LAUREA
UNIVERSITY OF APPLIED SCIENCES
Together we are stronger

PORT SECURITY-Threats and Vulnerabilities

Case: Takoradi Port

Kusi, Bernard

2015 Leppävaara

Laurea University of Applied Sciences
Leppävaara

PORT SECURITY-Threats and Vulnerabilities

Case: Takoradi Port

Bernard Kusi
Degree Programme in Security Management
Bachelor's Thesis
October 2015

Laurea University of Applied Sciences
Leppävaara
Degree Programme in Security Management
Bernard Kusi

Abstract

Port Security-Threats and Vulnerabilities

Year 2015 Pages 55

The main objective of this thesis is to identify the threats and the vulnerabilities concerning Takoradi port, and finally recommend measure to overcome the identified threats and vulnerabilities. Various categories of potential threats and vulnerabilities have been studied throughout the literature review. However, because each port presents a unique sets of threats and vulnerabilities, there was a need to look critically into how Takoradi port operations are being conducted in other to identity the potential threats and vulnerabilities pertaining to the said port.

This study applied Case Study Approach as a research strategy by using Qualitative research method as a means of exploring and understanding how individual or group ascribe to social or human problem, and also identify new theoretical propositions or managerial actions is needed. The empirical data for this study was collected through primary and secondary sources. With primary source, questionnaire, observation as well as informal discussion were used. Whereas with secondary source, raw data and publish summaries that have been collected by organizations and individual, excluding researchers were used.

The results of the study revealed the strength and the vulnerabilities within security system at the port of Takoradi. Apart from the strength and weaknesses, potential threats that confront the security systems, were also identified through the result. This thesis provides the recommendation needed to tackle the identified vulnerabilities and threats that are likely to disturb the effectiveness and efficient operating of the security systems.

In the future, it is important to identify how human factor impact the successful implementation of port security measures. Further research in this particular area will help reduce the threat that human factor poses to the successful implementation of Port security measures

Keywords: Threats, Vulnerabilities, Cargo Security, and Supply Chain Security

Table of contents

List of Abbreviations and Symbols

AIS	Automatic Identification Systems
BNI	Bureau of National Investigations
CCTV	Closed Circuit Television
CSI	Container Security Initiatives
CEPS	Custom Excise and Preventive Services
C-TPAT	Customs-Trade Partnership Against Terrorism
EEZ	Exclusive Economic Zone
EUAEO	European Union's Authorized Economic Operators
GIFF	Ghana Institute of Freight Forwarders
GMDSS	Global Maritime Safety and Distress Systems
GPHA	Ghana Ports and Harbours Authority
GRA	Ghana Revenue Authority
IAPH	International Association of Ports and Harbours
ILO	International Labour Organization
ISO	International Standard Organizations
ISPS	International Ships and Port Facility Security
IMO	International Maritime Organization
IMOC	International Maritime Organization Convention
LOSC	United Nations Convention on Law of the Sea
MTSA	Maritime Transportation Security Act 2002
OECD	Organization for Economic Cooperation and Development
PFSP	Port Facility Security Plan
SAFE Port Act 2006	Security and Accountability for Every port Act 2006
SLOC	Sea Lines of Communication
SOLAS	Safety of Life at Sea
SUA	Suppression of Unlawful Act
UNCTAD	United Nations Conference on Trade and Development
VTMIS	Vessel Traffic Management Information System
WCO	World Custom Organization

1 Introduction

This section of the study presents a brief outline of the research, the problem and objective of the research. It goes further to explain research questions, delimitation and structure of the study.

1.1 Background

Thomas Friedman (2007,8) described in his book entitled, “The world is Flat”, that the interconnected global economy enabled by advances in Information and Communications Technology and other factors that he terms “Flatteners”, does not only empowers the software writers and the computer geeks to collaborate on the work in the flat world, but also AL Qaeda and other terrorist networks. The playing field is not being levelled only in ways that draw in, and super empower a whole new group of innovators, but also a whole new group of angry, frustrated, and humiliated men and women”. Organization for Economic Cooperation and Development (OECD, Paris: July 2003) reported, “The world pattern for global prosperity has been predicated on near-frictionless transport and trade." Seaport is a crucial component of the world economy and global transportation infrastructure, Nevertheless generally there hasn’t been a comprehensive governmental regulation and security oversight. The terrorist attacks of 11th September 2001 that collapsed the World Trade Centre and Pentagon in the United States, has significantly impacted multitude of sectors internationally. The tragic incident has brought radical change in the maritime industry. One of the major elements that arose in the response to that attack was the approach to security. This change led to change in the manner in which security is being conducted and practiced, due to the numbers security measures, rules as well as regulation to avoid such incident in the future. International Maritime Organization (IMO) and U.S have implemented several measures after the tragic event, for the purpose of heightening the security of maritime business. For instance, International Ships and Port Facility Security (ISPS) Code, was ratified by International Maritime Organization in 2002, and called on every member states to apply the code by 2004. The Maritime Transportation Security Act 2002(MTSA) and the Security and Accountability for Every port Act 2006(SAFE Port 2006) by United State was designed to improve national maritime security though, these two Act have international elements planned to strengthen security of the facilities by which Goods destined to United State are travelled. The main focuses were on the vulnerabilities of the ships and the port facilities, which could be exploited by the terrorist and other criminals. Though the current security measures have enhanced some aspects of security at Takoradi port, yet some of the vulnerabilities, which are crucial, still hang out. The current regime has made security at the port very rigorous, for instance strict measures regarding containerized cargo. Port security measures could be infiltrated by terrorist or illicit traffickers, if appropriates mechanism are not put in place to verify identities, credentials,

and the intention of individual, ships or cargo arriving at the port. This thesis shall define research problem and the objective, then the issues relating to port security threats and the vulnerabilities, including its economic impacts on the port. Also how port security measures have been applied in Port of Takoradi shall be demonstrated. Though, current security regime have enhance some part of the port security, nevertheless they have failed to tackle the important vulnerabilities which terrorist and other criminals are capable of exploiting. Despite the fact that there is strong physical security at the ports, as well as the strict inspection rules for the containerized cargo, the absence of mechanisms to verify the identities and credentials of every individual who has access to the ports, secure non-containerized cargo, and prevent criminal from accessing and exploiting the port facilities, the whole port security measure can be undermined.

1.2 Problem Discussion

All sections within Ghana and international community have welcomed the breakthrough of offshore oil and gas in the Western part of Ghana. Ghanaians have is expectation that this breakthrough will bring significant economic benefit to Country. Takoradi Port being the main facility for receiving ships and transferring cargoes, the offshore oil and gas exploitation and development, has brought enormous responsibilities and challenges to the port Authorities and the users. The significant issues among, is how authority is going to manage the security, safety and environmental issues that will arise over the next decade. The challenge is that, offshore oil and gas extraction includes a complex net of ships, structures, installations and people, all interacting with each other. These activities raise concern to security, safety and environmental protection considerations at a high level of intensity, at this time that the offshore production is in full swing. Therefore there is the need to identify the related threats and vulnerability to be able to develop a comprehensive, but resilient security system to deal with the threats and vulnerabilities.

1.3 Research Objectives

The main objective of this thesis is to identify the threats and the vulnerabilities concerning Takoradi port in Ghana, and finally recommend measure to overcome the identified threats and vulnerabilities.

1.4 Research Question

The research has recognized, and seeks to answers the main question of “how to develop resilient security system for Takoradi Port? This question came to mind after reading various concerns regarding the security of the maritime commerce. In trying to answer the main

question, the following question also came to mind: (ii) has there been any security incident linked to Takoradi Port? (ii) If yes, how many time are those incidents linked to Takoradi Port? (ii) How do those incidents happen? (iii) Are there in place, security measures to prevent those incidents? (iv) Are those measures, effective to prevent potential security incidents? These prompted me to develop a questionnaire to search for the information regarding the existing security control measures, including vulnerabilities and threats associated with the security control measured, as well as operational activities within the port.

1.5 Delimitation

The theoretical part covers analysis of various literature sources that describe the international maritime regulations and requirements for shipping industries and ports as well as the weaknesses and the strengths of the regulation. Moreover, it shall describe the threats and the vulnerabilities regarding the shipping industries and the ports, including the competitive and economic impact on the ports. The theoretical framework shall be developed to describe the threat and vulnerabilities relating to the port and the measure to overcome the threat and vulnerabilities base on the literature review. The empirical part-case study will focus on the analysing the threats and vulnerabilities concerning Takoradi port. The case study will be restricted to only Takoradi Port. Other threats that can adversely impact the security system including the port operation shall be considered. For instance, threat from the supply chain.

1.6 Thesis Chapter Structure

Thesis is divided into Five (5) chapters. The chapter 1 presents the thesis background, the research problem, objectives, research question as well as delimitations. Chapter 2, covers the review of various literature sources regarding the current maritime security measure for ships and ports, maritime and port security threats and vulnerabilities, supply chain/cargo security and it likely economic impact on the competitiveness on the port the. Chapter 3 contain the strategy and methods used in collecting the data. Chapter 4 contains profile of the Takoradi Port and Security Measures in place. Chapter 5 present the results, analysis of empirical data,conclusion and recommendations.

2 The Theory

This chapter presents the various theoretical conception to enable establish clearer understanding and knowledge regarding port security.

2.1 Security Regulations and Requirements for Ships and Ports

The preceding chapter explains the thesis background and the problem, research objective and question, delimitation and the chapter structure. However, this part gives brief explanations on the various regulations and requirements for ports and ships.
Ships are a registered in their respective countries and for that matter has their own legal status. However, because they travel throughout the world and enter another country's seaport, the port state has the right to enforce supervisory obligations on any ship that enters their waters as well as applying international requirements to which the flag state is signatory. Regarding the regulatory requirement, there are international treaties and codes as well as national regulations related to security. The following are the main international treaties and code that influences the port states supervisory effort:

We have 1982 United Nations Convention on Law of the Sea (LOSC), which tackles the full range of legal issues affecting the seas and it's relevant to both port and the flag states. Examples of issues are; environmental protection, regional cooperation, disputes resolution, territorial sea and many more.

There is also 1948 International Maritime Organization Convention (IMOC) as a specialized group of the United Nations, which concentrates particularly on maritime issues such as marine safety, marine environmental protection, and marine security including marine legal systems.

I974 International convention for the Safety of Life at Sea and its Protocol of 1978(SOLAS 74/78), is convention intended to govern maritime safety and security, which form the basis for several port states regulations such as lifesaving requirements, navigational safety, crew licensing and competence as well as vessel management. Beside these, International Ship and Port security (ISPS) Code is also incorporated into the convention, which form the key standard for maritime security for ships and the ports.

Last but not the least is the 1988 convention for suppression of unlawful Act against the safety of maritime Navigation (SUA). It has the following key element; first it empowers the country over any criminal or violent acts carried out on vessels based on the vessel flag, location or the nationality of the wrongdoer. Besides, it mandates the country with the given authority to either prosecute suspected wrongdoers or deport them to different location for prosecution. There is an added protocol that deal with the potentially terrorist related crimes. For instance using the ship as weapon or transporting terrorist, weapon of mass destruction or other related substances and cargo. (Edgerton, M. 2013, 17-18)
Some countries have developed their own internal legislation to improve the implementation of the port-state security obligations. However, for the sake of this project, the detail expla-

nation shall not be given. Below are some of the national regulations and legislative instruments:

UK Statutory Instrument No.1495: 2004: The ship and port facility security regulations 2004

2002 US marine Transportation Security Act (US MTSA)

Australian Maritime transport and Offshore Facilities Security Act 2003(Australian MarSec Act) (Edgerton, M. 2013,19)

2.2 International Ships and Ports Facility Security (ISPS) Code

The previous section explained the security regulations and requirements for ships and ports. However this part briefly explains the International Ships and Port Facility Security (ISPS) Code, which is the current international regime for safeguarding international ships and port facility. It was introduced after the September 11 attacks on United States of America in 2001. International community through convention agreed on the need to develop new security regime to detect security threats and take preventive measures against security incidents affecting ships or port facilities used in international commerce. In respond to this threat, International Maritime Organization developed International Ship and Port Facility Code (ISPS) through co-operation among Governments, Government agencies, local administrations and shipping and port industries. An amendment was made to the 1974 Safety of Life at Sea Convention (SOLAS) in 2002 to enhance maritime security (IMO.2002.SOLAS/CONF.5/31, 1). International Ship and Port Facility Security (Code) is set of security measures to heighten the security of the Ships and Port Facilities, which was developed to respond to the potential threats to ships and ports facilities. The main derive of the ISPS code is to create a standardized, consistent plan for analysing risk. This will assist governments to determine the right security levels with parallel security measure and to balance the changes in threats as well as changes in vulnerabilities for ships and port facilities. (IMO.2004.IMO Security Measures)
The ISPS code consists of two major parts: “A” and “B”.

Part A of includes the detailed requirements for governments, port authorities and chipping companies, whereas Part B serves as guidance by which these requirement would be met, and it’s not mandatory. It includes series of resolutions adopted by the Conference for the purpose of improving maritime security on board of ship, and at ship/port interface area. Measure to mitigate risk and responsibilities relating to the three levels of security are stipulated in Part the A. The requirement also gives the state right to impose control and compliance measures on any ship that visit the port. Contracting Governments are being mandated by the ISPS Code to take necessary or further action whenever the ISPS code make no provi-

sion for such situation. Moreover, to better communicate the threat at the port facility or for a ship, ISP code requires Contracting Government to set appropriate security level. Security level 1(one) represent the normal threat situation. Whereas security level 2, represent medium threat situation. Security level 3, represent high threat situation. ISPS demands both Ships and ports to develop security port plan based on the security assessment. It also requires both ships and Ports to have designated security officers who will deal with all the security related matters on behalf of their company or organization (IMO Briefing 42/2002). Regarding access to the Port Facility, under the section 16.12 of ISPS Code, Port Facility Security Plan (PFSP) ought to establish each security level, means of identification, which is required to permit individual to enter the port facility and perform their respective functions without any difficulties. These may require developing a proper identification system, which will permit permanent and temporary identifications for both regular staff of the port and visitors.

Section 16.17, under security level 1, require Port Facility Security Plan (PFSP) to establish the control points at restricted areas, which must be controlled by fencing or other barriers, up to a required standard for checking identification of individual, who wish to access the port facility to carr yout their respective assignment. Section18.4 under the ISPS Code stipulates the requirement and the main objective for drill and Exercises. For port facility personnel to perform the assigned security duties, at all security levels, and be able to identify any shortfalls related to security, drill and exercises must be carried out at regular interval. Section 18.5 of ISPS Code regard drill and exercises, require drill to be conducted at least quarterly, unless otherwise its influence by specific circumstances. It was stipulated under the Section18.5 of ISPS Code that, all form of exercises that involves the participation of port facility security officers, as well as relevant authorities of contracting governments, company security officers, or ship security officers, if possible ought to be conducted at least annually with no more than 18 months between the exercises. Because each port and the ship present unique and diverse risk, the contracting governments have the responsibility to comply with the ISPS Code measure that they believe it is right. Regarding SOLAS, IMO a body has no responsibility under the convention to monitor compliance; instead, the provision has been made for individual contracting government to adopt the rules into their national or local legislation. Several international treaties have been designed to tackle the other aspect of maritime security as result of ISPS Code. For instance, security regarding merchant seamen is another aspect to be dealt with in ensuring secured maritime security. To tackle the security issues whiles guaranteeing the right of global merchant seamen; International Labour Organization through convention in 2003 drafted the revised seafarer's Identity Card, which was approved in 2004, to issue a standardized biometric ID card to the merchant seamen. (ILO-london.2005)

2.3 Critiques of current Maritime Security Measures and Approach

When developing policies for regulating international crime, it is very important to understand neoliberal power in worldwide governance. There is the need to recognize the relationship between biopolitics and neoliberalism to be able to construct a wider formation of laws and security strategies beyond the borders of the states. This is because there is fundamental relationship between development of procedures to regulate crime at international level and the establishment of the modern politico-economic theory, which favours free trade, minimal government intervention in business etc. Bio politics focus on protecting and caring for the wellbeing of the citizens. Whereas Neoliberalism emphasis on free trade, privatization, minimal government intervention in business, reduced public expenditure on social services and so on. That is why controlling crime at global level requires the understanding of the relationship or the features between biopolitics and neoliberalism, since they represent some key determinants factors for securing/protection of society through managing populations and their businesses and other properties (Nieto, D. 2012, 137-143). Notwithstanding that, consideration must be given in respect to the resources and technical Know-how of the states, multinational actors, and economic interest. A country may be motivated to comply with or follow international rules/policies due to lack of unilateral and bilateral law enforcement measures in the face of criminal activities that surpass national borders. Besides that, religious beliefs, humanitarian sentiments, fears, prejudices, paternalism, faith in universalism, the individual conscience, and the compulsion to proselytize could also be influential factors (Ethan A. Nadelmann.1990, 481). Nevertheless, it is not always the case as stated above, positive incentives rather than negative could also inspire a state to comply with international regulation or rules. Within the domain of port security, this could be true, “highly compliant companies could enjoys certain benefits such as, facilitated clearance arrangements, an entitlement to self-assess, and reduced regulatory scrutiny, which provide compliant companies with the incentive to demonstrate their commitment to comply with regulatory requirements” (Widdowson, D & Holloway, S.2009, 20).

Effective maritime security cannot be single out within the purview of International trade, since it affect and impacted by numerous external factors. For instance, socioeconomic drivers, political priorities, transportation-system connected to business trends, as well as international event. Therefore, risk-based approach to security is vital when developing maritime security policies to regulate international commerce. Moreover, due to the complex nature regarding the interaction of port and ships, in addition to other economic interest, logistics, and transportation modes within the purview of maritime, security must be seen as element of system resilience and risk management (Edgerton, M. 2013, 141). So, in the process of devising security measures to regulate maritime business, adoption of credible risk management tactics is necessary to balance the commercial and security needs. Such security measures

must be selected based on carefully analysis. The right way to make these selections is by comparing the benefits of less- frequent, less-extreme terrorist events to the costs of security measures, direct and the indirect cost, as well as loses that arises as a result of long waiting lines at the port. For security measure to be considered efficient, marginal benefits must be equal or exceed marginal costs (Jon, D. Haveman & Howard, J. Shatz.2006 31).

When security strategies and measures are skillfully and appropriately designed, it functions as enablers, which permit constant cost-effective and reliable operation of industries, government services, and economies. Habitually, security is seen as a cost center in the commercial setting, nevertheless an approach whereby security is incorporated into daily business operation, security could be guaranteed, thus, offer resilience service to minimize the cost of disruption, and at the same time, reliability would be maximized as well as competitiveness of business operations" (Edgerton, M. 2013, 141). One of the major concerns by the maritime industries after the introduction of ISPS code was the economic impact that the new security measures would bring to their business operation, despite the fact that they agreed and welcome the need for tougher security measures (Wade, J. 2005, 41).
Another challenging and critical issues ahead of international maritime community is how the new security regime would be financed, and it effects on the maritime business. Nevertheless, same things, which have allow economic growth in maritime transport, also makes it vulnerable to be exploited by criminals or terrorist groups. The challenges that the shipping community would be facing are both immediate and long-term, in respect to the implementation of ISPS code. Among the various challenges is the costs of financing ISPS code implementation, and it commercial impacts on the different stages of their implementation (Alexandros and Agisilaos.2005, 472).

Despite some concerns about the costs of implementing ISPS code, there has been significant development in the global maritime commerce as a result of introducing ISPS code. According to Bichou, K. (2004,323) "International Ships and Port facility Security (ISPS) code is the most important global security initiatives ever, with impacts affecting the entire international shipping industry and beyond. "Though ISPS code has deeply impacted the entire maritime commerce, but since IMO has limited power to force the sovereign states to secure their ports, the term "port facility", which signify the area where vessels are covered by SOLAS, was created for the purpose of implementing ISPS code requirements. But it left to the IMO member state to declare which area of its ports falls within port facilities, which will be affected by the security requirements "(Nuthall, K., Fine, P., & Thomson, J. 2003, 84–87).

Even though some people argue that ISPS code and other post -2001 programs have positively impacted maritime commerce in one way or the other, nevertheless the code lack certainty, because of that, the organizations do not apply the policy and procedures up to the standard

requirements. For instance, instead of applying the technology, they use existing manpower. Considering the challenges in controlling such a large volume of people and vehicle in and out of the port, inspection of cargo, in addition to constant costly issues regarding waterside security. (Botelho, R. 2004, 18). Obviously the current regime does not address the wider security concern of the maritime commerce. According to Shah, S. K. (2004,32) "ISPS code may be good start to protect international shipping against physical terrorist attacks, but what appears to be missing is an emphasis on safeguards against vulnerabilities associated with information systems and technology."

The current maritime security measures do not tackle non-seaborne or Pier-side vulnerabilities related to the information system and the technology. Computers and communications system are the strength of modern-day business. Many activities in the international maritime commerce could not be successfully done without efficiency computer and communication networks. So, any attempt to ignore it, when safeguarding international maritime commerce, will make the maritime business vulnerable to be exploited by criminals or terrorists. For example, Terrorists may use a port's computer information systems to locate hazardous cargoes for their subsequent destruction. From the study of port security incident cycle, the following four different categories of potential port security incidents were identified: "Waterside, Landside, Employee and Information-release related" (C. Ariel Pinto and Wayne K. Talley, 2006, 270).

According to Michael Edgerton (2013), ISPS Code is "reasonably effective initial step in establishing low-low base line security in global shipping. It is because of the drastic differences in size, technological development, and resources available to ports, administrations and shipping companies around the world." Many are of the view that, U.S government has performed well in harmonizing the need for improved supply chain security, and the concerns of the industry's business. Nevertheless, some main concerns still remain (Thibault, M., Brooks, M. R., & Button, K. J. 2006, 13). Several concerns have been raised regarding the effectiveness of the new regime in securing the international supply chain, and their impact on cross-border commerce, whether the benefit of compliance will balance or outweigh the cost of implementing the program. For example, one of the concerns was fact that, ISPS Code's does not apply to fishing vessels and vessel with cargo not above 500 tones, meanwhile those vessels could be used for Piracy, smuggling of people and/or illegal goods (drugs, firearms, alcohol, etc.) and stowaways (John P. Hogan & Chapman, L. 2005, 24).

Primarily, ISPS Code do not address the supply-chain security concerns as the crucial security issues regarding maritime commerce, it emphases is on external threats. Because it attention is on the external threat, the criminals or terrorist could capitalizes on the vulnerabilities within internal security system to launch criminal activity or terrorist act. In addition ISPS

code mainly places and externally mandatory set of conditions on port and shipping companies, nevertheless does not inspire the development of security culture alongside daily operations, and within the organizational structure. Besides, there is absence of enticement for organizations that partaking beyond the minimum requirements of the code (Edgerton, M. (2013, 110–111). Several writings have identified some lapses within the current maritime security regime, pointing to the fact that, International Maritime Organization is unable to enforce the new maritime regulations, but can only monitor compliance. Simply because, according to Flynn, S. E. (2007), "ISPS compliance lies largely in the eye of the beholder, where each nation is allowed to determine whether its vessels or port facilities are up to par." The implementation of ISPS programs has encountered some difficulties. Accoding to International Maritime Organization (IMO), the last minute for the new regulations to be effected in 2004, "only 53 % of the world's shipping fleet had the security certificates to carry; with the same proportion of ports had the officially approved security plans that," (Perils on the sea. O7 July 2004,). With all the substantial amount resources spent on the ISPS Code implementation, the Code has been unsuccessful. In practice, it's the crew that ensures actual security of the vessel, and so, the number of the crew should have been increased, after the initiation of ISPS Code, but that was not the case. The situation turn to be the other way round, as shipowners demands the cost reduction by cutting down crew sizes. This is contrarily to the life force of the Code as initially envisaged (Bateman, S. 2009, 115). It may be unfair to focus on only the shortcoming of ISPS code. The report by OECD in 2003 on Security of Maritime Transport claimed, the benefit that comes from reduced delays, faster processing times, better asset control, and decreased payroll due to IT improvements, fewer losses due to theft, decreased insurance costs, and many more cannot be overlooked. In fact, some of the measures may slow the operations nevertheless many others may reduce trade costs. In an organization where there is much dependent on paper and fax transmissions, the savings that may accrued from more IT integrated system cannot be covered. Many more manufactures and shippers have already achieved much from increased productivity as result integrating IT in their supply Chain. Customs authorities, port and terminal operators are not excluded.

Some countries perceive the current maritime security regime as expensive, and for this reason they feel reluctant in complying with, for example China. It could also be that the perceived cost or how expensive the new security requirement is, may be reflected by the extent to which the country or the port view itself as a terrorist target. Nevertheless the cost of successful attack against the vital component of maritime trade such as oil transportation and other critical infrastructure could be much more than the cost of inaction (Perils on the sea; 2004).

Moreover, the International Chamber of Shipping claimed that, "the whole package of US legislation is potentially trade disruptive." In their opinion, there is the need for maritime secu-

rity framework that avoids costly information sharing and exchange, including privacy protection pitfalls implied by the US approach (Stasinopoulos, D. 2003, 318). United States (U.S) and international initiative is just an additional rule, procedures, and technology to improve security, whereas ways that people enter and operate within maritime system have not been changed (Harrald, J. R.2005, 175). One of main concern regarding the developing countries is that, the cost involved in acquiring technology and technical know-how for the implementation of ISPS and CSI, will prevent the small entities within developing countries, from competing in global trade. Survey conducted by International Association of Ports and Harbors (IAPH) among its member ports demonstrated some challenges. "70 % out of 53 member ports, which responded to the survey, were confident they would meet the deadline of July 1, 2004, 19 % were uncertain. The reason cited was due to financial constraints, lack of staff and expertise, and delay in legislative enactment and procedures by governing bodies and authorities". According to report, smaller ports and ports from developing nations called for information sharing and technical assistance, including guidelines, models and samples, as well as financial assistance, through the establishment of a funding plan to raise public finance for developing countries." (UNCTAD 2004, 20–34).

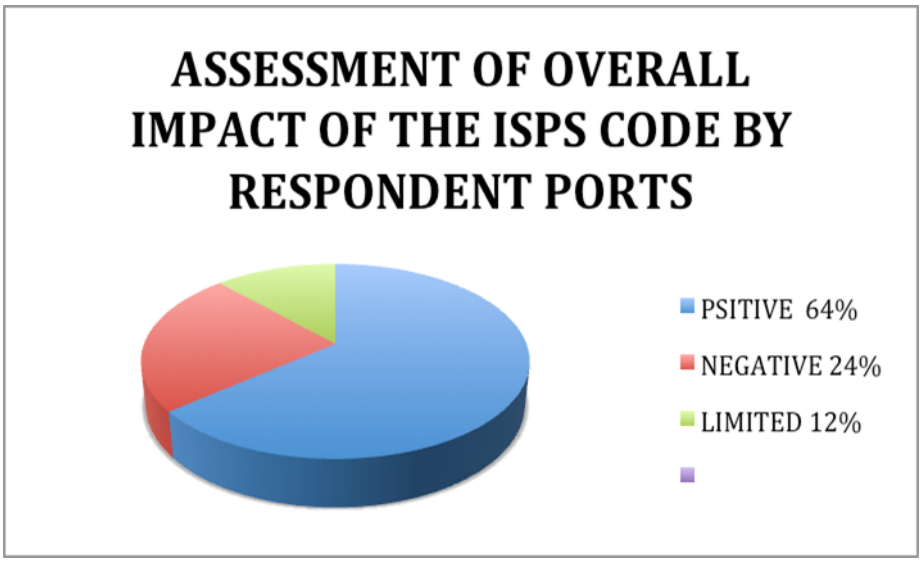
According Dr. Ikokide Zebulon (2014), Nigeria Port Authority started the implementation ISPS code on 1st July 2014, meanwhile ISPS code was supposed to be implemented since 2004, after the introduction. This was due to lack technical know-how, capacity and willingness to implement the measures. Report from the audit conducted by U.S government Anti-Terrorism Assistance in Kenya and Mozambique, in 2007 indicated that, both states needed to improve their port security standard, because their facility does not meet the standard for which successful implementation of ISPS code can be done (Kennedy, F. 2007). According to Langewiesche, W (2004,7) "It is not by accident that the more high-level technology pirate group and terrorist appear to imitate the operational techniques and method of ship owners, though their incentive and ideologies are different. Certainly, they have learnt to work without the need for home base, and most importantly to escape the forces of order not by running away, but complying with the laws and regulations to be able to move freely and to hide in the plain sight. Should they choose to comply with the new laws and regulations in order to move freely and to hide in the plain sight for their own gain, without a doubt, the ways and the manner in which ISPS has been implemented might be irrelevant." A research conducted about Port and Supply-chain Security Initiative in United States and abroad claimed that the people involved in the implementation of these recent initiatives have voiced out their distress regarding increased workloads, difficulty understanding the code, and communication difficulties, due to numerous acronyms and longer hours. However it was argued that these anxieties are temporal. Nevertheless, there is the need to improve upon ISPS with further legislation to ensure successful implementation of a standardized biometric identification card and the improvement of information gathering and sharing to target perpetrators with-

out disturbing the whole supply chain. Moreover, there should be ways to increase worldwide awareness, so that countries can understand benefits from ISPS compliance. (Lyndon B. Johnson.2006, 55)

Similar studies were conducted in the Caribbean region to find out whether the adoption and implementation of the International ships and Port Facility Security (ISPS) would have a measurable impact on the productivity on the port. It was discovered that there were some challenges when implementing the requirements of the Code. Apart from that, it is expensive for ports and shipping lines. Nevertheless physical improvement has been made regarding the security personnel, as result of better training, and procedures such as, access and documentation. Moreover, following the implementation of ISPS Code, the port has experiencing increased in productivity, which probably as a result of improved access control and surveillance, which directly affected the theft cases (Linda, T. B.2006, 68). According to 2010 report published by United Nations Conference on Trade and Development (UNCTAD.2010,8) regarding the Emerging challenges, and recent developments affecting transport and trade facilitation, "amendments of Safe Of Life At Sea (SOLAS) and International Ships and Port Security (ISPS) Code imposes an extensive responsibilities on governments, shipping companies, and port facilities." Implementing new security requirements effectively shall face both immediate and long-term challenges, especially from the perspective of developing countries. Though it has been accepted that the new regime will improve security in maritime transport and across the supply chain, nevertheless the cost associated with the security measures will impact the cost of doing business. The concern by developing countries is that any extra cost burden will hinder the progress of the maritime and supply chain business.

As far as the cost of implementing SOLAS and ISPS Code is concerned, the prevailing global estimated cost by UNCTAD for the implementation of ISPS Code in ports ranges between nearly $1.1 billion and $2.3 billion as a start-up cost, and between approximated amount of $0.4 billion and $0.9 billion annually thereafter. Nearly the same as increase in the international maritime freight payments of about 1 %, with regards to the initial expenditure, and 0.5 % with annual expenditure respectively. These seem very small though; these costs are too high for smaller ports in developing countries (UNCTAD.2010, 8). T he figure 1 simplified the overall assessment of the impact of ISPS Code survey, conducted by United Nations Conference on Trade and Development in 2007. Based on the respondent ports; 64 % of the respondent said ISPS Code had an overall positive impact as it provided a mechanism to standardize security at all facilities under ports' jurisdiction. 24 % of the respondent said, ISPS Code is seen as having negative implications. These include being too expensive, burdensome, including causing distraction to regular business operation. 12 % were of the view that ISPS Code has partial impact, because of the prior investments made before implementation of ISPS Code in order to prevent theft and other criminal practices.

Figure 1



(UNCTAD secretariat.2007, 26)

Considering the strengths and weaknesses of the current maritime security regime, it effectiveness can be measured base on its ability to address the maritime security risk areas of cargo, vessels, people and money. (McNaught F. & RAN. 2005, 94)

2.4 Port Security threats

The term "threat", in most cases misunderstood by many people, therefore being used interchangeably with other terms like "risk" or vulnerability. Hence, to be able to prevent or institute measures to safeguard against the threat, clearer understanding of the term "threat" is very important. The term threat could be defines as an act or actor that may bring harm or damage to a country, organization, person, or facility (Edgerton, M. 2013, 47).
Alternatively, it is an "expression, by any means of communication (Witten, verbal, body language, etc.), of the intention to inflict or cause some type of harm against a person, group, building or other entity." Obviously, from these two definitions, the central element of the threat is action or the potential for action. It may be a threat of death, physical harm, political harm or legal or an unspecified/unarticulated harmful action. Threat probably is as result of natural occurrence like earthquakes and flood, accidents or intentional act to inflict harm. Based on the context of maritime security, threat consist of possible harmful or damaging activities carried out by nation-states and their proxies and/ terrorist and criminal groups or individual not acting on behalf a nation." However, for the purpose of this study I will dwell on only "terrorism and criminal activities".

2.4.1 Terrorism

Terrorism is up to date a big threat globally. It does not matter what causes it, or how it is being carried out, it is a crime, which cannot be justified or given an excuse. Terrorism is not a threat to one particular region, country or society, rather a threat to each individual's right. Though there is no globally approved standard definition for "terrorism" it is perceived generally as deliberate assault on civilians with the aim of intimidating people or forcing a state or global establishment to take certain action or abstaining from certain action Typical examples are Boko Haram in Nigeria, and Al-Shabab in Kenya and Somalia.

2.4.2 Criminal Activities

Criminal activities includes the following actions; smuggling, theft, corruption, trade-regulation violations, and any action other illegal activity found in the maritime or port domain. Below is the list of examples: cargo theft, robbery, extortion, trafficking of people, drugs, stolen goods, weapons, or money Hijacking of vessel of vehicles, Embargo violations Customs violations

2.4.3 Cargo theft

Cargo theft is well paid and occur day in day out, throughout the world. It was reported in 2010 that, the loss as a result of cargo theft in US was nearly 171 million dollars. (Edgerton, M. 2013, 62-63). Ghana's supply chain, those that moves by the country's seaports especially is wrought with cargo theft. The local freight forwarders called it a "silent" crime. Cargo theft costs the Ghanaian economy several million cedi's annually. (GIFF Secretariat) Despites the fact that there no reliable crime statistics on cargo theft locally, approximately, it was indicated that West Africa countries have the uppermost risk of cargo theft on the entire continent of Africa (Burges, Global risk, 2009 .47). Globally, the theft of goods in transit expected to reach 50 billing dollars a year or more. According to law enforcement agencies, half of the cargo theft cases have not been reported, and if reported it the figure may even exceed 100 billion dollars annually. Sometimes robbery forms part of the tactics used in cargo theft. Particularly, cargo hijackings

2.4.4 Extortion

Extortion involves illegal activities through criminal organizations in the ports and their environment, whereby usually citizens who obey the laws are coercing to offer material, services, or money to organized criminal groups.

2.4.5 Trafficking

Trafficking is one out of everyday crimes found in seaports and maritime domain. It includes trafficking or smuggling of persons, money, drugs, weapons, or other contraband goods. Some smugglers use the proceeds from the trafficking or smuggling to support terrorism. “For example in December 2011, a Lebanese man named Ayman “Junior” Joumaa was indicted in United States of America for smuggling cocaine and laundering money as part of an intricate plot that involved both raising money for Hezbollah and laundering money for Mexican “Zeta” drug cartel.” Vessels hijacking are usually connected to piracy and is a criminal activity. Currently, Somali pirates hijacked commercial ships and as well as cargo ships and tankers, they released the vessels after millions of dollars have been paid.

2.4.6 Corruption

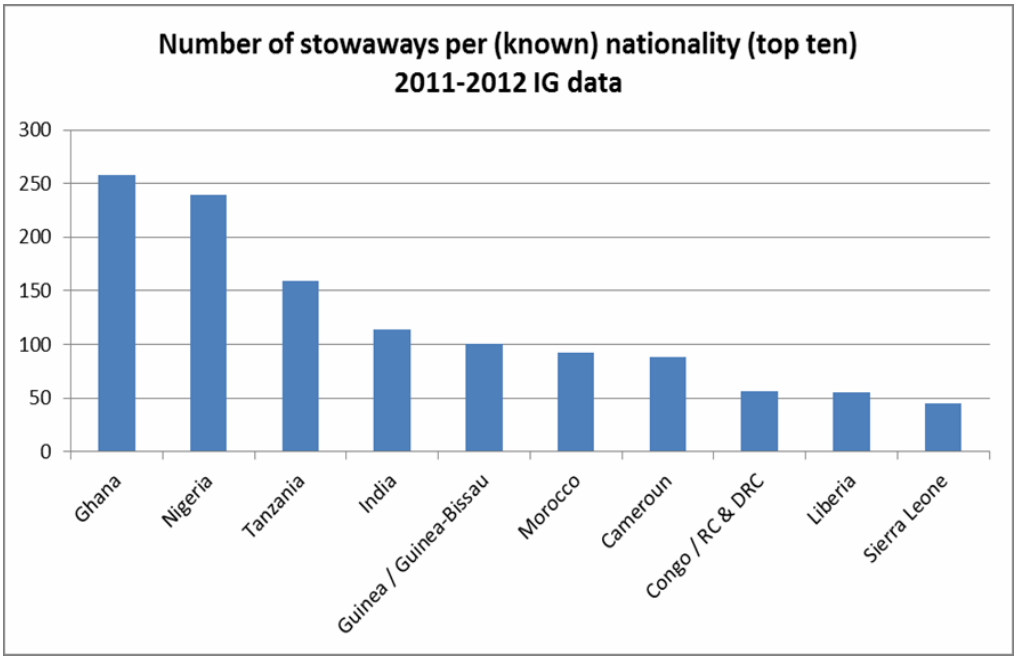
According to Schreier, F. 201. (Geneva Centre for the Democratic Control of Armed Forces), “Corruption may be defined as soliciting or accepting, promising, offering or granting an undue advantage for the commission or non-commission of an action.” To be able to growing a successful sustainable business requires the following: an uncompromising devotion to developing products and services that contribute real value to the client; passionate leadership that attracts and inspires the best to join the venture; and an unwavering commitment to act as a responsible player in the community, nurturing public trust and support on which all businesses eventually depend. Corruption erodes each of these pillars of business success. It means three things: cutting corners and shirking honest competition rather than producing real value for the clients; compromising corporate and individual integrity, deterring and demotivating the best and most innovative entrepreneurs and scientists from signing on; and consenting to, and propping up, a business environment in which complicity is for sale, entrusted public power is routinely abused for the sake of private gain, and public trust in the beneficial partnership between business and society is slowly uncompleted. The action of corruption can be active or passive. Promising or offering an individual undue advantage is what is refers to as active corruption, whereas passive corruption can be soliciting or accepting this kind of benefit. The following can be described as some of the corrupt act; bribery, graft, sweetheart deals, political payoffs, influences peddling, cronyism, patronage, nepotism and so on. Lobbyism emerges as modern form corruption, which has more than about 20,000 Lobbyist in Washington D.C. and 15,000 in Brussels and many more in the world. (Schreier, F. (DCAF), 2010, 57) Mostly, the economic, social and administrative factors initiate and open way for corruption. For instance Low salary workers may be influence to earn supplementary income from corrupt means. Hiring, job advancement or promotion, which is based on more connections and payoffs instead of merit, also contribute to corruption. Such actions decreases professionalism and competence of the bureaucracy, thus solidifies the cycle of corruption.

Corruption promotes smuggling, misappropriation of public funds, tax and customs revenue, extortion and fraudulent award of public procurement contract.

2.4.7 Stowaway

A stowaway is an individual who hide on a ship, or in cargo, or in a container which is then loaded on onto the ship without the ship-owner or master's permission, remains on-board the ship when she leave the port. Stowaway is perceived to be long-standing threat for shipping companies specifically those that have been doing business on the coast of West Africa, in Central America, Colombia, Venezuela as well as Dominican Republic. Apart from the Vessel's patterns of trade, this threat is also connected to the vessel and /or cargo type including security training and awareness of the crew. The majority of stowaway is normally found on container, bulk and general cargo vessels. The International Group of P&I club gathered stowaway case from 20th February 2011 to 20 February 2012 totals of 774 incidents including 1,640 stowaways. Meanwhile, there has been minor decrease in the number of incidents, by comparing the time period from 20th February 2007 to 20 February 2008 that recorded 842 incidents including 1,955 stowaways. From the data, though there has been decreased, but it's not substantial amount. On the bases of nationality of stowaways, the IG data shows that, the margin of the stowaway were from Africans, particularly Ghana, Nigeria and Tanzania as indicated in table 1 below. As indicated through table 1, Ghana leads in term of highest number of stowaway per country, while Sierra Leone is the least on the top ten of the table.

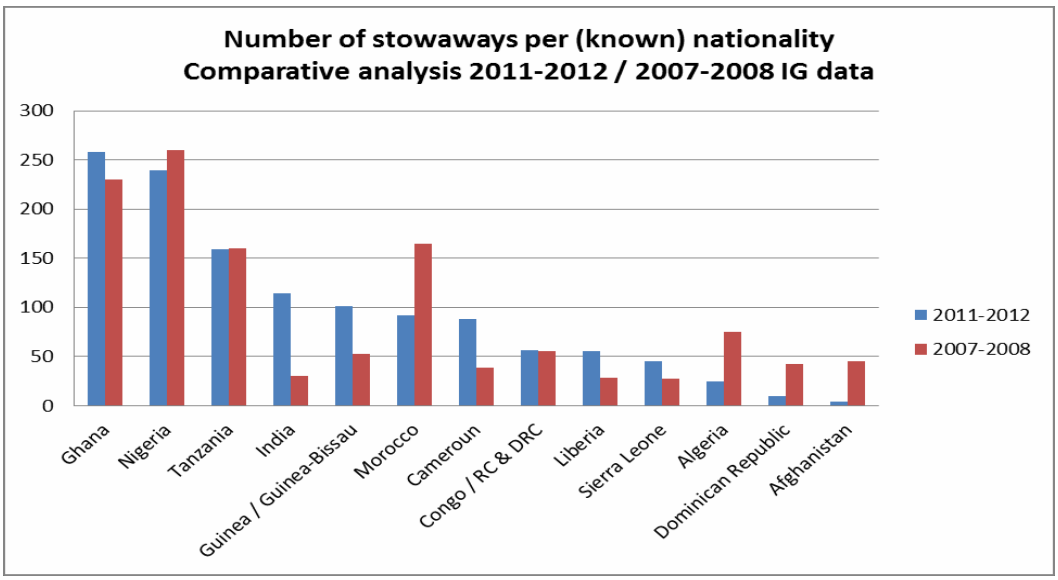
Table 1



Source: I:\FAL\38\6-2.doc, 3

By comparing 2011-2012 and that of 2007-2008, table 2 shows very slid shift in nationalities of stowaways

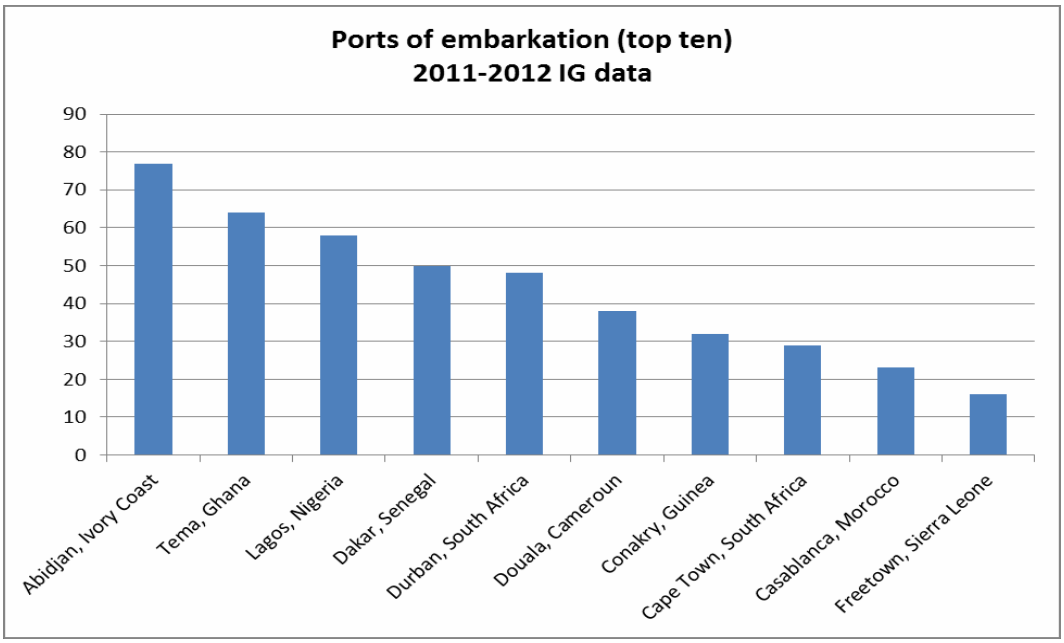
Table 2



Source: I:\FAL\38\6-2.doc, 4

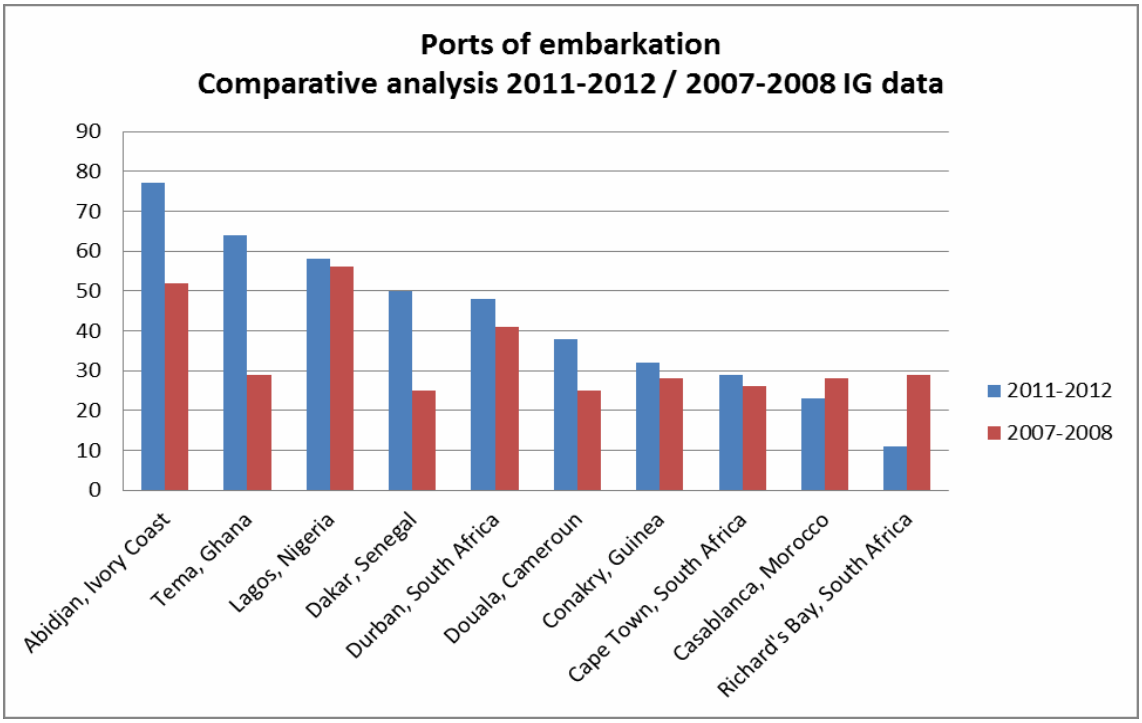
Regarding the port of embarkation, the International Group of P&I Club data, for 2011-2012 shows that the top ten port of embarkation based on number of reported cases are in Africa, mostly West part of the continent been painted on table 3 and 4 below

Table 3



Source: I:\FAL\38\6-2.doc, 5

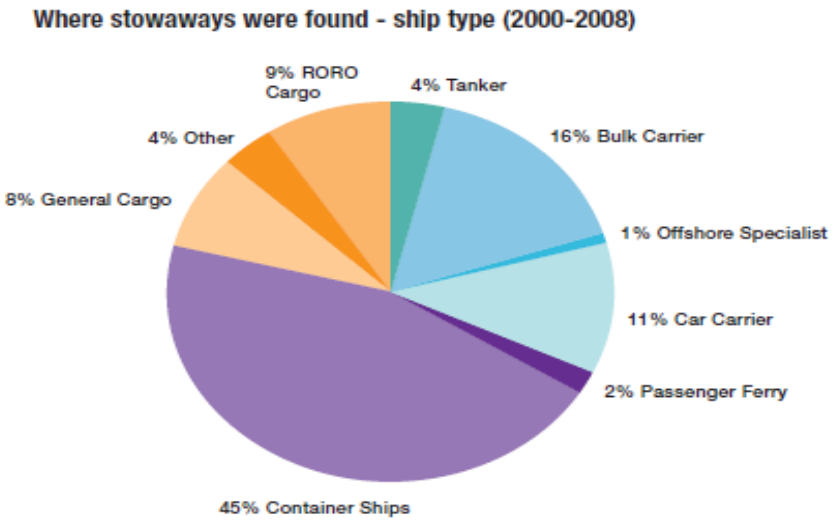
Figure 1. Table 4



Source: I:\FAL\38\6-2.doc, 6

Based on table 4, the data from 2011-2012, if compare to the 2007-2008 data, there isn't any substantial amount of differences in terms of the stowaways' nationalities, port of embarkation and number of stowaways.

Figure 2



Stowaways are normally found in a specific type of ships, and as indicated in figure 1 above, container ship carries the highest percentage of stowaway due to it multipurpose type of ship and consistency in trade. Bulk carriers, car carriers, and general cargo and Ro-Ro ships also carries considerable number percentage. (SPENCER, C .209,2)

2.4.8 Human factor as a threat

Considering the threats and vulnerabilities regarding port security, human factor cannot be overlooked, when implementing security measures or safeguards. This is because human factor can serve as an obstacle to the successful implementation of the security measures. Preventing internal threat to security is one of the most challenging and complex task facing security and law enforcement at the port, because of employees' unique access to vessels and the infrastructure with the port. Example restricted access area of the port. This places a difficult challenge on the security manager to prevent unauthorized access to the port (Christopher, K .2014, 64) Modern day security has been considered to be more or less technical field, yet it is important to know how human affect security measures or safeguards. Human problem are the vital part of security. Most often than not, security is regarded as technology, nevertheless, it is always concerns human beings. Security exists because of human being and for that matter; people are the center of any security defiance or breach. Even though, technology helps both the attacker and the defender in deferent ways, nevertheless security is basically about people. The port users and other individuals may follow the best and re-

quired security practice recommended by the ISPS Code and the security experts, install the needed security products, with complete vigilant regarding the security systems, still individuals are still vulnerable. Why? According to Kevin D. Mitnick William L. Simon (2002) "the human factor is truly security weakest link. One of the worlds most renowned scientist of the twentieth century, Albert Einstein, said, "Only two things are infinite, the universe and human stupidity, and I am not sure about the former." Criminals can infiltrate the security system and succeed when people are corrupt or ignorant regarding good security practice. "Anyone who thinks that a security product alone offers true security is settling for the illusion of security". Such people should anticipate for future security incident. According to Security consultant Bruce Schneier (2008), "Security is not a product, it's a process." "Further security is not a technology problem it's a people and management problem." According to Bruce Schneier, (2008) "Security is both a feeling and a reality. And they're not the same." Personality and Behavior are the most persistent hindrances to teamwork in organization interpersonal conflict. Most conflicts are established in various personality traits.
Kabay, M. E (2002) presented the following example as a set of categories for describing people's personalities:

a. Extroversion
    - High: active, assertive, energetic, outgoing, and talkative
    - Low: quiet, reserved, shy, silent, and withdrawn

b. Agreeableness
    - High: affectionate, appreciative, kind, soft-hearted, sympathetic
    - Low: cold, fault-finding, hard-hearted, quarrelsome, and unfriendly

c. Conscientiousness
    - High: efficient, organized, responsible, and thorough
    - Low: careless, disorderly, frivolous, irresponsible, and slipshod

d. Emotional stability
    - High: calm, contented, stable, and unemotional
    - Low: anxious, moody, nervous, tense, and worrying

e. Openness
- High: imaginative, insightful, intelligent, original, wide interests
- Low: commonplace, shallow, simple, narrow interests, unintelligent

Some Peoples assume some kind of personality trait as superior and this affect communication among colleagues. For example, people with "low" characteristics might perceive the above, might be a hindrance to team work in an organization, which will definitely impact the organization security system negatively.

Personality traits often cause conflict more than problems of understanding. If the team recommends that all the staff or employees must challenge or defy individual who is found inside the port premises or within port facility without badge or protective cloth, person with low extroversion as stated below, for instance may find it difficult regarding the notion that they should inform individual what to do, particularly if the person is his Boss or of superior ran.

f. Extroversion
    - High: nervous, aggressive, excitable, pushy, chattering
    - Low: dignified, respectful, unassuming, attentive, self-sufficient

g. Agreeableness
   - High: clinging, gushy, soft-headed, knee-jerk reactive, uncritical
   - Low: stately, analytical, rational, principled, reserved

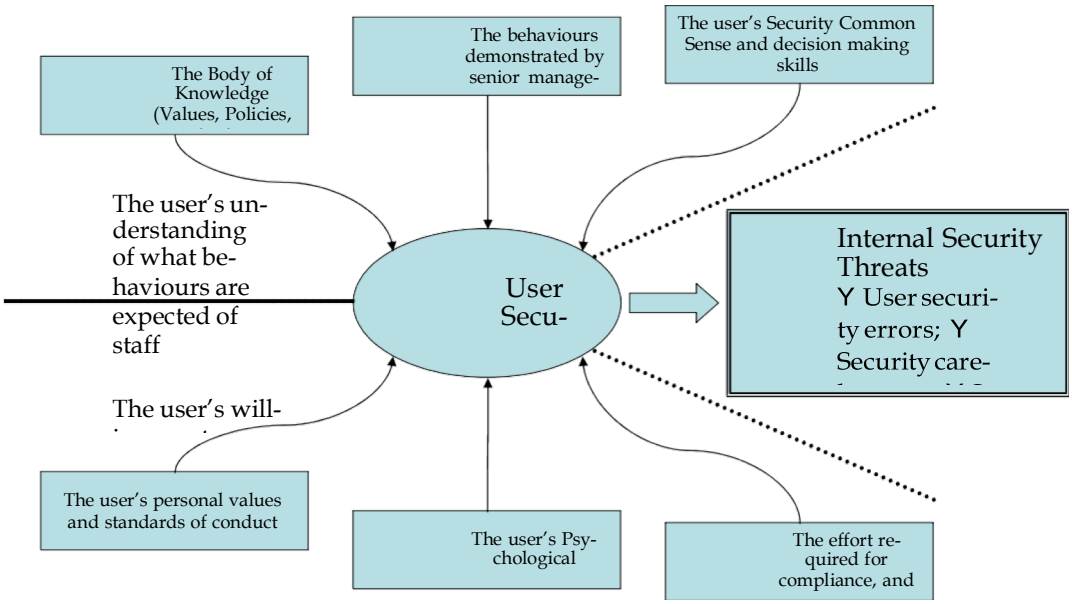
h. Conscientiousness
- High: obsessive, compulsive, unspontaneous, pompous, slavish
- Low: free, spontaneous, creative, fun, youthful, having perspective

i. Emotional stability
   - High: frozen, ambitionless, boring, dead
   - Low: vibrant, romantic, alive, strong, sensible

j. Openness or Culturedness
- High: flaky, theoretical, complicated, off-the-wall, dilettante
- Low: earthy, smart, grounded, focused, practical

John Leach (2003) observes two sets of factors, which changes the employee behavior. The first set comprises user knowledge regarding what the company hopes from the employee and second sets includes factors that empower the willingness of the employee to conduct him or herself within acceptable and approved standards and practices of the company. Figure 3 illustrates the two sets of influential factors. Leach specifies that human knowledge is based on what they are told, what they see practice around them and their past experience.

Figure 3, Factors That Influences Security Behaviour



With regards to what Employee have are told, several companies have documented security policies, practices, standards and procedures. The effectiveness to influence the security behavior depends on the body of Knowledge accessibility, the completeness of its coverage, clarity of the stated security values and its uniformity.

Again with respect to what employees see practice around them, the existing employee or new employee who want to comport him or herself in conformity with company norms and practices, are commonly motivated by what they see being practice by their peers or superior. Mostly, employees are seriously influenced especially, based on their superiors' attitude and behavior towards the security norms and practices of their work environment.

When it comes to employees past experience, sometime not all the security policies and procedure are expressly documented, some are implied, even some may not made know until certain circumstance, and so, employees at that situation may take their own security decision as part of their daily task based on their previous knowledge and experience before even they are expressly stated or build up.

According to Leach (2003) willingness is based on personal values and standards, sense of obligation and degree of difficulty. Even though, employee can to take up and apply the organization's system of values and standards, with comfort, it possible they may be demotivated or tensions, and this possibly arise when there is conflict of interest between the individual's values and standards with that of organization's own believes and standards. If that happened, individuals turn to follow their own values and standards.

Apart from personal values and standards, every employee has a sense of obligation (psychological contract) with the company or the employer he or she works for, which forces him/her to act in accordance with company expectations, voluntarily to restrain their behavior to be within the bounds of accepted practice, particularly if individual feels well treated, recognized and rewarded by the employer. Nevertheless, if employee feel he or she have been treated unjustly by their employer in any aspect of his/her employment relationship, he or she will feel that the bonds have been breached or loosened and when that happens the employee can lose the willingness to act in the company's best interests or employee will feels the employer have been unfair to him/her and that will cause the employee to feel angry so that he or she will wish to punish the company. When that happens, then the employee becomes the company's security enemy and that will stands as a major security threats. Hence the sense of obligation towards employer impact behavior.

Last but not the least, levels of difficulties employees encounter in complying with the company's policies and procedures also impact behavior. If the security countermeasures are difficult to perform or are operationally burdensome, the controls appear to be ineffective and

inefficient; the employee may have little tolerance to comply even if the employee recognizes that the security countermeasures are implemented for good reasons.

2.4.9 Economic Espionage

When there is a competition among the private sector companies, some may try to steal trade secret or confidential information, including compromise business practices to get economic advantage. Seaport is not out of target location for espionage activities due to the confluence of private sector trade, transportation, and import /export interest. (Christopher, K .2014, 69)

2.4.10 Poorly train security personnel

If the staff responsible port security lack adequate training there is higher possibility that for crime and infiltration by internal conspiracies. (Christopher, K .2014, 68)

2.5 Ports, Ships and Supply Chain Vulnerabilities

Despite the effort by the International Maritime Organization (IMO) to prevent crime and terrorism against maritime commerce by introducing ISPS Code and other programs, criminal activities still occur day in day out through various seaports. With all the measure and programs in place, criminals still find their way out with their nefarious activities, due to the vulnerabilities that present themselves within the supply chain and the seaport. Ports are really complex and particularly vulnerable, and very important to global trade. From a security perspective, ports always need to be assessed from the following dimensions: target, conduit, and border. Moreover, ports are critical node within the global maritime transportation system because they are fixed, permanent locations, which make it more vulnerable and less easily replaced than other elements. Port is a target, because it serves as a link between land transportation and maritime trade routes, and has since been identified as strategically important target. It forms a single point of failure for Sea Lines of Communication (SLOC), and due to its unique characteristics or geographic locations, it difficult or impossible to replace. Moreover, it serves to convey cargo or goods into foreseeable and known storage area. For Example, containers yard or shed. Thus permit potential attackers or criminals to readily locate potential cargo for theft or damage. It serves as a conduit, because it purposes is to help bring a full range of goods and services to people globally. As distribution and receiving of goods and services taking place, it creates vulnerability to be exploited by criminal groups, terrorists, or state actors for importation and exportation of illicit material into the country. Nearly 90 per cent of global trade passes through sea, everything from raw materials to automobiles, clothing as well as high-end electronics. This high volume of cargo that passes through the port bring many challenges to government and other bodies that have been

tasked to ensure safe and secure transportation of cargoes, globally. What makes it more challenging is, increase in just-in-time delivery, whereby a movement of huge amount of cargo as quickly as possible passes through the port to their intended destination of delivery. This creates significant vulnerabilities in the security of the cargo and the port by which that cargo transit. The vulnerabilities that the ports as channel face are, cargo theft and smuggling of banned goods or people out of the port. (Edgerton, M. 2013, 34-43)

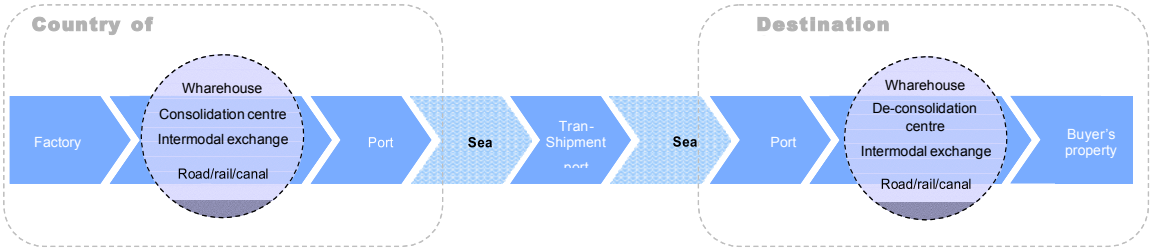
2.5.1 The Three Critical Flow Of International Trade Cargo

This part observes the main flows connected to the process or the movement of maritime cargo in broader broader scale, especially the containerized cargo. In this modern day, most of the global trade passes through sea, from raw materials to automobiles, clothing as well as high-end electronics. The maritime journey is just a single element in a complex chain. Regarding a typical door-to-door journey whereby goods are shipped using container, involve different actors, documents, who interact with each other through divers means, and be handled at several physical locations. The system of people, their interaction, movements, and information connected to the transnational movement of goods can be categorized into the following: Movement of goods from place to place, Movement of custody from person to person, Movement of information regarding the cargo

2.5.1.1 Place and Process

In the first place the chain comprises the physical process of moving cargo from one place to another, and from one process to another process. Security view this chain is very physical, and so, immediately there is feeling of suspicions or established fact, threats can be pinpointed down this chain, and necessary steps can be taken to physically counteract the threat. Once you know where the shipment started, it mode of transportation and the particular places it passed, whether the integrity of the chain have been compromised or not. The security staffs or security agencies that want to stop threatening cargo must begin to probe or ask questions. Issues relating container cargo security can be simplified under the following stages: Loading stage at the warehouse, land transportation, port of origin, sea transportation and port of destination. At every stage within this chain, there are actions or activities by different agents, offloading, restaging, reloading, and transshipment. The chain described above is not consistently secure and the level of protection offered regarding the containers and their contents could be altered while moving from one node to another, and between the modes. If the security at one contact is breached, it compromises the security of the entire chain. Cargo theft remains a problem, even at a situation where there is existence of high-level security. The areas that are more vulnerable within the physical process of cargo movement have been circled, as shown in figure 3 below.

Figure 4



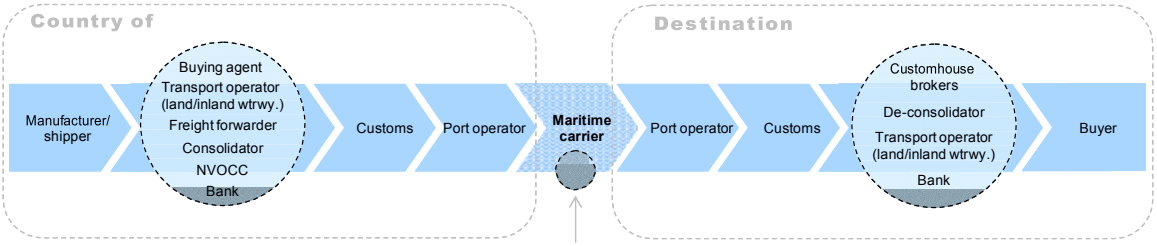
The International Container Logistics Chain Vulnerability Assessment: Places in the logistics chain

Source: (OCDE.Paris: July 2003,24)

2.5.1.2 Actors in the logistics chain

There are several representatives involves in each trade transaction, including individuals who involves during loading and transporting of the containers alongside the logistics chain shown above. Knowledge regarding exact content, identifying each item, and checking the background of individual who comes into contact with the container at the warehouse or distribution center from which the cargo is transported, becomes a main challenge to government agencies and port security guards globally. There are many buyers or manufactures globally, and out of these manufactures or buyers, some may ship full container load straight away, while others may produce less than container shipments, which must be joint together before being transported by sea. From the initial stage of logistics chain before the shipment is done, several intermediaries mainly buying agent and/ or freight forwarders between originating shippers and ocean carriers, who performs various task, ranging from assembling and consolidation of less than container load shipment into full containers. Again, when in cargo is in transit or in port areas, several workers at the warehousing/staging yard/ within the port may have physical access to shipping containers. Among this group of workers, one may have criminal or wicked intention to exploit the loopholes within the logistic chain. To succeed in this, criminal or terrorist may exploit the loopholes in physical, either through the people or procedural security of these facilities. As show by figure 4 below, loopholes or vulnerability could be found in area been circled.

Figure 5



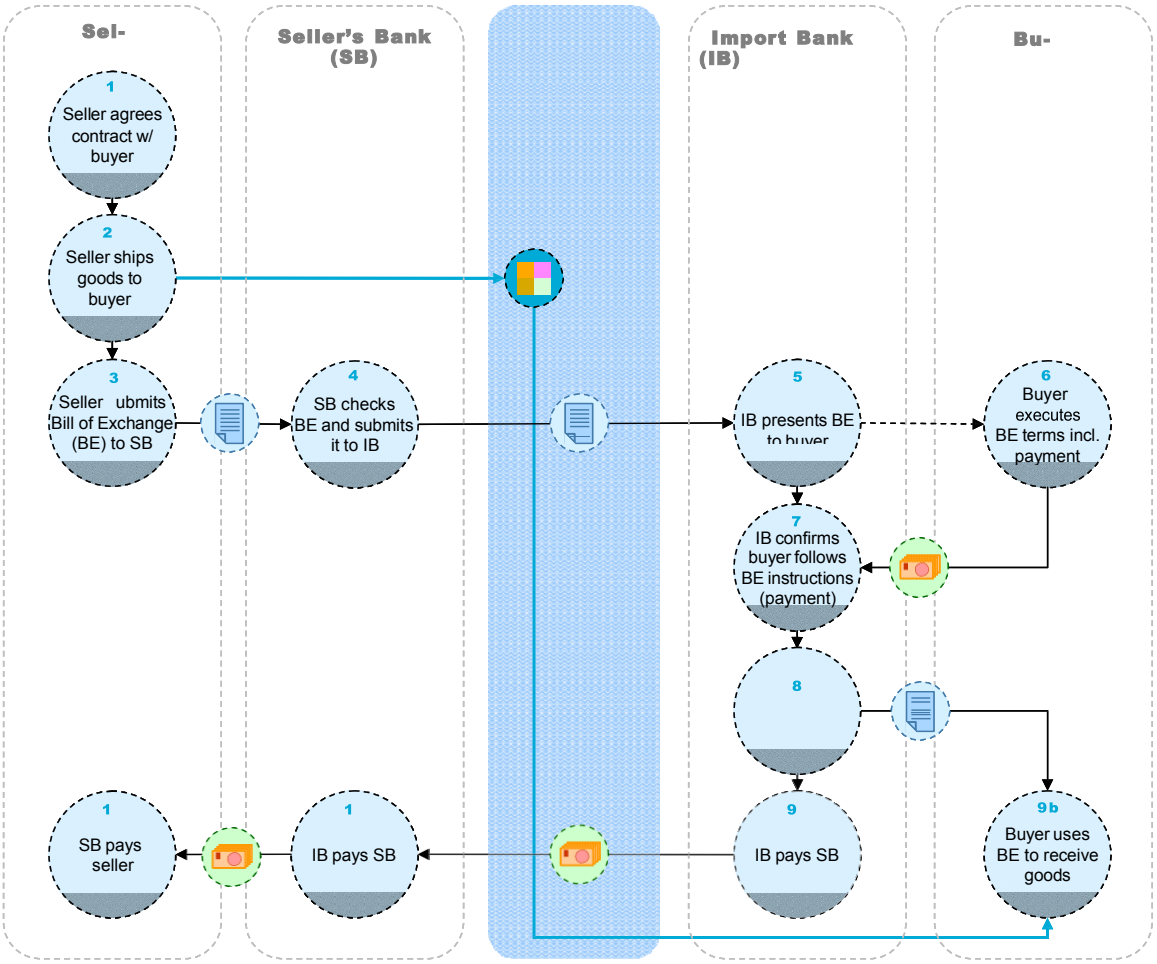
The International Container Logistics Chain Vulnerability Assessment: People/ Actors involved

Source: (OCDE. Paris: July 2003,25)

2.5.1.3 The flow of information/money: bill of exchange

There are many actors in the global trade and some of them have never met physically but they are able to transact business based on the exchange of information. Without the secure communication of pieces of information, the global trade cannot be possible, due to fact that some of them never meet. The content of the information may include the specification of the goods to be transported, quantity, number of items on each pallet and into each container, particulars regarding the custodian one who is liable for the goods, information about the delivery date and responsibility for payment, information about the agent of the shipper and the receiver and so on. From the above information, every transaction include will be more than 10 separate document because some of them may be duplicated. For instance forwarder may issue a bill of lading duplicated by the vessel or the carrier. Without the bill of lading, the customs and security agencies cannot take a decision on which container to inspect and the result from any little manipulation will be very serious. The risk is real, as anyone can agree to the fact that, incident of document fraud could be used for cargo theft. Moreover most of the information flow in the international trade is still on paper-based, which is costly but inefficient. This flow of information /money: bill of exchange is been illustrated through figure (OECD.2003.23-27)

Figure 6. Flow of information /money: bill of exchange



2.6 Supply chain security and its impact on ports operations

It is very important to understand supply chain when dealing with supply chain security. According to Arthur G, Arway (2013, 3), "Supply Chain is a chain of interconnected links that facilitates the movement of supplies or in other words cargo, goods, materials, products etc According to British Standards Institution (BSI) Group, it combines the traditional supply chain management practices with security measures to safeguard business against cargo theft, terrorism and piracy.

Though it is the responsibility of every person that gets in contact with the cargo to ensure it safety and reduce the risk of the theft, the actual responsibility is upon the shipper. Supply chain security policies and procedures, contractual agreement, visibility of every cargo movement and the ability to audit compliance with supplier are the very significant to secured supply chain. Nevertheless these steps are often seen as too costly and overburden on the shipper. Since the supply chain activities have change from traditional way as result of technology, criminals also have changed their activities and their ways of doing things. (Burges, D. 2013, 12-15). According to Thomas Friedman (2007,8), "the interconnected global economy enabled by advances in Information and Communications Technology and other factors that he terms "Flatteners", does not only empowers the software writers and the computer geeks to collaborate on the work in the flat world, but also AL Qaeda and other terrorist networks. Whiles international commerce expands, it also opens opportunities for criminals to infiltrate the supply chain." After the attack on USA, supply chain was seen as important gap in country's security, as there were panic that criminals could exploit supply chain beyond the normal smuggling of product, people, and narcotics. Criminals can smuggle weapon of mass distraction and other dangerous chemicals through supply chain. The threat of terrorism and other criminal activities serve as a security challenges to supply chain, and has a significant consequences on firms and other supplies, customers, carriers, terminal operators, governments and international partners as well. Certainly, the worldwide economy depends on how secure and resilient the supply chains are, and the ability of the supply chain to withstand and recover from incident, depends on the resiliency of the supply chain. The security of the supply chain is paramount as far as the global economy is concerned. According to Andrew R. Thomas (2010,166) "A resilient supply chain is one that can reduce cost and improve customer satisfaction and customer relations under normal supply chain operations, while sustaining supply chain operations during major disruptions."

In dealing with these challenges, several programs have been introduced with the partnership of businesses, and governments to secure the supply chain. For instance; Customs-Trade Partnership Against Terrorism (C-TPAT), World Customs Organization (WCO), and The European Union's Authorized Economic Operators (EU AEO) (Andrew, R. Thomas.2010, 170)

Customs-Trade Partnership Against Terrorism (C-TPAT), and Container Security Initiative (CSI) are voluntary initiative by US to tackles diverse aspect of the supply chain security. These security Programs focus on distinct aspect of the chain of transportation. The purpose of the initiative is to build cooperative relationship, which will boost international supply chain and US border security.

WCO – World Custom Organization - is an international organization responsible for customs issues. It consists of national Customs administration worldwide.

World Custom Organization (WCO) in 2005 adopted SAFE Framework to protect the supply chain trade from threat of terrorism. The world Customs Organization (WCO) SAFE framework is a to ensure member countries commitment to employ trade security programs like C-TPAT which provide benefits to business that apply SAFE-defined standards and best practice

The European Union's Authorized Economic Operators (EU AEO) program is similar to Custom Trade Partnership Against Terrorism (C-TPAT) program. The intention of AEO program is to upgrade supply chain security, and at the same time contributing toward facilitating of trade reforming and modernizing customs globally.

To establish a framework for supply chain security, the International Standard Organizations (ISO) has instituted its ISO 28000:2007 standards, which define procedures, policies and mechanism for corporations or organizations to identify the critical parts to the security of the their supply chain, and also for managing vulnerabilities as well as establishing preventive actions plan. With ISO 28000:2007 supply chain security management standard procedures; goods can be protected from the factory to the point of sales. (Andrew R. Thomas .2010, 169)

Why supply chain security is needed in port security operation is obvious from different view-points. If port security officers and mangers integrate supply chain security into port security systems based on ISO standards, it will offer the following benefit:
First, it will prevent illegal commodity to be intermingled with the shipment, or prevent shipment to be used as a weapon or any explosive substance into the port.

Again, trade involving transportation of good across the borders will be facilitated and expe-dited, which will also enable the management of the port and the security officers easily monitor and manage the security risk throughout the business and the supply chain.

Moreover, the port can achieve a completive advantage as well as gaining new business, thus encourage the stakeholders of the port, their commitment to safety of individuals and securi-ty of goods and services.

Notwithstanding the above benefit, port can gain cost of saving via a decline in security inci-dent and likely minimization of corporate insurance premiums.

2.7 Security and it potential impact on the competitiveness of the port

According to Michael Edgerton (2013, 141) "maritime security cannot be considered in isola-tion. It affects and is impacted by numerous external factors, including socioeconomic driv-ers, political priorities, transportation-system linkages, business trends, and international

events." Looking at the complexity of the interactions between the ports, ships, including maritime field with other economic interests, logistics, and the mode of transportation, security must be perceived as a component of risk management and system resilience. (Michael Edgerton.2013, 141). Security regarding port operation must not be seen by it self as a primary objective, but should be seen as safeguarding safety and efficient port operations and trade. Historically, organizations could construct a secure perimeter around their crucial and sensitive business environment and safeguard it again attack from various viewpoint. With the wall and barbwire, anti-virus install on your information technology systems, including other physical security, you are well safe. Nevertheless that is not case in the modern-day, or environment we live in today. Advancement of technology, which has made it possible for remotely access company information, tracking of cargos using technology and so on, means the organizations are no longer, and cannot be secured with traditional way of ensuring security. Many at times security is perceived as cost centre in the business or commercial environment, and sometimes considered as business inhibitor. Nonetheless, if security is incorporated into daily port operations, it will bring efficiency, and guaranteed resilient security system, which

2.8 Benefits of making security an enabler

Incorporating security into daily port operation, where security is perceived as an enabler instead of objective, will bring efficiency and effectiveness in safeguarding the companies' assets. Alternatively it will enable the security officers carry out the responsibilities successfully. Ultimately the mission and purpose security will clearly be understood by the entire organization, and eventually will not be seen as cost centre for business, rather as added value. For instance, it will prove the value of security department by ensuring that buyers and sellers are able to safeguard their shipment via the supply-chain security initiatives.

This could be achieved by vising the site of the suppliers and assesse the mode of operation, then develop measures that will positively impact on the efficiency and minimizing organizational delay such as truck and container movement, ship arrivals as well as minimizing cargo theft that could be as a result of security measures. Apart from that, the meaning of security could be presented as valuable element of safeguarding the sustainability the organization by protection of property, goods and the life of people, including protection of supply-chain integrity and intellectual property. Also the stereotype mind set people that security is a burden in the organization, heavy-handed, obstacle to free flow of information, goods, and individuals as well hindrance to business operation, which eventually create bad image for the professionals in the security field, will then be changed to positive. (Michael Edgerton.2013, 142-44)

3 Research Methodology

This chapter shall describe research methodology applied in this thesis and the research question that this study aims to address. Further explain the study approach, Process of the research, data collection methods, and data analysis methods. Data collection methods include both primary and secondary methods.

3.1 Research strategy

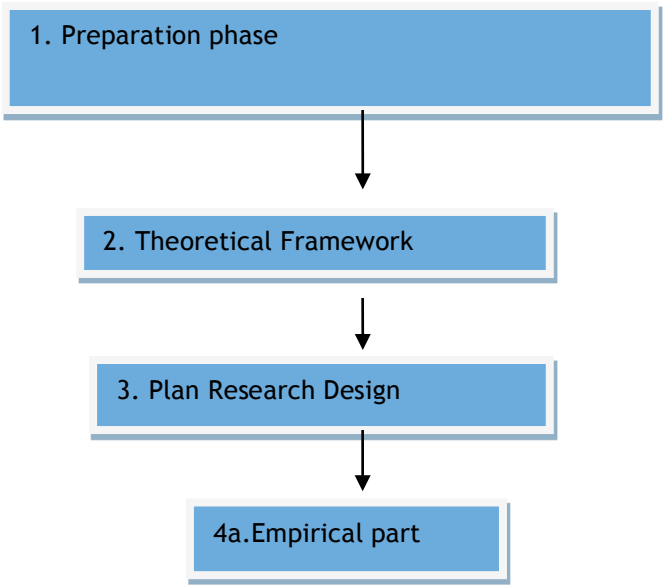
This research shall apply case study and qualitative approach as a strategy to identify the threats and vulnerabilities. Case study was chosen because it provides and in-depth understunding of phenomena , their constructive process and the actors involved . It is said to be appropriate for describing , explaining , predicting or controlling process associated with a variety of phenomena at the individual , group, and organizational levels.(Yves-C,Gagnon.2010,2).

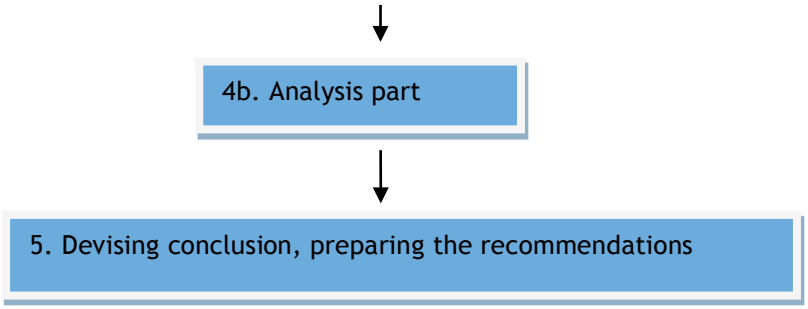
Qulitative method is applied to understand and interpret social action. Usually, the objective of qualitative metheod is to explore, discover and construct. This method involves analysis of data from interviews, images, pictures or object. This type of method is subjective, and uses observation, interview and open-eded answers to collect data (Johnson, B. & Christensen, L.2008). I used qualitative approach because it will enable me get deeper understanding of people the operation, and the activities.

3.2 Reseach Process

Below diagram consists following steps, which shows the whole process of the research;

Figure 7. Research process





In the planning stage, initial examination of various literature sources shall be carried out to ascertain the potential problem areas. Define the research problem, objectives, research question and delimitation. Phase two is where the review of the literature shall be done to ascertain the clearer picture of the potential threats and the vulnerabilities. The outcome of the phase two would be used to plan the review, and then research design shall be plan in the phase three. This is where the methodology to be applied for the study would be defined. Subsequently, analysis of various methodologies, case study research strategy is chosen. The fourth stage is practical settings where more detailed process of the empirical part would be outlined. Data collected would be examined and compare it to the theoretical part to ascertain the possible threats and vulnerabilities. The last but not the least stage is to develop conclusions and recommendations

3.3 Process of Data collection

This part provides the details of the process of data gathering for this research project. Diverse methods were been used during investigation for gathering both primary and secondary data as presented below.

3.3.1 Primary Research

3.3.1.1 Questionnnaire

I used closed-ended questionnaire to respect the confidentiality of the organizations' information. The questionnaires were given to responders with no possible way of identification, and with no sex or age distinction. The questionnaire targeted only Takoradi port, and focus was on: ISPS code Documentation, Security Level Coordination and Implementation, Port Facility Security Officer knowledge and training, Port Facility Personnel with security duties, Port Facility Personnel without security duties, Security incident reporting procedures, Drill and Exercise requirement, Security Measures for Access Control-Perimeter, Security Measures for Access Control –Personnel, Vessels and Port Facility, Security Measures for handling cargo,

Security Measures for monitoring ,Safety Measures for handling or storing dangerous substances, and the last but not the least , Communications.

3.3.1.2 Interview

The expert interviews were conducted on the January 2015, and 4 experts from 2 organizations partake in the interview. These experts represent Takoradi Port in Ghana and Port of Helsinki in Finland. The case company is Takoradi Port, but I used Port of Helsinki for Benchmarking purpose. Categories of the threats served as a model for the interview as well as a basis for the interview. I used interview when participants cannot be directly observed. The interview form was divided into six (6) main categories: security incidents regarding non sea borne vulnerabilities to information systems and the technologies, smuggling, stowaway, theft, terrorism, and piracy. The aim of the interview was to identify the threat type and the likely place for the threat to happen, and to employ appropriate measures to ensure security at the Port of Takoradi. Further, the interview aimed to identify vulnerabilities within the existing security system at Takoradi Port.

3.3.1.3 Observation

Applying qualitative approach in a research, there are various ways primary data can be achieved. The primary data could be obtained via interviews, conversations, photographs, recordings, memos and so on. (Denzin and Lincoln.2003, 4). Using observation as a methodology offers more understanding as it can use in 'natural' settings, than interviews. Primary data for this project was gathered mostly by questionnaire with the main respondents from the security department with the Takoradi Port. However, observation also played a role in data gathering. "If your research question(s) and objectives are concerned with what people do, an obvious way in which to discover this is to watch them do it. This is essentially what observation involves: the systematic observation, recording, description, analysis and interpretation of people's behaviour". (Saunders, Lewis, and Thornhill.2009, 288). To better understand what people do (their roles, actions, and behaviour) and how these can change in reaction to situations and over time, observational method are suitable. I used observation to explore the vulnerabilities and threat regarding the daily port operations that security officers found it difficult to articulate. For instances I found that, when interviewed, the security officers feel reluctant to divulge certain information for security reasons.

Again, the skills and actions of the security officers or workers without security duties that had not been described, and had not have been shown in the interview base-studies were revealed, through observation. For example, how security officers and other workers handles customers and their attitude towards corruption. Though interview can be applied to discover

the interpretation of 'actors' in the field, observation can be critical to exposing people's behaviour and discloses information not found through alternative methods.
Nevertheless, observation is not only a techniques for difficult circumstances, yet it helpful in uncovering the taken-for-granted work of security professionals and other operational staffs.

3.3.1.4 Informal Discussions

To get additional information, informal discussions were assumed with other stakeholders within Takoradi Port and some of the port workers, both casual and permanent. The selection of these people was on casual bases, because I already knew some of them. Most of the discussions took place whiles I was on field assignment during my internship period, and the issues was some time about how certain operations were been carried out. The discussion also some time concerns the issues regarding my research. This discussion assisted in verifying the feedback received from the distributed questionnaires. Nevertheless, under no circumstances was the data/information gathered from the chosen people or informants were intentionally or unintentionally shared with anyone during the discussion.

3.3.2 Secondary Data Research

3.3.2.1 Data Collection

Secondary data consist of both raw data and publish summaries that have been collected by organizations and individual, excluding researchers. They are considered as essential element in addition to primary data in most social science research. (Saunders, Lewis, and Thornhill.2009, 256). When using case study approach, combining primary data and secondary data facilitate in authenticate the results. According to John J. Green (2012) at the state data centre of Mississippi, during annual affiliate meeting, stated that mixing both types of data offer a practical strategy for conducting efficient and useful assessments and evaluation. Taking into account significance of integrating both data, necessary attention is given to secondary data. There is multiple numbers of secondary data. (Saunders, Lewis and Thornhill.2009, 258–259). In support of this study, port security regime, Port security rules and regulation (ISPS Code), published material from recognized agencies, form the bases for the information analysis. Trusted web-based information is additional sources of secondary data. The fact that nearly all organisation and agencies usually publish their information via websites, it was confirmed by Saunders, Lewis and Thornhill (2009, 263–267) that this form of media offer a good quality secondary data through several organisations worldwide, whose information's are frequently updated. Based on this, different sources of information have been sourced from associated websites, for example; IMO, International Group of P&I club,

Ghana Institutes of Freight Forwarders, Bureau of International Narcotics and Law Enforcement Affairs, UNCTAD, etc.

3.3.2.2 Data Analysis

Just after the feedbacks from the questionnaire were received, they were compiled, and compared to each other. They were therefore compared to the literature review and most relevant ones presented in the results section. The analysis were not only limited to the questionnaires, but also the existing security measures were physically examine through observation and informal discussion with security guard and the officers, during the trip to the premises of the Takoradi Port. Finally, the most relevant information was presented in the finding section of this study and recommendations were made based on the findings.

4 Case Company –Takoradi Port

Profile

Takoradi Port, the older of the two ports in Ghana was built in 1928 as a commercial port to handle all types of cargo including containerized cargo. The port is located in Western region of Ghana. The industrial district of Sekondi-Takoradi, and is the midway between Accra the capital city of Ghana and Abidjan the capital of Côte d'Ivoire. The port is preferred and perfect entryway to middle and northern parts of Ghana and landlocked countries in the Sahel region of Africa, due to good link to its hinterland. Examples are, Mali, Burkina Faso, and Niger. The port operates as the main export port for Ghana as the main export port for Ghana, as it handled 31% of Ghana's seaborne traffic, 66% of national export and 19% of national import. Cocoa, Timber, Bauxite and Manganese are the key export from the port. Primary imports include clinker, wheat, petroleum product and containerized cargo. When Ghana started commercial quantities of oil in the Western Region of Ghana, because the port is well close to the Oil and Gas fields, it supports exploration and production activities at the Oil and Gas fields. Most of the oil supply vessels call at the port to load and offload equipment, chemicals and other supplies that are warehoused in the port facilities including the sheds own by private partners near the port. All the leading shipping lines operated with the port. For example; Maersk Ghana Ltd, Hull Blyth, Safe Marine, Super Maritime Ghana Ltd, Panalpina Ghana Ltd, Bolore group, Maritime Agencies of west Africa, Baj Freight, GETMA and ISAG and others .The port has full range of equipment for all operation alongside other private stevedoring companies.

Interms of performance, the port started its operation with the initial capacity was 1 million tons of cargo, and after the first expansion in 1956, the port was able to handle 1,153 vessels with 2.3million tons of cargo in 1964.The port handled 31% of national seaborne traffic, 17%

of national seaborne imports, 66% of national seaborne exports, as well as increase in vessel calls from 485 in 2003 to 1,664 in the year 2012. This rising occurred as a result of call from Oil supply vessels servicing the oil fields at Cape Three Points. From 2007 when the commercial quantity of oil started, the supply vessel calls have increased from 11% to 65%, total traffic from 3.1 million tons of cargo in 2000 to 5.3 million tons in 2012. Exports too have increased from 1.9million tons to 2.9 million tons, whilst import increased from 1.1million tons to 2.3 million tonnes within the same period of time. There are different kinds of services offered by Takoradi port.

Vessel handling is one aspect of the services Takoradi port offers. The Department of Maritime operation wholly handles vessels that call at Takoradi port, as it is the sole responsibility of Ghana Ports and Harbours Authority, supervised by the Harbour Master.
The following are the vessels handling services:

Again, Pilotage activity is available 24/7, and is compulsory for all vessels entering and leaving, as well as shifting berths within the main harbour, and also has modern slipway with equipped dry-dock facility to accommodate vessels and crafts up to 400 tons.

The port has Tugs that tow vessels within the main harbour as well as mooring and berthing, not excluding tying of ropes and the supply of necessary boats and crew for the purposes of mooring and the allocation of berths to vessels. Notwithstanding these, the port supply fresh water for vessel at berth, and the rate of supply is 20 tons per hour.

In addition the above mention services, Ghana Ports and harbour Authority Offers stevedoring services with other private companies. For cargo handling services, the port authority handles only containerized cargo whereas private company handles non-containerized cargo, with the exception of bulk cargoes. The port has modern storage facilities with covered area of 140,000m^2 including open storage areas of 250,000m^2 with container holding capacity of 5000 tons.
Takoradi port has experienced and dedicated clearing and forwarding agents that offer professional services on handling of all cargoes via the port.
Custom Excise and Preventive Services (CEPS):
The Ghana Revenue Authority (GRA) Customs Division offers services on all Imports and exports through the port of Takoradi.

The port has Fire and Safety department with well-organized, well-trained, committed and dedicated fire – fighting service with modern firefighting equipment. The department offers 24hour services. Including these is an excellent security network with skilled operations staff, as well as trained and dedicated security personnel to ensure the safety and security of

all types at the cargo. Port security department works hand in hand with the National Security, Police, The Bureau of National Investigations (BNI) and the Narcotics Control Board. Takoradi Port is operating at Security Level 1 (one), and the statement of compliance regarding ISPS code was issued on the 7th June 2004.

4.1 Analysis of Existing Security Measures based on media publications and the reports from various international organisations

4.1.1 Security Measures: Identity and Credential Verification

Physical security is obviously a significant factor in thwarting illegal activities though, security could be evaded, if there are absence of effective measures for issuing credentials and verifying the individual or individual intention, ships or cargo(shipment) arriving at the port. What is the usefulness of the strongest lock, if the thieves have the key or the password? Based the questionnaire distributed, and personal observation, the entire Port Facility has been fenced with concrete wall with barbwire. All entrances are equipped with gates and barricades. Before one can get access into the port the person must show his or her harbor pass, which is small booklet issue to the port users to be able to enter the port. The extent to which these measures are actually effective at controlling access by criminal, or other illicit actors is uncertain. On the 14th December 2014, it was reported in the general news through Ghana Webb that, “Two Ghanaian stowaways have been arrested in Spain and have been repatriated to Ghana for prosecution. They were brought back to Ghana through the Takoradi Harbour in the Western Region. According to preliminary investigations carried out by the Takoradi Marine Police, the duo left the West African country through the same port onboard MV Maesk Volta.” Another Stowaway incident happened at Takoradi Port, and was reported by Cityfmonline on 17th October, 2014 that, “nine had concealed themselves in a Singaporean vessel, MV Kota Bunga which had come to Takoradi, loaded bauxite and was about to depart to China. According to Ghana police, the nine had entered the port and sneaked into the vessel. They hide themselves in various places including the anchor hole (area created for the anchor). After going through the normal processes before departure, the crew detected some human activities and had to conduct a search all over again. Realizing danger the nine came out of their holes and jumped into the sea”.

4.1.2 Security Measures: Physical Security

Government of Ghana and Ghana Port and Harbours Authority has invested substantially to enhance physical security at Takoradi Port, particularly in the port facilities, by which petroleum products are exported. The Government of Ghana perceives it oil infrastructure and

port facilities as a strategic asset for the nation, which deserves to be protected by the state. The Ghana Ports Harbours Authority in Takoradi have dedicated much of their expenditure on security by acquiring different kinds of security gadgets and other technologically advanced equipment, as well as CCTV cameras. The Takoradi Port Facilities are protected by concrete wall fence with barbwire. All entrances are equipped with gates and barricades. Most of the security precautions at Takoradi port are hidden from view. The security infrastructure of Ghana Ports and Harbours is linked to all the public security institutions within, and around the port for re-enforcement in case of emergency. With trained security personnel's who can effectively respond to threats with new security equipment, yet internal conspiracy among the security personnel's and the staff without security duties, regarding cargo theft has been the major threat for years. The Port Authorities believes with the implementation of ISPS code, they had imposed rigorous measures to avoid unauthorised access to the port premises or facility. But the ISPS code applies to only the interface of the port facility and the ship. The main focus of ISPS code is on external threats and does not address supply-chain security issues as a primary concern. As the main attention is on the external threat, it is likely that the internal security system may be vulnerable for internal conspirator to initiate criminal activity or terrorist act from inside the fence line of an ISPS-complaint facility.

Moreover, form the critiques regarding ISPS code; it came to notice that it does not apply to fishing vessels and vessel with cargo not above 500 tones. It undeniable fact that Pirate, Trafficker of illegal goods (drugs, firearms, etc.) and stowaways can carry out their criminal activities through fishing vessels." (John P. Hogan and Lindsay Chapman. 2005)
With sufficient number of security personnel's in and out of the port, as well as regular patrols alongside Marine Police on the anchorage area of the Takoradi port. On the 12th Octber, 2011 it was reported in Ghana Oil Watch through public News Paper (Daily Graphic) that "Crews on board some merchant and supply vessels that call at the Takoradi Port engaged in illegal bunkering of large volumes of petroleum products for cash at the Takoradi anchorage. The danger, however, is that the perpetrators engage state security personnel in uniform to give them cover during their operations." The pilfering at the ports in Ghana has been a dilemma and repeatedly being a key to discouragement in doing business through the ports. For many years the threat of pilfering has been increasingly in a complicated trend, and the ports authorities find it difficult in their quest to arrest this situation. The information reaching Ghana Ports and Harbours Authority (GPHA) indicates that pilfering is a key problem at the ports which negatively impacting the Shipping business and National economy. This prompted a research survey to be conducted in 2007 to figure out measures to curb menace. "Among the major findings of the research was the involvement of Port security personnel, Port Terminal workers and GPHA drivers involved in the many cases of theft at the ports. The research study was done at both the Tema and Takoradi ports with a sample size of over One Hundred and Fifty (150) respondents.

Forty percent (40%) of respondents interviewed indicated there was collusion between Port security personnel, terminal workers and GPHA drivers in various acts of pilfering at the Ports. About fifty-six percent (56%) of respondents indicated that the procedure involved in reporting problems regarding pilfering related matters would lead to waste of time. As a result, this situation served as an incentive for the many pilfering activities at the ports as procedures for reporting such cases proof counterproductive. Twenty percent (20%) of respondents were not even aware of where to report such issues, compounding the difficulty in reducing the menace further. Fifty-six percent (56%) of respondents were unaware of the procedures for redress when cargo is lost. This picture creates a very serious affront to the efficient and cost effective operation of the ports."

The substantial amount of investment made by Government and the GPHA to heighten the security system of the port may be undermined by the potential traffickers and others criminals who will infiltrate either security systems design to protect the port infrastructure or institutions associated with maintaining the port infrastructure. The extent, to which the cases regarding the trafficking, cargo theft, and stowaways are linked to the port infrastructure and the security systems, proves the effectiveness of the port security system.

The Ghana Government and the Takoradi port authorities have made physical security in port an important foundation in every aspect of their port operation. The development of large and competent in source security is another component of the effort. However, regarding the allegiance and professionalism of some of the port security staff that has been assigned to ensure security at Takoradi Port, raises a question.

4.1.3 Security Measures: Illicit Use of the Port

"The Port of Takoradi is renowned for its excellent security network, with skilled operational staff and drilled as well as dedicated security personnel to ensure the safety and security of all types of cargo.The security network has further been improved with the installation of a closed – circuit television network in the Port. Under this system, cargoes and personnel working in the port are safe and secured. The department works hand in hand with the National Security, Police, The Bureau of National Investigations (BNI) and the Narcotics Control Board.) On the year 2011, Ghana Maritime Authority through Ministry of Transport, secured secure a loan of 16,625,835 Euros from Finland, to procure Vessel Traffic Management Information System (VTMIS) with the intention of establishing 24 hour electronic surveillance and monitoring of Ghana's coastline as well as Exclusive Economic Zone (EEZ) to safeguard Oil terminals, gas pipelines, prevention of illegal fishing, piracy and prevention of ship source pollution, including maritime resources as well as offshore installations . The system consist of eight (8) Remote sensor site each will have communication Towers and equipped with ma-

rine radars, Automatic Identification Systems (AIS) and CCTVs for detecting and identifying ships and boats. These are in compliance with the International Maritime Organization (IMO) mandated Global Maritime Safety and Distress Systems (GMDSS). Ghana port and harbours Authority is a beneficially of the VTMIS. With all this system in place, yet there are various reports in connection with illicit use of the port for trafficking Drugs.

According to 2013 International Narcotics Control Strategy Report, "Ghana continues to be a transshipment point for illegal drugs, particularly cocaine from South America and heroin from Afghanistan and Pakistan to Europe and United States. Law enforcement officials reported that traffickers are increasingly exploiting Ghana's relatively unguarded and porous maritime border, offloading large shipments at sea onto small fishing vessels, which carry the drugs to shore undetected. Some narcotics enter Ghana from other locations in West Africa. Narcotics are often repackaged in Ghana and then hidden in shipping containers or secreted in air cargo." From the report, the traffickers exploit both Takoradi and Tema port. "As a matter of government policy, Ghana does not encourage or facilitate illegal activity associated with drug trafficking. Corruption continues to be an issue in Ghana with citizen having perception that, corruption is endemic in the police service, as well as in other government institutions". However Ghana Law enforcement is working with neighboring countries on joint interdiction efforts to overcome the menace.

Notwithstanding that, the report stated that United State and Ghana Law enforcement U.S. and Ghanaian law enforcement is taking pleasure in excellent cooperation on counternarcotic by providing technical support to some Ministries and offices in Ghana. Also United States funded the formation of West Africa Regional Training Centre in the Capital city of Ghana which was open on 2013 as part of the West Africa Cooperation Security Initiative. Meanwhile, 2014 NACOB reports stated "the method of transit for drugs is slowly shifting from air to land through Ghana's border with Togo." This might be as a result-improved security measures the port.

4.1.4 Security Measures: Supply Chain and Cargo Security

Takoradi facility has an installed gamma ray container scanner to facilitate the clearing of containers and improve the quality of services delivered to customers as well as detecting illicit material been loaded into the container for shipment.

4.1.5 Terrorism and Tarkoradi Port

The information gathered indicates that Takoradi port has never been linked to any case associated with Terrorism. The level of security at the port has always been at level 1(one)

4.1.6 Port Of Helsinki

For the purpose of benchmarking, the same interview was conducted at Port of Helsinki the port security Adviser to ascertain the how security services is being carried out over there. Unfortunately, due to security reasons the officer could not divulge the needed information which will enable me to do proper benchmarking. Nevertheless some little information was ascertained through the interview. Unlike Takoradi port, the major part of the security services at the Port of Helsinki has been outsourced to private security company. All the guarding services are being provided by private security. Measure regarding Identity and Credential Verification, all the staff and port users must pass through the gate with coded ID cards which; they swipe through an electronic reader and then enter the PASSWORD. If you are a visitor, the moment you arrived at the reception, after few interrogation by the security guard, then he or she will offer you a visitor's tag after satisfied with your mission, which will identify you as a visitor. From few observations and little information ascertained, when it comes to security measures, Takoradi has similar efforts to build stronger security for its ports. However, the extent to which similar protections is provided by Takoradi port, may create vulnerabilities in the port infrastructure security system.

4.2 Conclusion

The purpose of this study is to identify the threats and the vulnerabilities and finally recommend measure to overcome the identified threats and vulnerabilities.
Various categories of potential threats and vulnerabilities have been studied throughout the literature review. However, because each port presents a unique sets of threats and vulnerabilities, there was a need to look critically into how Takoradi port operations are being conducted in other to identity the potential threats and vulnerabilities pertaining to the said port. The result of this study shall be the basis upon which the necessary recommendation will be given. However several researches need to be conducted in order to identify the best possible solution to overcome the potential challenges presented by the Port.

This research was based on the following key question: How to develop resilient security system for Takoradi Port?"
Answer the main question; the following question also came to mind: (ii) has there been any security incident linked to Takoradi Port? (ii) If yes, how many time are those incidents linked to Takoradi Port? (ii) How do those incidents happen? Are there in place, security measures to

prevent those incidents? How effective are these measures, in preventing those security incidents? These prompted me to develop a questionnaire to search for the information regarding the existing security control measures, including vulnerabilities and threats associated with the security control measured, as well as operational activities within the port.
Case study methodology was used to research on this research question. The material for this research was collected through questionnaires, informal discussion and observation. The above mention techniques were used in gathering material for this research though, some of the material were also gathered through local media and international institutions' website.

4.2.1 The current Picture of the security at the port

The feedback from the respondents has demonstrated the strengths and the weaknesses regarding the security systems at the Port of Takoradi.
Looking at face of the feedback, the strength of the security systems falls on the; Security Measures For Access Control Personnel, Security Measures For Access Control-Perimeter, Security Measures For Delivery Of Ship Stores, Security Measures For Monitoring, and Communications systems. Even though there are few area that need to be looked into for improvement. For instance, security measures for handling Cargo, and also availability of necessary information to the security guards. Because from their responds you could feel that though some security systems or measure were in place but when questions were asked some could not answer due to lack of information or knowledge.

From the feedback receive from the respondents you could see that the most of the security staf have little or no knowledge regarding the ISPS code, which is the new security regime for ports and ships. Again, the feedbacks received from questions under Port Facility personnel with security duties regarding adequate and regular security training, the feedbacks got from the respondents were conflicting with each other. Some replied no, whiles others replied yes. In my opinion, the feedback is an indication that some of the security staff lacks adequate security training and education.

Moreover, the feedbacks from the questions under drill & exercise requirements show some misunderstanding between drill and exercise on the part of the respondents. From their responds, drill and exercise are the same. The responds given to the questions regarding drill were the same as the responds for the exercise. Meanwhile the scope of the drill is different from that of exercise.

Again, there was a question that asked for the last date for drill, and one of the respond stated that, the last date for the drill was 2011. Meanwhile I distributed the questionnaire at the end of April 2014. Some even didn't give the date at all. This is an indication that the re-

quirement, which stated, drill must be carried out; at least every three month has not been carried out accordingly. An exercise is yearly activity, which includes extensive training in which different part of the Port Facility Security Plan (PFSP) or Port Security Plan (PSP) are practised. During exercise, communication, coordination, availability, resources, as well as reactions, is practice and reviewed. Drill on the other hand, is a small, coordinated practice of which, at least one aspect of the Port Facility Security Plan (PFSP) is tested. Normally, drill is applied to examine, or test a procedure or a specific function, and serves to keep high level of readiness. (European handbook of maritime security exercises and drills, 27).
In my view, this will produce in inefficiency and ineffectiveness on the part of the security force as they try to enforce the existing security measures. It could also serve as potential threat to the implementation of the security requirement to prevent criminal or terrorist activities. According to Christopher, K (2014, 68), if the staff responsible port security lack adequate training, there is higher possibility for crime and infiltration by internal conspiracies.

Furthermore, the feedback received from questions under measures for monitoring the show that facility has adequate lighting but the light does not project onto the water/sea. Most of the stowaways use the water as their way to get into the ship, and so, if there weren't any light that project onto the water, then, it would be easy for the stowaways to have their way into ships easily, due to the darkness on the water or that sea.
Also from the questionnaires distributed, the feedback shows that security education is not extended to non-security staffs. The more security conscious the employees are, the better the effectiveness of the security measures will be achieved. John Leach (2003) observes two sets of factors, which changes the employee behavior. The first set comprises user knowledge regarding what the company expects from the employee. Second sets include factors that empower the willingness of the employee to conduct him or herself within acceptable, approved standards and practices of the company. According to John Leach (2003), human knowledge is based on; what they have been told, what they see practice around them, and their past experience. Several companies have documented security policies, practices, standards and procedures, however, the effectiveness to influence the security behavior depends on the body of Knowledge accessibility, the completeness of its coverage, clarity of the stated security values and its uniformity

Base on personal interaction with the security staff and other employees, it was discovered that their attitude toward security very bad. This is because they perceive security as threat to their daily operation. Whenever they see security guard around them, the first thing that comes into their mind is that, the security guard is there to spy them. This will not bring cooperation among the security personnel's and personnel's without security duties. If such persist, it will always bring unnecessary tension between the security staff and non-security

staff, which will not assist in providing adequate security measures, because risk analysis will always be based on assumption due to lack of cooperation. It came to realisation that non-security staffs lack adequate information about security in relation to their work.

Apart from the weaknesses identified through the questionnaire, the material gathered through the local media and international institutions reveal some pothole in the security systems operated in Takoradi port.

Considering the stowaway and drug trafficking cases that have been linked to the Port of Takoradi, there is no doubt that the security system within Tarkoradi port is weak and leaky. Even though according to 2014 NACOB reports "the method of transit for drugs is slowly shifting from air to land through Ghana's border with Togo." Which did not mention Takoradi port, yet it doesn't mean the port is immune to drug trafficking, because the human factor within the security system has not been removed.

The difficulties of the security cannot be isolated from broader security context. Even though there may be stringent checks point in and around Takoradi Port. The Management of Takoradi port may have purchase the best security technologies that money can afford, trained their employees so well that they secure all their facilities, including what is contain in the facility, locked every access before going home, and have well train security staffs to guard the port premises and the facility, yet the port is still vulnerable. The port users and other individuals may follow the best and required security practice recommended by the ISPS Code and other security experts, installed the needed security products with complete vigilant regarding the security systems, individuals are still vulnerable. Why? According to Kevin D. Mitnick &William L. Simon (2002), "the human factor is truly security weakest link. One of the world's most renowned scientists of the twentieth century, Albert Einstein said, "Only two things are infinite, the universe and human stupidity. But what is much more prevalent than the real stupidity is living stupid, closing your ear, not listening and not seeing
Criminal can infiltrate the security system and succeed when people are corrupt or ignorant regarding good security practice. With similar attitude, as how security-conscious the employees and management of Takoradi Port may be, it a mistaken belief that the port is largely protected from attack or cannot be infiltrated by criminal because they have set up standard security products – CCTV systems or strong authenticated device such as biometric smart cards. If anyone thinks, security products alone offer true security, that person is deceiving him or herself in term of security. Such people should anticipate for future security incident. According to Security consultant Bruce Schneier (2008), "Security is not a product, it's a process." Moreover security is not a technology problem it's a people and management problem.

The results of the study show that there is; in adequate education and knowledge regarding ISPS Code. Requirement of Drill and Exercises are not been followed. Base on the report from local media and internal institutions, though terrorism is perceived to be non-existence in the Takoradi port, the other maritime crime particularly, stowaway, trafficking of illicit drugs and cargo theft still remain. These threats are gaining their root in the port, because the system through which individual credentials and identity as well as individual intention are being verify, proves ineffective. This is because integrity of some of the law enforcement agencies and security personnel including personnel's without security duties may have been compromised. I therefore propose the following measures to be applied.

4.3 Recommendations

4.3.1 Preventing Theft And Other Criminal Activities

Individual criminal motive alone cannot be amount to a crime without opportunity and the means. All (motive, opportunity and means) need to come to together for crime to happen. Individual motive cannot be controlled, means is difficult to control, but opportunity can be controlled. So the security measure must focus on the opportunity to minimise it as much as possible to affect the final result. Necessary measures must be put in place to make sure those opportunities, which will encourage crime, is reduced. If the opportunities for the attack or criminal activities are minimized considerably, then the criminal will be discouraged from focusing on the port facility, person or the infrastructure being protected.

4.3.2 Extensive or Adequate education on ISPS Code

Feedback receive from the respondents shows that the most of the security staf have little or no knowledge regarding the ISPS code, which is the new security regime for ports and ships. Therefore, there is the need for the security personnel to be educated extensively on the ISPS code.

4.3.3 Training, Drill And Exercises

Though security exercise could be practiced on the managerial level and the operational level with the port facility, nevertheless, when operational level and the managerial level are join together, it has a great benefit, since it will assist management to recognise the security loopholes throughout the entire levels within the organization, and as a result of that, wider support will be welcome for improvement. Moreover, it will enable the security management team to prepare the needed programs and the security measure to fix the loopholes.

4.3.4 Stowaway

The danger that comes as a result of stowaway incident affects all the stakeholders (port, ship, and maritime industries including the image of the country. Shipping companies have shown more concerned regarding the high cost and risk from stowaway. If the shipping lines keep on paying penalty on stowaway incidents, the will lose interest in transacting business through the said port. If such happened, the income of the port will be decreased. Automatically, every one that depends on the port for a living will be negatively affected. Fighting against the threat of stowaway must be welcome by all the stakeholders regarding maritime commerce.
There is possibility that, stowaway incident will be getting worse in the coming years, should current global economic problems persist. For instance, areas like Africa.
Hence, comprehensive and effective stowaway search and procedures should be applied to all ships that enter Takoradi port before the ship leaves the port. As part of quarterly drill program stowaway search should be included on potential stowaway target vessels or ships. This include the following steps:

First, stowaway search list should be divided into sections for orderly search, before it leaves the port. Sufficient time must be allowed for stowaway search, and there should be acknowledgement from the Master showing his satisfaction regarding the search.

Secondly, Port authority should employ a permanent Gangway for the Ganway operation, and also huge amount of penalty for all the security officers and guards, not exluding all workers on duty that give way for stowaway, during discharging and loading.
Inaddition to the above mentions measures, there must be regular patrol both anchorage and with the port.

Moreover there should be documented terms and condition to be complied by the agents and security staff on duty, whilst the ship is in port be held liable for all cost of disembarkation and repatriation, if it discovers later that the stowaway have managed to on board the ship or vessel from Takoradi Port.

Last but not the least, to motivate the angents and the security staff to be more vigilant while on duty, the agents and security staff should be rewarded for stowaway free sailing.

4.3.5 Controlling Illicit Drug Trafficking

Controlling illicit drug traffickers and the criminals from exploiting port; the stringent measures are needed to enforce immigration rules concerning merchant seamen and passen-

gers' access to the port facility. I suggest the following measures to be carrying out to control the illicit use of the port for drug trafficking and criminal activities through the port.

In the first place, port operators and individuals working or accessing the port must be go through thought investigation check before allowing them to access the port

Secondly, Cargo should be presented 24h hour before loading, for necessary inspection to be done.
Thirdly, Loading operations should be re-programmed, and then security staff be trained to deal with container inspection.

Further, container platform or yard surveillance technology programs should be developed and implemented to improve security throughout the entire supply chain by inspecting the identity of all players concerning the supply chain to safeguarding the integrity of the port premises the supply chain.

Access control is crucial while vessel(s) is or are in port, and for that matter all the person on board be identified, and also ensure that seals are fastened on all the loaded containers.

4.3.6 Ensuring Integrity and Countering Corruption

All the stakeholders must be made to understand the importance of the integrity of the system, which is being protected from internal threats as the key component for evaluating the security measures. To combat internal threats, there should be a process to assess the transparency of the every operation and activities that concerns the port. There should be continuous interaction among all the players within the port to make sure every activity is being carried out appropriately, and that corruption is not allowed.

Furthermore, application of human resource management activities to improve the operation's competitive position, through recruitment and development of competent employee and managers, via development of staffing plans, and must be a key contributor to their economic success.

4.3.7 Cost

Regarding the cost aspect, there is the need for partnership and cooperation among Ports and Governments within West Africa sub-region, in relation to information sharing, capacity building, technical assistance, and financial support, through the establishment of a funding plan to raise fun from public to enable the ports to ease financial burden, which will also create

opportunity for the port within the sub-region to build a strong security network, to enable authory to track down the criminal and stowaways menace.

4.4 Future research

Human factor as a threat to the implementation of Port security measures is still not fully studied and need further exploration despite the fact that within past few years there has been emphasis on corruption and espionage from the point of security threat. Considering the threats and vulnerabilities regarding port security, human factor cannot be overlooked, when implementing security measures or safeguards. This is because human factor can serve as an obstacle to the successful implementation of the security measures. Preventing internal threat to security is one of the most challenging and complex task facing security and law enforcement within the port, because of employees' unique access to vessels and the infra-structure with the port. According to Kevin D. Mitnick &William L. Simon (2002), "the human factor is truly security weakest link. One of the world's most renowned scientists of the twen-tieth century, Albert Einstein also said, "Only two things are infinite, the universe and human stupidity.

References

LITERATURE

Andrew, R. Thomas.2010.International Practices and Innovations in Moving Goods Safely and Efficiency. Vol.1. California: Greenwood press, 166-170

Arthur G, Arway .2013.Supply Chain security: A comprehensive Approach. Boca Raton, Florida: Taylor &Francis Group, 3

Burges, D. 2013. Cargo Theft, Loss Prevention, and Supply Chain Security. Waltham, USA: Butter-worth-Heinemann, 12

Christopher, K .2014.Port Security Management.2nd ed. Boca Raton, Florida: Taylor &Frances Group, 67.

Creswell, J.W. 2009.Research Design: qualitative, quantitative, and mixed methods of approaches .3rd ed. Thousand Oaks, California: Sage, 4.

Denscombe, M.2008.The Good Research Guide: For small-scale Social Research Projects (3rd Ed.).Maidenhead: Open University Press

Denzin, N.K and Lincoln, Y.S. (Eds). 2003. The SAGE Handbook of Qualitative Research. Introduction: The Discipline and Practice of Qualitative Research.2nd Ed. London: Sage Publication.

Edgerton, M. 2013. “A Practitioner's Guide to Effective Maritime and Port Security”, John Wiley &Sons, Inc., Hoboken, New Jersey

Hammersley, M.1990. Reading Ethnographic Research: A Critical Guide. London: Longmans

Hammersley, M.1992.What’s wrong with Ethnography? Methodological Explorations. London: Routledge.

Johnson, B. & Christensen, L.2008. Educational research: quantitative, qualitative and mixed approach. Thousand Oaks, CA: Sage Publication. 34

Kabay, M. E.2002.Computer Security Handbook: Using Social Psychology to Implement Security Policies 4th ed. Wiley & Son, New York, 35.1-6

Kevin D. Mitnick &William L. Simon. 2002. The Art of Deception. Wiley publishing, Inc., Indianapolis

Lee, T.W.1999.Using Qualitative Methods in Organizational Research. Thousand Oaks, California: Sage

Lincoln. S., & Guba, E. G.1985. Naturalistic inquiry. Beverly Hills, CA: Sage, 303

Louisa A. Tyska, CPP Lawrence J. Fennelly.2001. Cargo Theft Prevention: A hand book for Logistics Security.3rd Ed. American Street for Industrial Security. Alexandria, USA, 83

Moisander, J. and Valtonen, A.2006. Qualitative Marketing Research: a cultural Approach. London: Sage, 27

Rowbotham, J.Mark. 2014. Introduction to marine cargo management .2nd Ed. New York: Taylor & Francis Group, 277

Saunders, M. Lewis, P. & Thornhill, A.2009.Research Methods for business students. 5th Ed. Harlow: FT/Prentice. 256-288

Schneier, B.2008. Schneier on Security. Wiley publishing, Inc. Indianapolis, 1

Seale, C. (1999). Quality in qualitative research. Qualitative Inquiry, 5(4), 465 478.

Stenbacka, C. (2001). Qualitative research requires quality concepts of its own. Management Decision, 39(7), 551-555

Thomas L.Friedman.2007.The World Is Flat: A brief History of the Twenty-first Century.3rd Ed. New York: Farrar, Straus and Giroux, 8.

William Langewiesche.2004. The Outlaw Sea: A world of freedom, chaos, and crime. New York: North Point Press, 7.

Yves-C,Gagnon.2010. Case Study as Research Method. Canada , Del' Universite' du Que'bec

INTERNET

Alexandros M. Goulielmos, Agisilaos A. Anastasakos. 2005. "Worldwide security measures for shipping, seafarers and ports: An impact assessment of ISPS code", Disaster Prevention and Management: 14, 472
http://dx.doi.org/10.1108/09653560510618311 (accessed 10 October, 2014)

Bateman, S. 2009. Maritime security implications of the international shipping recession. Australian Journal of Maritime and Ocean Affairs, 1(4), 115. http://search.proquest.com/ (Accessed 14 October, 2014)

Bichou, K. 2004. The ISPS code and the cost of port compliance: An initial logistics and supply chain framework for port security assessment and management. Maritime Economics & Logistics, 6(4): 323.
http://search.proquest.com/ (Accessed 9 October, 14)

Botelho, R. (2004). Maritime security: Implications and solutions. Sea Technology, 45(3), 18. http://search.proquest.com/ (Accessed 14 October 2014)

BUREAU OF INTERNATIONAL NARCOTICS AND LAW ENFORCEMENT AFFAIRS.2013. International Narcotics Control Strategy Report (INCSR)
http://www.state.gov/j/inl/rls/nrcrpt/2013/vol1/204049.htm#Ghana (Accessed 29 January 15)

Citifmonline.2014.Stowaway Drowns after jumping into sea at Takoradi Port
http://www.citifmonline.com/2014/10/17/stowaway-drowns-after-jumping-into-sea-at-takoradi-port/#sthash.PFCc7L5N.dpuf (Assessed 20th January 2015)

C-TPAT-BSI-Supply Chain Soulutions
http://bsi-supplychainsolutions.com/en-US/about-us/government-programs/ (Assessed 10th Jan. 15)

Dr. Ikokide Zebulon .2014. "Does Nigerian Deserve the US Sanction over ISPS code Implementation?" The Shipping position online new
http://shippingposition.com.ng/article/does-nigerian-deserve-us-sanction-over-isps-code-implementation (Accessed 19 October 2014)

Ethan A. Nadelmann.1990. "Global Prohibition Regimes: The Evolution of Norms in International Society" "International Organization, 44(4), 481
http://www.jstor.org/stable/2706851 (accessed 14th October, 2014)

European handbook of maritime security exercises and drills, 27
http://www.kystverket.no/Documents/Havner/Havnesikring/H%C3%A5ndbok%20for%20planlegging,%20organisering%20og%20gjennomf%C3%B8ring%20av%20%C3%B8velser%20og%20driller.pdf (Assessed 11th February 11, 2015)

Flynn, S. E.2007. The morning-after problem. Journal of Commerce

http://search.proquest.com/ (accessed 10 October, 2014)

Gard Guidance on Stowaways, 4 http://www.gard.no/ikbViewer/Content/2287134/Guidance%20to%20stowaways.pdf (Assessed 3 December 2014)

Ghana Maritime Authority-Maritime Security http://www.ghanamaritime.org/en/about-us/programmes/maritime-security.php (15th January 2015)

Ghana Oil Watch.2011. Illegal oil Bunkering in Takoradi Port http://ghanaoilwatch.org/index.php/ghana-oil-and-gas-news/646-illegal-oil-bunkering-in-takoradi-port (Assessed 27th January 2015)

Ghana Ports and Harbours Authority: Services Takoradi http://ghanaports.gov.gh/tr/page/42/Services-Takoradi (Assessed 2nd January 2015)

Ghana Ports and Harbours Authority http://ghanaports.gov.gh/tr/default (Assessed 20th January 2015)

Ghana Webb.2014.Ghanaian Stowaway arrested in Spain http://mobile.ghanaweb.com/GhanaHomePage/NewsArchive/artikel.php?ID=339108 (Assessed 20th January 2015)

GIFF Secretariat, Supply Chain Security under threat in Ghana, 6 http://www.ghanafreightforwarders.org/GIFF%20JOURNAL.pdf (Accessed 2 December, 2014)

Glenn Faulk & Diego Archer .2010. OFFSHORE AND MARITIME SEAFARER ID STANDARDS UNDER ILO 185, 1. http://library.luminaryglobalimmigration.com/wpcontent/uploads/2013/12/Offshore-and-Maritime-Seafarer-ID-Standards-Under-ILO-185.pdf(Accessed 16 November 2014)

Harrald, J. R.2005. SEA TRADE AND SECURITY: AN ASSESSMENT OF THE POST-9/11 REACTION. Journal of International Affairs, 59(1), 158-159. http://search.proquest.com/ (Assessed 13th October 2014)

ILO-london.2005.New international labour convention for seafarers' ID documents comes into force February 10th 2004. (Assessed 12th June 2015).

IMO. Jan 2013. Formalities connected with the arrival, stay and Departure of persons, 3-6 http://www.igpandi.org/downloadables/submissions/imo/ FAL%2038-6-2%20%20StowawaysInternational%20Group%20of%20P&I%20Clubs%20Data%20on%20Stowaway%20cases%20 (P&I%20Clubs).pdf (Assessed 3 December 2014)

IMO-Maritime Security and Piracy http://www.imo.org/en/OurWork/Security/Pages/MaritimeSecurity.aspx (Assessed 10th June 2015)

IMO Briefing 42/2002. IMO Adopt Comprehensive maritime security measures (assessed 15th June 2015) https://www.infrastructure.gov.au/transport/security/maritime/isps/files/final_act.pdf (Assessed 10th June, 2015)

International Maritime Organization/ISPS Code http://www.imo.org/OurWork/Security/Instruments/Pages/ISPSCode.aspx(Accessed 16 November, 2014)

2014 International Narcotics Control Strategy Report http://www.state.gov/j/inl/rls/nrcrpt/2014/vol1/222893.htm (Assessed 2nd February 2015)

ISPS Code http://www.svg-marad.com/Downloads/International%20Conventions/ISPS%20Code.pdf (Accessed 16 November, 2014)

Jon D. Haveman & Howard J. Shatz.2006. "Protecting the Nation's Seaports: Balancing Security and Cost", 31 Www.ppic.org/content/pubs/report/r_606jhr.pdf (Accessed 26 October 2014)

John J. Green.2012. State data Centre of Mississippi, Annual affiliate meeting. The University of Mississippi Centre for Population studies. https://institutecbr.files.wordpress.com/2011/07/assessment-and-evaluation-presentation-for-sdc-meeting2.pdf (Accessed 20th October 2014)

John P. Hogan & Chapman, L.2005. "International Ship and Port Facility Security (ISPS) code — what does it mean for fishing vessel security?" Number 113, 24.

http://www.spc.int/DigitalLibrary/Doc/FAME/InfoBull/FishNews/113/FishNews113.pdf (Accessed 22 October 2014)

Kennedy, F.2007. "Port ISPS compliance remains problematic" Gulf news.com http://gulfnews.com/business/shipping/port-isps-compliance-remains-problematic-1.206530 (Accessed 19 October 2014)

Leach, J.2003. Improving user security behavior. Computer & security, 22(8), 685-692 http://www.jlis.co.uk/papers/improving_security_behaviours_030903.pdf (Accessed 20th March 2015)

Linda T. Babins.2006. Measuring the Impacts of Increased Security on Ports and Shipping in the Caribbean Basin, Master of Arts, Public Policy & Public Administration, Concordia University,68.
http://spectrum.library.concordia.ca/9126/1/MR20702.pdf (Accessed 20th March 2015)

Lyndon B. Johnson.2006.Port and Supply-Chain Security Initiatives in the United States and Abroad, School of Public Affairs, the University of Texas, Austin, 55.
http://www.utexas.edu/lbj/archive/pubs/pdf/prp_150.pdf (Accessed 14th January 2015)

Maritime Transport Committee, Organization for Economic Co-operation and Development Directorate for Science, Technology and Industry. Paris: July 2003. Security in Maritime Transport: Risk Factors and Economic Impact, 4
http://www.oecd.org/sti/transport/maritimetransport/18521672.pdf (Accessed 5 November 2014)

McNaught, F & RAN.2005. Effectiveness of the International Ship and Port Facility Security (ISPS) Code in addressing the maritime security threat, 91-92
http://www.defence.gov.au/adc/docs/publications2010/publcnsgeddes2005_310310_effectiveness.pdf (Accessed 17 November 2014)

McNaught F. & RAN. 2005. Effectiveness of the International Ship and Port Facility Security (ISPS) Code in addressing the maritime security threat, 94
http://www.defence.gov.au/adc/docs/publications2010/publcnsgeddes2005_310310_effectiveness.pdf (Accessed 26 October 2014)

NEBRASKA STATE PATROL, EXECUTIVE PROTECTION/CAPITOL DETAIL DIVISION, 1
https://statepatrol.nebraska.gov/media/11408/threat_information.pdf (accessed 27 November, 2014)

Nieto, D. 2012. Neoliberalism, biopolitics, and the governance of transnational Crime1/Neoliberalismo, biopolíticay gobernanza del crimen transnacional. Colombia Internacional, (76), 137-143
http://search.proquest.com/ (Accessed 12th October 2014)

Nuthall, K., Fine, P., & Thomson, J. (2003). IMO sets course for port security. Security Management, 47(4): 84-87.
http://search.proquest.com/ (Accessed 9 October 2014)

O'Connell, J.2004. Marine cargo security. Risk Management, 51(3), 30-32
http://www.wilfridlaurieruniversity.ca/documents/20829/Marine_Cargo_Security.pdf (Assessed 24th February, 2015)

OECD.2003. Security in Maritime Transport. 23-27.
http://www.oecd.org/newsroom/4375896.pdf (Assessed 10 June 2015)

Office of the Press Secretary, U.S. Department Of Homeland Security. 2003. PROTECTING AMERI-CA'S PORTS: Maritime Transportation Security Act of 2002 (MTSA 2002), WASHINGTON, D.C, 3.
http://www.maritimedelriv.com/publications/press/DHS/MTSA_OCT_FINAL_KIT_DRAFT.pdf (Accessed 15 November 2014)
Perils on the sea.2004, Jul 07. Economist.Com / Global Agenda, 1.
http://search.proquest.com/ (Accessed 13 October 2014)

Pinto, C. A., & Talley, W. K. 2006. The security incident cycle of ports. Maritime Economics & Logistics, 8(3), 270
http://dx.doi.org/10.1057/palgrave.mel.9100159 (Accessed 10 October, 2014)

PSM One.2014.Cargo Theft on the Rise across the Nation
http://www.freightwatchintl.com/sites/default/files/attachments/FreightWatch%202013%20Global%20Cargo%20Theft%20Threat%20Assesment%20Full_0.pdf (Assessed 11January 2015)

Robmarine.2013. Archive Stowaway News and Reports
http://www.robmarine.com/html/stowaway-data/archive-news/13-news.html (assessed 2nd January 2015)

Schreier, F. (DCAF). 2010. Trends and Challenges in International Security: An Inventory. Occasional Paper – №19, 57-60

http://www.dcaf.ch/Publications/Trends-and-Challenges-in-International Security (Assessed 6th February 2015)

Senate homeland security and governmental affairs committee hearing. 2014. (). Lanham: Federal Information & News Dispatch, Inc. http://search.proquest.com/ (Assessed 19 November 2014)

Shah, S. K. (2004). The evolving landscape of maritime cybersecurity. Review of Business, 25(3), 32.
http://search.proquest.com/ (Accessed 10 October, 2014)

SPENCER, C .209. The Standard Safety Special Feature - Stowaways
http://standard-club.com/media/23802/standard_safety_april_09-2.pdf (Assessed 9th February, 2015)

Schneier, B.2008. "The Psychology of security"
https://www.schneier.com/essays/archives/2008/01/the_psychology_of_se.html (Assessed 10th February 15)

Stasinopoulos, D. 2003. Maritime security - the need for a global agreement. Maritime Economics & Logistics, 5(3), 318.
http://search.proquest.com/ (Accessed Oct. 13, 20014)

Supply Chain Secuirity in the 21St Century
http://www.securitas.com/Global/Pinkerton/Supply%20Chain%20Security.pdf (Assessded 10th January, 2015)

Supply Chain Security Programs and Issues
http://www.worldshipping.org/industry-issues/security/cargo-and-the-supply-chain/supply-chain-security-programs-and-issues (Assessed 1st June,2015)

Thibault, M., Brooks, M. R., & Button, K. J. (2006). The response of the U.S. maritime industry to the new container security initiatives. Transportation Journal, 45(1), 13
http://search.proquest.com/ (accessed October 10, 2014)

United Nations Conference on Trade and Development, .2004. Container Security: Major Initiatives and Related International Developments, 20-34. (Accessed 11 November 2014)
http://unctad.org/en/Docs/sdtetlb20041_en.pdf

United Nations Conference on Trade and Development.2010. Emerging challenges and recent developments affecting transport and trade facilitation, 8 http://unctad.org/en/docs/cimem1d8_en.pdf (Accessed 21 October, 14)

UNCTAD secretariat.2007. MARITIME SECURITY: ISPS CODE IMPLEMENTATION, COSTS AND RELATED FINANCING, 26 http://unctad.org/en/Docs/sdtetlb20071_en.pdf (Accessed 22 October 2014)

Using Social Psychology to Implement Security Policies http://www.mekabay.com/infosecmgmt/Soc_Psych_INFOSEC.pdf (Assessed 9th February 2015)

Wade, J. 2005. MARITIME SECURITY. Risk Management, 52(12), 41. http://search.proquest.com/ (Accessed 26 October 2014)

Widdowson, D & Holloway, S.2009. Maritime Transport Security Regulation: Policies, Probabilities and Practicalities, 3(2), 20 www.internationaltransportforum.org/2009/forum2009.html. (Accessed 25 October 2014)

Walsh, C., Ewing, G., & Griffiths, J.2012. Using observation as a data collection method to help understand patient and professional roles and actions in palliative care settings. Palliative Medicine, 26(8), 1049. http://dx.doi.org/10.1177/0269216311432897 (Assessed 11 January 2015)

Figures

Tables

Appendixes

QUESTIONNAIRE

International Ships And Port Security (Isps) Code Documentation

Q1a). Does facility have an approved Port Facility Security Plan (PFSP)? YES/NO

Q1b). How often is the PFSP reviewed?

Q2). Was facility issued a statement of compliance/plan Approval?

- ✓ Security Level Coordination & Implementation

Q4). At what security level is the terminal operation?

Q5). Can you explain the different between security levels 2&3?

Q6). Who sets faciltiy's secirity level?

Q7). What are the major changes to the security of the facility as the security level increases?

Port Facility Security Officer Knowledge & Training

Q8). Has the PFSO received appropriate training to fulfil his/her responsibilities? Yes/No

- ✓ Port Facility Personnel With Security Duties

*Q9a). Do facility personnel with security duties receive **regular** security training? **YES/NO***

Q9b). I, how often does does the security personnel receive regular security training?

*Q10). Do facility personnel receive **regular** training in-house? **Yes /No***

*Q11). Do facility personnel receive **regular** training off-site? **Yes/ No***

*Q12). Are records maintained to document training and exercises? **Yes/ No***

- ✓ Port Facility Personnel Without Security Duties

Q13). Did facility personnel without security duties receive initial ISPS Code training? Yes/NO

Q14a). Do facility personnel without security duties receive regular ISPS Code training? Yes / No

Q14b). If yes, how often:

*Q15). Do facility personnel attend in-house security training? **Yes / No***

*Q16). Do facility personnel attend off -site security training? **Yes / No***

*Q17). Are new personnel indoctrinated with all relevant with all relevant security measures? **Yes / No***

Q18). Are records maintained to document training and exercise? Yes/No

- ✓ Drill & Exercise Requirements

Q19a). Are drills conducted at least every 3 months? Yes/ No

Q19b). Date /Type of Last Drill:

Q19c). Who participates?

Q20). Are exercises conducted each calendar year, with no more than 18 months between exercises? Yes / No

Q20a. Date/Type of Last Exercise:

Q20b). Who are the participants?

Q21). Are records of drills and exercises maintained? Yes/ No

Q22). To whom is the result of drills and exercises reported to?

- ✓ Security Measures For Access Control-Perimeter

Q23). Does a fence or wall surround the entire facility? Yes/ No

Q24). Is the fence clear of debris/ Vegetation? Yes /No

Q25). How many access gates does the facility have? Yes / No

Q26). Are there separate access gate/ portals for pedestrians and vehicles? Yes / No

Q27). Are all entrances equipped with gate or barricades? Yes/ No

Q28). Are guards posted to all access point? Yes / No

Q29). Is all access point equipped with appropriate warning signs? Yes/ No

- ✓ Security Measures For Access Control –Personnel

Q3a). Describe access control procedures for employees (badges, etc.).

Q31b). If access cards are issued, are they:
Colour-coded? Yes/No

*Q31c). Include a photograph of the employee? Y**es/No***

Q31d) Have expiration date? (ID expires – month/ years from issue) Yes/ No

31e,) does the card include biometric info? Yes/No

Q31f). Is the card connected to an electronic card reader system? Yes/ No

Q31g). Do all employees have access cards? Yes / No

Q32a). Are background checked conducted before access card are issued? Yes/No

Q32b) which people conducts the background checks?

Q33). Are ship crewmembers allowed ashore? Yes / No

Q34). Are ship crewmembers screened by immigration? Yes / No

Q35). Does the facility have segregated areas for embarking/disembarking passengers? Yes/No

Q36). Describe the passenger screening process

Q37). Are vehicle screened prior to entering the facility? Yes/ No

Q38a). Do government agencies have access to screen baggage? Yes / No

Q38b). If yes, who are the agencies?

Q39). Do security personnel control access to restricted areas? Yes/No

- ✓ *Vessels(Passenger and Vehicle) & Cruise Ship Terminals Only*

Q40). Does the facility have segregated areas for embarking/disembarking passengers? Yes /No

Q41). Are accompanied baggage's screened priors to entry into the facility? Yes/ No

Q42). Are vehicles screened prior to entering the facility? Yes/No

Q43a). Do government agencies have access to screen baggage? Yes/No
Q43b). If so, what agencies?

- ✓ *Security Measures For Handling Cargo*

Q44). Describe method for screening truck drivers:

Q45). Describe methods for screening cargo vehicles

Q46). Is x-ray equipment used to screen cargo? Yes/No

- ✓ *Security Measures For Delivery Of Ship Stores*

Q47). Are ship stores received at the facility? Yes/No

Q48). Are vendors and ship stores screened prior to entering facility? Yes/No

Q49). Is advance notification of deliveries required? Yes/No

Q50). Are vendors supervised while delivering ship stores? Yes/No

Q51). Is there a separate storage area for ship stores? Yes/ No

Q52a). *Do government agencies have access to screen ship stores? Yes /No*

Q52b). *If yes, what agencies*?

- ✓ *Security Measures For Monitoring*

Q53). How is the landside of the facility monitored?

Q54). Does the facility have a CCTV system? Yes / No

Q55). How much of the facility does the CCTV system cover?

Q56). Are the CCTV cameras monitored at all times? Yes /No

Q57a). Are CCTV recordings stored? Yes/No

Q57b). How long?

Q58). Are stored CCTV recordings protected with restricted access? Yes/No

Q59). Does the CCTV system have a secondary (backup) power source? Yes/No

Q60). What procedure to follow if the cameras suddenly fail at night?

Q61). Does facility have an effective plan for limiting waterside access? Yes /No

Q62). How often are waterborne patrols conducted?
Answers from the respondents:

Q63). Does facility have signs facing the water stating that access is restricted? Yes/ No

Q64). Does facility maintain one or more waterside patrol boat(s)? Yes/ No

Q65). Are guards maintained on docks at all times when ships are in port? Yes/ No

Q66). Does the facility have any anchorages or berthing areas? Yes/No

Q67). Does the facility have a plan to monitor these areas? Yes/No

Q68). Does the facility have a means to access a vessel in their anchorage? Yes/No

Q69). Does the facility have adequate lighting?

i) At access point? Yes /No

ii) At the pier/ship-port interface areas? Yes/No

iii) *Projected onto the water? Yes/No*

Q70). *Do the lights have a secondary (backup) power source? Yes/ No*

- ✓ Communications

Q71). *Do all guards have communication devices (radios/phones)? Yes/ No*

Q72). *Do facility guard/employees share radio frequencies with law enforcement? Yes/No*

Q73). *Do radios and phones have an emergency backup power source? Yes/ No*

Q74). *Does each active facility access point provide a means of contacting police, security control, or an emergency operations centre? Yes /No*

Q75a*). Does facility hold periodic port security meetings?*

Q75b). If yes, who are the participants?

Q75c). How many times do they meet?