulating a framework for implementation. Additionally, it will be instrumental to ensure that the benefits of the use of RFID technology are presented to demonstrate that any initial financial implications can be offset over a relatively short time frame.

5.1 Recommendations

5.1.1 Partners in Protection (PIP) and Customs-Trade Partnership Against Terrorism (C-TPAT)

The Canadian and USA programs, PIP and CTPAT, respectively, are currently very aligned and both indicate in their seal requirements the use of ISO Standard 17712. It is important to reiterate that participation in the C-TPAT and PIP program is largely voluntary; however, it is also fair to state that they have evolved into an industry norm and have essentially become compulsory for any company who wishes to remain at a competitive advantage. Industry has been largely engaged in meeting the requirements of the program and enjoys incentives such as reduced inspections as a result. It is recommended that the CBSA work with the CBP to focus efforts on improving the security of supply chain by jointly amending the seal requirements to ensure the use of the new ISO standard, ISO 18185, at a minimum on all imported and exported containers. It is suggested that this be carried out by introducing a phased approach to ensure that industry is granted adequate time to meet the necessary requirements and

so that shore facilities have ample opportunity to procure equipment and provide training to personnel with respect to the use of equipment that will be required to check RFID seals.

5.1.2 Marine Transportation Security Regulations

In Canada, the MTSR were developed pursuant to the Marine Transportation Security Act (MTSA) and in line with the ISPS Code. The MTSR, Part 3, is dedicated entirely to Marine Facilities, including container facilities. Section 334 of the MTSR outlines the general procedures for Cargo handling that are to be implemented at Marine Security (MARSEC) Level one, two and three. In general, the regulations state that "a marine facility security plan shall contain security procedures, as appropriate to the facility's operations, for cargo handling for each MARSEC level for deterring tampering and detecting evidence of it (s.334). Additionally, the regulations state that the facility is responsible to coordinate with the shipper and other persons responsible for cargo. The regulations do require facility operators to routinely inspect "cargo, containers, cargo transport units and cargo storage areas in the marine facility before and during cargo operations to detect evidence of tampering" (s.335(b)). Further, facility operators are required by the MTSR to have procedures in place to allow for the "examining of seals and other methods used to detect evidence of tampering when cargo, containers or cargo transport units either enter the marine facility or are stored there" (s.335(d)). The regulations do not prescribe exactly what measures are required to be in place.

It is recommended that the MTSR pursuant to the ISPS Code be used as an instrument for gradual change in the industry requirements. Specifically, regulatory entities, such

as Transport Canada, responsible for the enforcement of the MTSR, ensure that industry has approved procedures in place that align with the use of RFID seals and the associated electronic equipment and necessary training for adequate implementation. It is further suggested that funding be allocated under government initiatives through grants and contributions to assist with ensuring that industry has technical capacity to implement requirements of ISO 18185.

5.2 Further Research and Study

The research completed for this graduate project has outlined existing vulnerabilities with the ISO 17712 standard and national requirements for mechanical seals and has attempted to demonstrate the utility and advantages of implementing RFID technology to increase supply chain security, particularly in the marine mode of transportation. It should be noted however, that additional research is required to demonstrate how best this technology can be implemented globally.

Specifically, further study should be devoted to determining which common frequency should be used for transmitting the data. Additionally, research is required to determine what infrastructure is required and how best it can be incorporated into existing logistical systems. This may prove to be especially challenging for less developed nations that have limited technological capacity. Finally, further consideration should be given to exactly what data elements are to be transmitted regarding the cargo. This should be approached with the view of improving industry efficiencies as well as supply chain security.

5.3 Conclusion

Before the events of September 11th, 2001, security measures put in place on containerized cargo were there mainly to prevent and/or detect theft. Since that time, regulations and procedures have shifted focus so as to deter the introduction of illegal and illicit substances that have the potential to cause harm to individuals and to the transportation systems and supply chain.

It is fair to state that where vulnerability exists in the supply chain, it will be exploited in some way or another. Global participation from industry and governments will be essential in establishing mitigation strategies. New technologies to enhance supply chain security should be embraced with the understanding that there will always be a group of individuals who will endeavour to exploit and supersede them for their own gain. This however should not be a reason to not pursue the best available options to increase supply chain security as well as to protect the financial interests and reputations of shipping companies worldwide as well as improving logistical efficiencies.

The RFID container seal is a proven technology. With a robust framework and industry acceptance, the technology can have a positive influence on supply chain security and by extension, the protection of goods, people and infrastructure and a company's bottom line.

References

Analysis Report 2008. Retrieved from http://www.wcoomd.org/~/media/cen/member/wco-documents/container-analysis-report-2008-en.pdf

Canada Border Services Agency (CBSA). (2014). *Partners in Protection: Fact Sheet.* Retrieved from http://www.cbsa.gc.ca/security-securite/pip-pep/facts-faits-eng.html

Canada Border Services Agency (CBSA). 2015. *Partners in Protection Cargo Sealing Guidelines for PIP Members*. Retrieved from http://www.cbsa.gc.ca/security-securite/pip-pep/seals-scelles-eng.html

Chawla, V., & Ha, D. S. (2007). An overview of passive RFID. *IEEE Communications Magazine*, *45*(9).

CHEP. 2014. *CHEP Pallecon Solutions Recognized as Supply Chain and Technology Innovator*. Retrieved from http://www.chep.com/resources/media_releases20140116_CHEP_Pallecon_Solutions_Recognized_as_Supply_Chain_Innovator/

Closs, D. J., & McGarrell, E. F. (2004). *Enhancing security throughout the supply chain*. Washington, DC: IBM Center for the Business of Government. pp. 10-12.

Cuthbertson, M. 2010. ICAO MRTD & eMRTD Standards and Specifications. [PowerPoint Presentation]. Retrieved from http://www.icao.int/Meetings/AMC/MRTD-SEMINAR-2010-AFRICA/Documentation/5_CuthbertsonChalmers%20_MRTD-eMRTD.pdf p7.

Dahlman, O., Mackby, J., Sitt, B., Poucet, A., Meerburg, A., Massinon, B., & Alewine, R. (2005). *Container security: a proposal for a comprehensive code of conduct*. National Defense University: Washington DC, Center For Technology And National Security Policy. Retrieved from http://www.cesim.fr/documents/publications/Container_Security_NDU_Report.pdf).

Daschkovska, K. (2015). *Electronic Seals and their Influence on the Dynamics of Container Logistics* (Doctoral dissertation, Bremen, Universität Bremen, Diss., 2015).

Dimakopoulou, A. G., Pramatari, K. C., & Tsekrekos, A. E. (2014). Applying real options to IT investment evaluation: The case of radio frequency identification (RFID) technology in the supply chain. *International Journal of Production Economics*, *156*, 191-207.

Dontharaju, S. R. (2007). *Design Automation for Low Power RFID Tags* (Doctoral dissertation, University of Pittsburgh). Retrieved from https://pdfs.semanticscholar.org/0ee6/0f168408a95ef08436301475b02a844dfcaa.pdf

Ducruet, C., & Notteboom, T. (2012). The worldwide maritime network of container shipping: spatial structure and regional dynamics. *Global networks*, *12*(3), 395-423.

Government of the United States. (January 2012.) *National Strategy for Global Supply Chain Security.* Washington, DC: U.S. Government Printing Office.

ICAO. 2015. *Machine Readable Travel Documents.* Doc 9303: Seventh Edition. Retrieved from http://www.icao.int/publications/Documents/9303_p1_cons_en.pdf

International Civil Aviation Organization (ICAO). 2017. *Security.* Retrieved from http://www.icao.int/Security/Pages/default.aspx International Organization for Standardization (ISO). 2017. *About.* Retrieved from http://www.iso.org/iso/home/about.htm

ISO. 2007. *Freight containers -- Electronic seals -- Part 1: Communication protocol.* Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=41125

ISO. 2013. Freight Containers – Mechanical Seals. Retrieved from https://www.iso.org/obp/ui/#!iso:std:62464:en

Johnston, R. (2006). Tamper-Indicating Seals From the earliest civilizations to the present, seals have provided evidence of unauthorized access. *American Scientist*, *94*(6), 515-523.

Johnston, R. G., Martinez, D. D., & Garcia, A. R. (2001). Were ancient seals secure? *Antiquity*, *75*(288), 299-305.

Kreowski et al, (2008). Electronic seals for efficient container logistics. In Dynamics in logistics (pp. 305-312). Springer Berlin Heidelberg.

Kumar, V. N., Srinivasan, B., & Narendran, P. (2012). Efficient implementation of electronic passport scheme using cryptographic security along with multiple biometrics. *International Journal of Information Engineering and Electronic Business*, *4*(1), p. 18.

Mapplebeck, G. 2009. *Container Security: Challenges for Seaports* [Powerpoint Presentation]. Retrieved from World Customs Organization Web Site http://www.wcoomd.org/~/media/wco/public/global/pdf/events/2010/technology-forum/panel-presentations/graham_mapplebeck_imo.pdf

McConnell, M. (2016). The ILO's Seafarers; Identity Documents Convention (Revised), 2003 (n. 185) after more than a decade: Ahead of its time or case of good intentions gone wrong?

Mehrjerdi, Y. (2010). RFID-enabled healthcare systems: risk-benefit analysis. *International Journal of Pharmaceutical and Healthcare Marketing*, *4*(3), 282-300.

Mundo Maritimo. (2007) Container Tracking: RFID vs. Satellite. Retrieved from http://mundomaritimo.cl/noticias/container-tracking-rfid-vs-satellite

Min, J.U., and Park, M. (2007). Electronic cargo seal for safe and secure supply chain traceability. *Journal of International Logistics and Trade(5)*1, p. 47-56.

Riahi, L., Li, K., Robertson, I., Jenkinson, I., Bonsall, S., Wang, J. (2013). A proposed decision-making model for evaluating a container's security score. *Journal of Engineering for the Maritime Environment, 228*(1), p. 81-104.

Rice, J. B., & Caniato, F. (2003). Building a secure and resilient supply network. *Supply Chain Management Review, (7)*5, p. 22-30.

Rizzo, F., Barboni, M., Faggion, L., Azzalin, G., and Sironi, M. (2010). Improved security for commercial container transports using an innovative active RFID system. *Journal of Network and Computer Applications, (34),* 846-852.

Rodrigue, J. P., & Notteboom, T. (2009). The terminalization of supply chains: reassessing the role of terminals in port/hinterland logistical relationships. *Maritime Policy & Management*, *36*(2), 165-183.

Siror, J. K., Huanye, S., & Dong, W. (2011). RFID based model for an intelligent port. *Computers in industry*, *62*(8), 795-810.

Statistics Canada. 2015. *Shipping in Canada 2011.* Retrieved from http://www.statcan.gc.ca/pub/54-205-x/2011000/part-partie1-eng.htm).

SteadieSeifi, M., Dellaert, N. P., Nuijten, W., Van Woensel, T., & Raoufi, R. (2014). Multimodal freight transportation planning: A literature review. *European journal of operational research*, *233*(1), 1-15.

Thibault, M., Brooks, M. R., & Button, K. J. (2006). The response of the US maritime industry to the new container security initiatives. *Transportation Journal*, *1,* 5-15.

US Customs and Border Protection. 2014. *Compliance with ISO's 17712 Standards for High Security Seals.* C-TPAT Bulletin. Retrieved from

https://www.cbp.gov/sites/default/files/documents/Bulletin%20-%20April%202014%20-%20ISO%2017712%20High%20Security%20Seals.pdf

US Customs and Border Protection. 2017. *[INSERT TITLE]*. Retrieved from https://www.cbp.gov/sites/default/files/documents/CBP-Vision-Strategy-2020.pdf page 16

US Department of Homeland Security. 2017. *C-TPAT: Customs-Trade Partnership Against Terrorism*. Retrieved from https://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-partnership-against-terrorism

Venus Lun, Y.H., Wong, Christina W.Y., Lai, Kee-Hung, Cheng, T.C.E. (2008). Institutional Perspective on the Adoption of Technology for the Security Enhancement of Container Transport. *Transport Reviews(28)*1, p. 21-23.

Vikan, G., & Nesbitt, J. (Eds.). (1980). *Security in Byzantium: locking, sealing, and weighing* (No. 2). Dumbarton Oaks center for Byzantine studies.

Willis, H. H., & Ortiz, D. S. (2004). *Evaluating the security of the global containerized supply chain*. RAND CORP SANTA MONICA CA.

World Customs Organization (WCO). 2007. WCO Safe Framework of Standards. Retrieved from

World Customs Organization (WCO). 2008. Global Container Analysis Report. Retrieved from http://www.mcmullinpublishers.com/downloads/OMDrcEN08.pdf

World Customs Organization (WCO). 2015. *The UNODC-WCO Container Control Programme*. Retrieved from http://www.wcoomd.org/en/topics/enforcement-and-compliance/activities-and-programmes/drugs-programme/unodc_wco_container_control_programme.aspx

Yang C.-C., Wei H.-H. The effect of supply chain security management on security performance in container shipping operations (2013) Supply Chain Management, 18 (1) , pp. 74-85. Retrieved from http://www.emeraldinsight.com/doi/pdfplus/10.1108/13598541311293195

Zelbst, Pamela, and Victor E. E Sower. RFID for the Supply Chain and Operations Professional. New York, N.Y.]: Business Expert Press, (2016). Web.