Talas, R., and Menachof, D (2014). "Using Portfolio Optimization To Calculate The Efficient Relationship Between Maritime Port Security Residual Risk And Security Investment", *International Journal of Shipping and Transport Logistics*, Vol. 6 No. 3, pp. 314-338

USING PORTFOLIO OPTIMIZATION TO CALCULATE THE EFFICIENT RELATIONSHIP BETWEEN MARITIME PORT SECURITY RESIDUAL RISK AND SECURITY INVESTMENT

Dr Risto Talas, ESRC Research Fellow, University of Hull Logistics Institute (R.Talas@hull.ac.uk)*
Professor David Menachof, Peter Thompson Chair of Port Logistics, University of Hull Logistics Institute (D.Menachof@hull.ac.uk)
**corresponding author*

ABSTRACT

The research employs an adaptive cross-disciplinary research strategy in an industrial example to address port facilities' inability to assess whether their security systems are efficient. The research uses portfolio optimization to construct the optimum theoretical portfolio of security systems drawn from six different container port facilities owned by a major ports company. The research builds on the existing literature and proposes new definitions of security, port security, port security risk and port security risk management. The contribution which the research makes is in terms of modelling and measurement of the impact of the introduction of new port security technology, changes in background port security threat levels and for the planning of port security in Greenfield sites. Furthermore, the research is generalisable to all nodes in the supply chain and is not limited to port facilities alone.

Keywords

Security; port security; port security risk; port security risk management; terrorism; efficient frontier; portfolio analysis; ISPS Code; port facility security officer; company security officer; benefit-cost analysis; residual security risk; expected loss.

INTRODUCTION

The International Maritime Organisation's International Ship and Port Facility Security (ISPS) Code was introduced in the wake of the 11 September 2001 (9/11) terrorist attacks (Bichou, 2004; Price, 2004). This has resulted in significant investment in security systems by companies in the supply chain (Bichou, 2004; Farrow & Shapiro, 2009) and in port facilities in particular (Dekker & Stevens, 2007). According to Sheffi (2001), companies in the supply chain must determine how to balance the costs and benefits of security needs and how to do so in the most efficient manner. The purpose of the research is to discover the efficient relationship between residual security risk and security investment for maritime port facilities. No new theory is generated but the research undergoes an adaptive cross-disciplinary research approach to assess whether the six port facilities in the study have efficiently allocated their resources to tackle the threats of terrorism. The research is generalizable to all nodes in the supply chain and is not limited to maritime port facilities.

LIERATURE REVIEW

Port Security

In trying to arrive at a definition of port security it is suitable to begin with some origins of the term 'security' from the social science literature. The definition of security is then considered in the context of the supply chain security literature and is subsequently refined in order to arrive at a suitable definition of port security. Maslow (1942) describes security as a "feeling of safety; rare

feelings of threat or danger". Maslow (1942) includes security as a basic human need, together with safety, in his hierarchy of needs model. Baldwin (2005) defines security as 'the absence of threat' and Buzan (1991, p19) includes such definitions as 'relative freedom from harmful threats' and 'absence of threats to acquired values'. Williams et al (2008, p258) describe how the origin of security stems from individual level theories in sociology and psychology. Fischer and Green (2004, p21) state that security "implies a stable, relatively predictable environment in which an individual or group may pursue its ends without disruption or harm and without fear or disturbance or inquiry." Robinson's (2008, p188) definition of security is that it "implies freedom from threat" and "one's desire not merely to be free from threat but to feel free."

Combining Maslow (1942), Baldwin (2005), Buzan (1991) and Robinson (2008), security can be defined as the absence of and/or the perception of the absence of threat. Thus an individual who is surrounded by threats but has taken steps to reduce the threats may feel secure. Conversely, an individual who does not feel secure but who is not surrounded by any threats is in effect secure. This concept is important because different individuals (with the appropriate security knowledge and experience) when questioned about the security of a port facility, may have differing views in terms of their own perceptions as to both the threats that the port facility faces and how effectively existing security measures address the threats.

Here it is also important to distinguish between security and security measures: security measures are the measures (personnel, procedures and technology) required to achieve the absence of and/or the perception of the absence of threat. Given that ports are considered to be nodes in a supply chain network (Yap & Lam, 2004), it is necessary when developing the definition of port security to examine the literature on supply chain security (SCS).

Williams et al (2008, p256) state that few formal definitions can be found in the literature and draw their definition of SCS from Closs and McGarrell's (2004, p8) definition of SCS management: "the application of policies, procedures and technology to protect supply chain assets (product, facilities, equipment, information and personnel) from theft, damage, or terrorism and to prevent the introduction of unauthorised contraband, people or weapons of mass destruction (WMD) into the supply chain." Speier et al (2011) update the original Closs and McGarrell (2004) definition by describing SCS as entailing "the prevention of contamination, damage, or destruction of products and/or supply chain assets, and includes an acknowledgement that these events may occur from intentional and intentional disruptions."

Nevertheless, in pursuit of a definition of port security it would be easy simply to substitute 'port' for 'supply chain' in the original Closs and McGarrell (2004) definition. However, this would not distinguish between port security and port security management, in the way that Williams et at (2008) do not distinguish between SCS and SCS management. Furthermore, this would limit the definition simply to the port's assets and exclude cargoes and, specifically, the ship-port interface which the ISPS Code seeks to protect. Also, the Closs and McGarrell (2004) definition is in some ways too specific in its reference to terrorism and weapons of mass destruction given that by naming threats they run the risk of excluding others such as sabotage or criminal damage arising from strikes and riots by locked out workers (see Miller, 1994, p452 for a fuller description of named threats to ports covered by marine insurance). The ISPS Code does not single out terrorism as a threat per se but refers to measures which provide protection from security incidents (which include terrorism), while the US Maritime Transportation Security Act (MTSA) refers specifically to the threat of terrorism in the maritime domain. This is understandable given that the MTSA was drafted in the United States in the wake of the attacks on 9/11. However, the MTSA focus on terrorism also

potentially excludes other forms of unauthorised acts such as maritime fraud, which is included in Regulation (EC) No. 725/2004. Furthermore, the focus on WMD appears to be centred more on the United States, specifically in consideration of containerised trade (Harrald et al, 2004; Gerencser et al, 2003). Therefore, it would be appropriate to amend the named threats in the Closs and McGarrell (2004) definition to 'unauthorised acts', which is wider in scope. 'Unauthorised acts' is chosen in preference to 'illegal acts' in order to avoid any confusion arising from differing definitions of legality between jurisdictions.

The proposed definition for port security is: the absence of and/or the perception of the absence of threat to port facility assets, cargoes and the ship-port interface from unauthorised acts. From this, it follows that port security management is: the application of measures (personnel, procedures and technology) to reduce the threat and/or the perception of threat to port facility assets, cargoes and the ship-port interface from unauthorised acts. The choice of words is significant for while it may be preferable to try to eliminate threats rather than to reduce them, it will never be possible to eliminate all security threats absolutely (Price, 2004, p335).

Port security risk

As risk is present in all walks of daily life, it is logical that an extensive literature exists on the subject. Whether considering individuals' attitudes to risk and decision making under uncertainty (Kahnemann and Tversky, 1979), or risk as a factor in decision making (March and Shapira, 1987), the interpretation of risk varies from person to person. Definitions of risk also vary according to the discipline in which the discussion is framed, be it operations management (Lewis, 2003); supply chain (Speier et al, 2011; Rao and Goldsby, 2009; Kleindorfer and Saad, 2005; Christopher, 2005; Juttner et al, 2003; Zsidisin et al, 2004; Chopra and Sodhi, 2004), supply chain security (Williams et al, 2008), port security (Bichou, 2004, 2009; Talas and Menachof, 2009), terrorism (Sheffi, 2001; Woo, 2003; Raymond, 2006; Price, 2004, Willis et al, 2005; Greenberg et al, 2006), sociology and psychology (Heimer, 1988) or more established disciplines such as economics, finance or management (Juttner et al, 2003). Rao and Goldsby (2009) present selected definitions of risk from the literature including from Lowrance (1980) "risk is a measure of the probability and severity of adverse effects" and Yates and Stone (1992) "risk is an inherently subjective construct that deals with the possibility of loss."

Definitions of risk relevant to this study can be found in Robinson (2008), March and Shapira (1987), Bedford and Cooke (2001), Markowitz (1952), Broder (2006), Greenberg et al (2006), Price (2004) and Willis et al (2005). Robinson (2008, p182) describes risk from a security perspective as "the probability that harm may result from a given threat." March and Shapira (1987, p1404) review managerial perspectives on risk and risk taking and define risk as "reflecting variation in the distribution of possible outcomes, their likelihoods and their subjective values." Bedford and Cooke's (1996) analysis of probabilistic risk analysis describes risk as having two particular elements: hazard and uncertainty. Markowitz (1952, p89) describes risk as "variance of return." Kleindorfer and Saad's (2005, p55) second principle of risk management is "an extension of portfolio theory in finance, where a fundamental result is that portfolio diversification reduces the investor's risk." Broder (2006, p3) describes risk as "the uncertainty of financial loss, the variations between actual and expected results or the probability that a loss has occurred or will occur." Greenberg et al (2006, p143) state that terrorism risk "does not exist without existence of threat, the presence of vulnerability and the potential for consequences." Price (2004, p335) claims that ports (in the context of terrorism) are actually faced with uncertainty, not risk because uncertainty implies that while the range of events is known, the associated probabilities of each type of event are not. To an insurance underwriter, risk can represent not only the vessel, aircraft or property under consideration for insurance (Broder, 2006,

p3) but also the product of the probability of the occurrence of an insured event and the financial consequences of such an event. Willis et al (2005) describe terrorism risk as consisting of the product of threat, vulnerability and consequence: where threat is the probability that an attack occurs; vulnerability is the probability that an attack results in damage, given that an attack has occurred; and consequence is the expected damage, given that an attack has occurred which resulted in damage. Drawing on this definition and the definitions by Robinson (2008), Broder (2006) and Bedford and Cooke (2001), the proposed definition for port security risk is: the product of the probability of a threat to port facility assets, cargoes and the ship-port interface which may give rise to a loss and the size of the financial consequences that might follow.

Port security threats

The security threats that ports face include but are not limited to acts of terrorism. While the focus on terrorism appears to be uppermost in the literature, there are limited references to such attacks being directed at port facilities. Examples found in the literature include the incident in April 1996 when the Tamil Tigers launched an attack on the port of Colombo and succeeded in damaging three vessels (Aryasinha, 2001), including one belonging to the Van Ommeren shipping line which was insured by the author; in 2004 Jamaat al-Tawhid attacked the Khawr Al Amaya and Al Basrah oil facilities in Iraq; and in the same year suicide bombers from Hamas and the al-Aqsa Martyr's Brigade launched an attack in the Port of Ashdod (Greenberg et al, 2006).

Prior to 9/11 the main security threats to ports were considered to be from drug smuggling and organised crime. These resulted in the creation in the United States of the Business Anti-Smuggling Coalition (BASC), which has now been superceded by the Business Alliance for Secured Commerce, a security initiative initially aimed at reducing the risk of legitimate cargo being used by illegal organizations for the narcotics trade (Gutierrez et al, 2007). Nevertheless, the potential for terrorist attacks to disrupt ports and supply chains dominates the literature post-9/11. According to Raymond (2006, p242) ports are vulnerable to attack by terrorists: they are extensive in size and accessible by water and land. Furthermore, their accessibility impedes the deployment of the types of security measures that, for example, can be more readily deployed at airports. Bichou (2004) highlights the additional security threats that ports face due to their "close spatial interactions with large city-agglomerations and seashore tourist attractions." According to Nincic (2005, p623), the Sri Lankan Liberation Tigers of Tamil Eelam (LTTE), Hizballah, the Popular Front for the Liberation of Palestine, the Abu Sayyaf Group, Gama al-Islamiya, the Moro Islamic Liberation Front and the IRA are all believed to have varying levels of maritime expertise. According to Raymond (2006, p240), the terrorist groups that are known to have a maritime capability include "Polisario, the Abu Sayyaf Group, Palestinian groups, Al Qaeda, the Moro Islamic Liberation Front and the Liberation Tigers of Tamil Eelam." However, Raymond (2006, p244) points out that "in order to be considered a threat, it is not necessary for a terrorist group to have already carried out a maritime terrorist attack against shipping or port facilities."

Overview of the ISPS Code

The ISPS Code was drawn up by the IMO's Maritime Safety Committee and its Maritime Security Working Group in little over a year following the adoption of resolution A.924(22) on the review of measures and procedures to prevent acts of terrorism which threaten the security of passengers and crews and the safety of ships, in November 2001 (ISPS Code, 2003, p iii.) The ISPS Code was adopted on 12 December 2002 by the Conference of Contracting Governments to the International Convention for the Safety of Life at Sea (SOLAS) 1974 when the existing chapter XI

was amended and re-identified as chapter XI-1 and a new chapter XI-2 was adopted on special measures to enhance maritime security. Amendments were also made to the existing SOLAS chapter V.

The ISPS Code is divided into two parts. Part A establishes the new international framework of measures to enhance maritime security by introducing mandatory provisions while part B provides non-compulsory guidance on the procedures to be undertaken in order to comply with the provisions of chapter XI-2 and of Part A of the ISPS Code (Bichou, 2004.) Certain countries, such as the European Union under EC Regulation 725/2004, have made compliance with part B of the ISPS Code mandatory through legislation (Dekker & Stevens, 2007; Anyanova, 2007).

The objectives of the ISPS Code are to enable the prevention and detection of security threats within an international framework; to establish roles and responsibilities; to enable the collection and exchange of security information; to provide a methodology for assessing security and to ensure that adequate security measures are in place. The objectives are to be achieved by the designation of appropriate personnel on each ship, in each port facility and in each shipping company, to prepare and to put into effect the approved security plans. The ISPS Code is applicable to vessels engaged in international trade including passenger vessels with 12 or more berths, cargo vessels of 500 gross tonnes and over, mobile offshore drilling units and all port facilities serving such vessels engaged in international trade.

Costs of ISPS Code Implementation

Estimates of the costs of the implementation of the ISPS Code can be found in Bichou (2004), Bichou and Evans (2007), OECD (2003), Dekker and Stevens (2007) and Benamara and Asariotis (2007). According to Bichou (2004), the US Coast Guard (USCG) estimated the cost implications of security compliance on US ports to be $1.1 billion for the first year and $656 million each year up to 2012. The OECD (2003) report estimated that more than $2 billion was required as an initial investment with 1$ billion annual expenditure for developing country ports alone. Bichou and Evans (2007) report that in the UK, total initial costs for ISPS Code compliance for 430 port facilities was US$26 million with annual costs at US$2.5 million. Dekker and Stevens (2007) carried out a survey of port facilities' security investments in EU Member States and EEA countries. The authors found that the average security investment per port facility was €464,000 and the average annual running cost was €234,000. Benamara and Asariotis (2007) present the findings of the UNCTAD (2007) report which surveyed 55 ports in 28 countries. They found that the average initial cost per ISPS port facility for ports with up to 10 port facilities was US$386,000 with annual costs of US$128,000.

Port Security Incident Costs

Greenberg et al (2006) describe how the economic consequences of a successful terrorist attack are likely to be large and widespread and that economic consequences of attacks on the container shipping system would have direct and indirect effects. The authors describe the direct effects as life and injury compensation, repair and replacement of port infrastructure and other public property, losses of cargo and damaged and destroyed private property. The indirect effects are a consequence of the role of the port in the supply chain: business interruption due to delayed or missing shipments, long term adjustments to the modified transport system, augmented security procedures and lost revenue to the port facility and to the public purse.

The OECD report (2003, p.19) describes how, after the attack on the tanker Limburg off Aden in November 2002, Yemeni terminals saw container throughput plummet from 43,000 TEU in

September 2002 to 3,000 TEU in November 2002. This resulted largely from marine war underwriters' increased war additional premiums rising to as much as USD 300,000 per vessel call. The Yemeni government estimated that 3,000 workers were laid off and economic losses arising from the attack were running at USD 15,000,000 per month. The OECD Report (2003, p.20) also states that property damage from a terrorist attack to a modern 16 hectare container terminal could be as much as USD 32,000,000. In a wider view, Farrow and Shapiro (2009) review the literature on the cost of potential terrorist attacks in the United States. They present estimates for the overall costs of various attack scenarios, some of which are based in ports.

Benefit Cost Analysis in Security

Farrow and Shapiro (2009) summarize a benefit-cost framework for investing in security. They also refer to a model developed by 'Risk Management Solutions', a private company, for insurance companies to use to estimate the risk of terrorist attacks. Willis and LaTourette (2008) describe a probabilistic risk modelling approach in break-even benefit-cost analysis which employs the Risk Management Solutions methodology. They describe terrorism risk in terms of the annual expected loss from damage caused by terrorist attacks where the expected loss combines the probability that the attack will occur and the consequence of the attacks. The authors also state that the benefit of a security regulation can be expressed in terms of the reduction in the expected loss of damage and that a regulation is justified if the incremental cost of implementing the regulation is exceeded by the incremental benefit generated by the regulation. Pinto and Talley (2006) propose a framework for calculating the risk-based return on investment (RROI) for a port's security systems based on the framework developed by Arora et al (2004, p35) which "uses a risk management approach that integrates risk profile with actual damages and implementation costs to determine the costs and benefits of information security solutions." On a wider scale, Chopra and Sodhi (2004) describe the challenges that companies face to mitigate supply chain risks without eroding profits. The manager's role is similar to that of a stock portfolio manager: achieve the highest possible profits for varying levels of risk, and do so efficiently.

RESEARCH METHODOLOGY

The research is set in an industry example and follows a cross-disciplinary research approach. The objective behind the research is not the generation of new theory about port security efficiency but is aimed at addressing some of the problems faced by port security managers today through the cross-disciplinary application of portfolio optimization in the field of port security. The research follows a mixed methods approach of survey questionnaires and structured interviews to collect largely qualitative data about the performance of the port facilities' security systems and the risks that they face. However, in this research the risks are limited strictly to terrorism owing to the limitations of the data available.

Epistemological and Ontological Considerations

The epistemology in this research is interpretivist-phenomenological (Bryman, 2004) given the researcher's role to see the World View of the company security officers and to interpret it from their perspective. Furthermore, as much of the data on the performance of port security systems is subjective in nature and cannot be easily measured with any physical gauge, and nor can the

perception of security be discerned by the 'effect' of the security measures alone, then the research can follow neither a positivist nor a realist epistemology. The nature of port security also guides the ontological considerations. Given that the perceptions of security threats are an interpretation of social phenomena and thus necessarily dependent on social actors, the ontology is therefore constructionist (Bryman, 2004).

Research Question

The main research question is: how can the efficient relationship between residual security risk and security investment be calculated for an ISPS Code compliant port facility. Assuming that the port facilities in question are ISPS Code compliant, the calculation of the relationship between residual security risk and security investment requires the posing of a further five questions, as set out below.

1. What are the security threats to the port facility and what are their probabilities?

The research concentrates on seven different types of security incident selected from examples in Pinto and Talley (2006), Parfomak and Fritelli (2007) and from discussions with an international ports company. The types of security incident are: bomb introduced by person on foot; car bomb; truck bomb; biological agent attack on the port facility – on foot; biological agent attack on the port facility – by vehicle; mining of port infrastructure; and vessel attacked by suicide boat. The security scenarios for each port facility were presented to a Lloyd's terrorism underwriter for his pure premium rating in an interview at his desk in the underwriting room in Lloyd's of London. Bigün (1995) relies on expert judgements in her empirical study of risk analysis of major civil aircraft accidents to predict future risks. The methodology which the underwriter applies for pricing a terrorism risk in a given country is as follows. He refers to his "notional base rate" for a terrorism risk. He then examines the Exclusive Analysis risk score for terrorism for the country in question which is represented as a number between 1 and 10 to one decimal place. This scale he has interpreted as a logarithmic scale of base 2. In order to arrive at his country rate for a particular terrorism risk he multiplies his base rate by 2 to the power of the Exclusive Analysis risk score minus 1. He then makes a further subjective adjustment depending on the nature of the business of the proposed assured. The underwriter's methodology subsequently yields a single country rate for a terrorism risk in a specific business sector. However, his methodology is unable to distinguish between two different locations in the same country and nor will it distinguish between different types of terrorism attack modus operandi. While authors such as Bier et al (1999) and Lambert et al (1994) question the ability to forecast low probability, high impact events where there is a lack of empirical evidence; and Lichtenstein et al (1978) point to the biases that affect individuals' tendency to overestimate low probabilities of fatal events, in this research the underwriter in question is using a combination of empirical data and expert knowledge in his subjective assessments.

2. What are the estimated gross losses to the port facility following each prescribed security threat? The data source for the estimates of potential economic damage to the port facilities following the prescribed security incidents listed above was obtained from the schedule of insurances of the facilities owned by global ports company.

3. What do the security systems consist of in each port facility? The security systems have been classified as access control, biometrics and detection, which in turn consist of individual security components. The access control systems include all the physical gates, fencing and security personnel engaged in access control procedures. The biometric systems, also described as 'enhanced access

control systems' range from pass cards to fingerprint scanning. The detection systems include CCTV systems, automatic intruder alerts, radar, sonar and also the security personnel involved in security patrols. The security components in the port facility were identified through the use of a survey questionnaire completed by each of the port facilities' Port Facility Security Officer (PFSO). The questionnaire was compiled following a line-by-line analysis of the port security equipment and components mandated by the ISPS Code. The data sources for the completed survey questionnaires are the Port Facility Security Officers in the six port facilities.

4. How well do the port security systems perform in the face of the prescribed security threats?

The performance of the individual security systems can be assessed based on a series of key performance indicators (KPIs) that the port facility security officers (PFSOs) report monthly to the company security officers (CSOs). They report, among other measures, the number of security non-conformities for each security system. This means that the CSOs are able to build a picture over time of how effectively the security systems are operating in the port facilities for which they have responsibility. In a series of semi-structured interviews conducted with the CSOs, they were asked to interpret and translate the KPI data into percentage performance measures for each of the three main security systems: access control, biometrics and detection for each of the port facilities.

5. What are the port security systems' costs?

The survey questionnaire also captured details of the investment of each port facility's security systems and their components. The data captured includes both the cost of the security infrastructure from 2004 to 2007 and the running costs of the port facility's security systems for the 2007 year. The term 'security investment' in this research combines both the cost of the security infrastructure from 2004 to 2007 and the running costs for the 2007 year.

Constructing the Port Security Risk Model

The port security risk model is based on Willis et al (2005).

Willis et al (2005) describe terrorist risk as "the expected consequence of an existent threat, which, for a given target, attack mode and damage type can be expressed as:

Risk = P (attack occurs) * P (attack results in damage | attack occurs) * E (damage | attack occurs and results in damage) = Threat * Vulnerability * Consequence"

Willis et al (2005) also state that if terrorist risks are independent, expected damages of a specific type can be aggregated by summing across threat types and target types. If l_j is the loss (consequence) from an attack type j and the probability of the occurrence of l_j is $p(l_j)$ and the vulnerability of the port facility from l_j is defined as $1-p(s_{ij})$ where s_{ij} is the ability of security system i to prevent l_j, then it follows that the aggregate port security risk is $\sum_{i=1}^{n}\sum_{j=1}^{m} p(l_j)\times(1-p(s_{ij}))\times l_j$ (1)

for n security systems against m different types of security incident.

RESEARCH FINDINGS

Table 1 contains the estimates of physical damage, business interruption and the expected gross loss (in US dollars) to the six port facilities in the research following the seven prescribed security incidents. The table includes the company security officer's assessment of expected loss and the underwriter's assessment of the probability of the occurrence of each prescribed security incident. The expected loss of each security incident is calculated as the product of the sum of the physical damage and business interruption amounts and the probability of occurrence.

Table 2 shows the company security officers' subjective assessment of the performance of the port facilities' security. The best performing port facility for access control is port facility B with a mean of 76.43% and with a standard deviation (s.d.) of 18.42% followed closely by port facility A with mean of 72.86% and s.d. of 15.77% respectively. However, port facility B's access control system cost $715,000 whereas port facility A's is only $187,826. The worst performing access control system belongs to port facility D with a mean of 22.86% and a s.d. of 7.56%.

In terms of biometrics, port facility F was the best performing with a mean of 67.86% and a s.d. of 46.36% followed closely by both port facility C (mean 66.43% & s.d. of 45.43%) and port facility B (mean 65.71% and s.d. of 45.04%). However, the cost of the biometrics systems varies considerably. The worst performing port facility for biometrics was port facility D with a mean of 34.29% and a s.d. of 15.12%.

In terms of detection, port facility B was the best performing with a mean of 87.86% and a s.d. of 7.56%. The detection systems in port facility E were worst with a mean of only 10.00% and a s.d. of 19.15%. What is of interest is the size of the difference in the performance of the detection systems in port facility F where the mean is 41.43% and the s.d. is 40.18% compared to port facility B given that the size of the investment in both port facilities' detection systems are quite similar.

Estimates of Physical Damage (PD), Business Interruption (BI) and Gross Expected Loss

Port Facility		Bomb introduced by person on foot	Car Bomb	Truck bomb	Biological agent attack on terminal - on foot	Biological agent attack on terminal - by vehicle	Mining of port infrastructure	Vessel attacked by a suicide boat	Total	Probability	Expected Loss
A	PD	5,375,000	36,769,695	125,012,575	16,902,973	87,432,657	56,000,000	113,242,880	440,735,780	0.522%	2,300,641
	BI	10,000,000	45,000,000	92,122,118	102,122,118	122,122,118	92,122,118	122,122,118	585,610,590	0.522%	3,056,887
	Total	15,375,000	81,769,695	217,134,693	119,025,091	209,554,775	148,122,118	235,364,998	1,026,346,370		5,357,528
B	PD	5,375,000	36,769,695	125,012,575	11,744,695	92,472,157	113,242,880	113,242,880	497,859,882	0.0152%	75,675
	BI	10,000,000	45,000,000	92,122,118	97,122,118	132,122,118	92,122,118	92,122,118	560,610,590	0.0152%	85,213
	Total	15,375,000	81,769,695	217,134,693	108,866,813	224,594,275	205,364,998	205,364,998	1,058,470,472		160,888
C	PD	5,375,000	36,769,695	176,226,244	11,744,695	124,126,575	164,456,549	164,456,549	683,155,306	0.018%	122,968
	BI	10,000,000	45,000,000	92,122,118	97,122,118	132,122,118	92,122,118	92,122,118	560,610,590	0.018%	100,910
	Total	15,375,000	81,769,695	268,348,362	108,866,813	256,248,693	256,578,667	256,578,667	1,243,765,896		223,878
D	PD	5,375,000	36,769,695	133,092,200	11,744,695	94,032,032	121,322,505	121,322,505	523,658,633	0.070%	366,561
	BI	10,000,000	45,000,000	92,122,118	97,122,118	132,122,118	92,122,118	92,122,118	560,610,590	0.070%	392,427
	Total	15,375,000	81,769,695	225,214,318	108,866,813	226,154,150	213,444,623	213,444,623	1,084,269,223		758,988
E	PD	5,375,000	36,769,695	211,302,016	11,744,695	163,548,848	199,532,321	199,532,321	827,804,897	0.030%	248,341
	BI	10,000,000	45,000,000	92,122,118	97,122,118	132,122,118	92,122,118	92,122,118	560,610,590	0.030%	168,183
	Total	15,375,000	81,769,695	303,424,134	108,866,813	295,670,966	291,654,439	291,654,439	1,388,415,487		416,525
F	PD	5,375,000	36,769,695	157,352,430	11,744,695	109,599,262	145,582,735	145,582,735	612,006,553	0.023%	140,762
	BI	10,000,000	45,000,000	92,122,118	97,122,118	132,122,118	92,122,118	92,122,118	560,610,590	0.023%	128,940
	Total	15,375,000	81,769,695	249,474,548	108,866,813	241,721,380	237,704,853	237,704,853	1,172,617,143		269,702

Table 1: Estimates of physical damage (PD), business interruption (BI) and gross expected loss.

Port Facilities' Security Systems' Performances										
Port Facility	Security System	Bomb introduced by person on foot	Car Bomb	Truck bomb	Biological agent attack on terminal - on foot	Biological agent attack on terminal - by vehicle	Mining of port infrastructure	Vessel attacked by a suicide boat	Mean	Standard Deviation
A	Access Control	80%	80%	85%	80%	85%	50%	50%	72.86%	15.77%
	Biometrics	90%	90%	85%	90%	90%	0%	0%	63.57%	43.47%
	Detection	75%	75%	80%	75%	75%	50%	50%	68.57%	12.82%
B	Access Control	90%	90%	80%	90%	85%	50%	50%	76.43%	18.42%
	Biometrics	95%	95%	85%	95%	90%	0%	0%	65.71%	45.04%
	Detection	95%	95%	80%	95%	90%	80%	80%	87.86%	7.56%
C	Access Control	80%	85%	85%	80%	85%	0%	0%	59.29%	40.56%
	Biometrics	90%	95%	95%	90%	95%	0%	0%	66.43%	45.43%
	Detection	70%	75%	70%	70%	75%	0%	0%	51.43%	35.20%
D	Access Control	20%	20%	20%	20%	20%	20%	40%	22.86%	7.56%
	Biometrics	40%	40%	40%	40%	40%	40%	0%	34.29%	15.12%
	Detection	40%	0%	0%	40%	0%	40%	20%	20.00%	20.00%
E	Access Control	60%	90%	90%	60%	90%	10%	10%	58.57%	35.79%
	Biometrics	80%	80%	80%	80%	80%	0%	0%	57.14%	39.04%
	Detection	0%	0%	0%	0%	0%	50%	20%	10.00%	19.15%
F	Access Control	90%	90%	90%	10%	10%	0%	30%	45.71%	42.37%
	Biometrics	95%	95%	95%	95%	95%	0%	0%	67.86%	46.36%
	Detection	80%	0%	0%	80%	0%	80%	50%	41.43%	40.18%

Table 2: Port facilities' security systems' performances

Residual Risk and Security Cost Calculations

Table 3 shows the calculation of the port facilities' residual risks following the application of the three types of security systems and includes the costs of the security systems in US dollars. These are important results in the research because for each of the port facilities A to F, there exists a calculation of the residual risk for each of the three security systems and an accompanying security investment. These combinations of performance in reducing residual risk and security investment are key to the portfolio optimization exercise below.

Port Facility		**Access Control**	**Biometrics**	**Detection**	**Total**
A	RR	520,227	798,016	594,387	1,912,629
	SC	187,826	33,637	261,999	483,462
B	RR	15,356	24,120	8,022	47,499
	SC	715,000	8,000	2,756,325	3,479,325
C	RR	37,738	33,354	42,926	114,018
	SC	412,734	2,680	51,538	466,952
D	RR	192,436	171,719	211,518	575,673
	SC	829,730	12,200	787,670	1,629,600
E	RR	64,276	74,433	118,426	257,135
	SC	207,000	84,000	453,000	744,000
F	RR	57,829	39,121	58,589	155,539
	SC	1,324,312	275,600	349,777	1,949,689

Table 3: Port facilities' residual risk and security cost calculations

Port Security Benefit-Cost Ratios

The findings also showed some interesting results concerning the port facilities' security benefit-cost ratios which show by how much each port facility's residual security risk is reduced for every $1 spent on security. While most of the ratios range from 0.0325 for port facility B to 0.235 for port facility C, the corresponding figure for port facility A is 7.13. It is possible that the size of this figure may reflect the higher level of terrorist threat that exists in that country. However, the figure for Port facility D is lower than for Port facility C where the terrorist threat is lower so it would be premature to try to draw such a conclusion. The figures for the security benefit-cost ratios are shown in table 4.

Port Facility	Security Performance Ratio
A	7.125
B	0.033
C	0.235
D	0.112
E	0.214
F	0.032

Table 4 – port security benefit-cost ratios

Residual Risk / Expected Loss Ratios

An analysis of the ratios for residual risk : expected loss per type of prescribed security incident show which of the port facilities are best placed to prevent such an attack. These are shown in table 5.

Port Facility	Bomb introduced by person on foot	Car Bomb	Truck bomb	Biological agent attack on terminal - on foot	Biological agent attack on terminal - by vehicle	Mining of port infrastructure	Vessel attacked by a suicide boat
A	18.30%	18.30%	16.70%	18.30%	16.70%	66.70%	66.70%
B	6.70%	6.70%	18.30%	6.70%	11.70%	56.70%	56.70%
C	20.00%	15.00%	16.70%	20.00%	15.00%	100.00%	100.00%
D	66.70%	80.00%	80.00%	66.70%	80.00%	66.70%	80.00%
E	53.30%	43.30%	43.30%	53.30%	43.30%	80.00%	90.00%
F	11.70%	38.30%	38.30%	38.30%	65.00%	73.30%	73.30%

Table 5: Port Facilities' Residual Risk : Expected Loss Ratios by per type of Security Incident

For the bomb introduced by person on foot, the best performing port facility is port facility B at 6.7% while the worst performing is port facility D at 66.7%. This means that for a given attempt on port facility B, only 6.7% are expected to be successful whereas in port facility D, two thirds of attempted attacks are expected to be successful. For the car bomb, port facility B again scores the highest with 6.7% and port facility D is again the worst performing with only a fifth of attempted attacks being thwarted. For the truck bomb scenario, it is port facility A and port facility C that perform equal best at 16.7% and port facility D is again the worst performer at 80%. In the case of the biological agent attack on the port facilities either by on foot or by vehicle, port facility B is again the best performing with port facility D the worst performing. However, for both the mining of the port infrastructure and the vessel attacked by a suicide boat, while port facility B is again the best performing, the worst performing being port facility C, which was judged to be unable to prevent any kind of attack from the water. This highlights that while port facility C is relatively good at preventing attacks that have their origins on the land, the port facility is very vulnerable to any waterborne threats.

PORTFOLIO OPTIMIZATION

The portfolio optimization resulted in an examination of all 216 (6^3) possible portfolios constructed from the 3 security systems in each of the 6 port facilities. The portfolios were analysed in terms of their security investment and their residual security risk. The 216 possible portfolios were then plotted on a figure and the figures are reproduced for each of the six port facilities (see appendix A figures 1 to 6 for port facilities A to F respectively). In the analysis, the possible portfolio combinations of the six port facilities' security systems which best result in both a reduction in residual security risk and security investment were selected and these are set out in tables 6 for port facilities A to F respectively, below.

Port Facility	Port Facility's Security System			Portfolio no.	Security Cost	Security Cost Reduction	Residual Risk	Residual Risk Reduction
	AC	BIO	DET					
A	A	C	A	13	452,505	30,957	1,849,503	63,136
B	A	C	B	14	2,946,831	532,494	46,638	861
	B	C	B	50	3,474,005	5,320	46,144	1,355
C	A	C	A	13	452,505	14,447	81,491	32,527
	A	C	C	15	242,044	224,908	98,869	15,149
D	B	F	A	67	1,252,599	377,001	265,836	309,837
	A	C	C	15	242,044	1,387,556	325,974	249,700
E	A	F	A	31	725,425	18,575	152,405	104,730
	A	C	C	15	242,044	501,956	185,847	71,288
F	B	F	A	67	1,252,599	697,090	96,160	59,379
	A	C	C	15	242,044	1,707,645	117,872	37,666

Table 6 - Optimal Security System Portfolios for the Port Facilities A to F

Port facility A has a security investment of $483,462 and a residual risk of $1,912,629. Following the portfolio analysis there exists only portfolio no.13 which results in both a reduced residual risk and a reduction in security investment. This can be achieved by maintaining the existing

access control (AC) and detection (DET) systems in port facility A but substituting the existing biometrics (BIO) system for the system used in port facility C.

Port facility B has a security investment of $3,479,325 and a residual risk of $47,499. The portfolio which minimises the residual risk is portfolio no.50, which consists of the access control and detection systems from port facility B and the biometrics system from port facility C. The portfolio which minimises the security investment is no.14 which consists of the access control system from port facility A, the biometrics system from port facility C and the detection system from port facility B.

Port facility C has a security investment of $466,952 and a residual risk of $114,018. The optimum portfolio for residual risk reduction is portfolio no.13, which represents the access control system from port facility A, the biometrics system from port facility C and the detection system from port facility A. The optimum portfolio for reduction in security investment is portfolio no.15, which represents the access control system from port facility A and both the biometrics and the detection system from port facility C.

Port facility D has a security investment of $1,629,600 and a residual risk of $575,673. The portfolio which provides the greatest reduction in residual security risk is portfolio no.67, which combines the access control system from port facility B, the biometrics system from port facility F and the detection system from port facility A. The portfolio which yields the greatest saving in security investment is portfolio no.15, which consists of the access control system from port facility A and the biometrics and detection systems from port facility C.

Port facility E has a security investment of $744,000 and a residual risk of $257,135. The optimum portfolio for reduction of residual risk is portfolio no.31 which consists of the access control system from port facility A, the biometrics system from port facility F and the detection system from port facility A. The optimum portfolio for reduction of security cost is portfolio no.15 which consists of the access control system from port facility A and both the biometrics and detection systems from port facility C.

Port facility F has a security investment of $1,949,689 and a residual risk of $155,539. The optimum portfolio for reduction of residual risk is portfolio no.67 which consists of the access control system from port facility B, the biometrics system from port facility F and the detection system from port facility A. As for port facility E above, the top performing portfolio for reduction in security investment is portfolio no.15 which consists of the access control system from port facility A and both the biometrics and detection systems from port facility C.

Results of the Portfolio Optimization

The portfolio optimization has produced some interesting results. The results are presented in two parts: first, the optimum and alternative portfolios which are most successful in reducing residual security risk; and secondly, the optimum and alternative portfolios which are most successful in reducing the security investment.

Reducing Residual Security Risk

The optimum portfolio for minimising the residual risk for both port facility A and port facility C is portfolio no.13, which consists of access control from port facility A, biometrics from port facility C and detection system from port facility A. The optimum portfolio for minimising the residual risk in both port facility D and port facility F is portfolio no.67, which consists of access control from port facility B, biometrics from port facility F and detection from port facility A. The optimum portfolios for minimising the residual risk in port facility B and port facility E are portfolio numbers 50 and 31 respectively.

Overall, the security systems which make up the optimum portfolios for the reduction of residual risk across all of the port facilities consist of the following (in various combinations):

- Access control from either port facility A or port facility B
- Biometrics from either port facility C or port facility F
- Detection from either port facility A or port facility B

Reducing Security Investment

The optimum portfolio for minimising the security investment for port facility C, port facility D, port facility E and port facility F is portfolio no.15, which consists of access control from port facility A and biometrics and detection from port facility C. It is particularly interesting that one optimum portfolio of security systems is so dominant in minimising security investment. The portfolio for minimising the security investment in port facility A is portfolio no.13; and the corresponding portfolio for port facility B is no.14, which consists of access control from port facility A, biometrics from port facility C and detection from port facility B. Overall, the security systems which make up the best performing portfolios for the reduction of security investment across all of the port facilities consist of the following (in various combinations):

- Access control from port facility A
- Biometrics from port facility C
- Detection from port facility A, port facility B or port facility C

Explanation for Clustering Effect

An explanation is offered for the clustering effect highlighted by the portfolio optimization. The clear division in the figures for the security investment between the two clusters makes the process relatively straightforward. The left hand cluster in figures 1 to 6 ends where the security investment is $2,387,582 (in portfolio no. 14) and the right hand cluster begins where the security investment is $2,946,811 (in portfolio #214). An examination of the portfolios where the security investment is $2,946,811 or greater yielded one common denominator: the inclusion in every alternative portfolio in the right hand cluster of the detection system from port facility B. However, in order to be able to prove conclusively that this security system is responsible for the clustering, an analysis was conducted of the other 180 alternative portfolios and none were found to contain the same security system. It is therefore shown that the clustering effect is entirely down to the inclusion in the alternative portfolios of the detection system from port facility B.

DISCUSSION

The nature of the research enables direct comparisons to be made between the security systems in the port facilities. Tables 2 and 3 allow for the comparison between the port facilities as to how the security systems perform, how they reduce risk and their costs. This is useful for a CSO to understand better where the strengths and weaknesses in the port facilities' security systems lie. The benefit-cost ratios in table 4 enable a CSO to compare how much the residual risk is reduced in the port facilities given the security investment across different port facilities. This ratio can be used to model by how much the residual risk might reduce given the introduction of new technology. The residual risk : expected loss ratios in table 5 allow a comparison of how well the port facilities' overall

security systems perform in the face of the prescribed security threats. It is from this table that a CSO can draw some conclusions regarding how secure the port facilities are: the lower the ratio, the higher the level of security.

The portfolio optimization exercise highlighted two key elements. First, the efficient relationship between port security residual risk and security investment as described in figures 1 to 6 for port facilities A to F respectively in appendix A: the points closest to the x- and y-axes describe the efficient frontier. Secondly, for each actual port security portfolio, alternative portfolios were discovered which both reduced cost and residual risk. This was done by selecting better performing security systems from the other port facilities and combining them in theoretical portfolios, in much the way that one might construct a fantasy football team. The resulting reductions in security investment and residual risk were calculated and shown in tables 6 to 11.

Linking the results to the literature

The figures for security investment for port facilities A, C and E are comparable with the average security investments in Dekker and Stevens (2007) and Benamara and Asariotis (2007). The figures for the security incident costs provided by the CSO are also comparable with the OECD (2003) report. The security benefit-cost ratios in table 4 show that the Willis and LaTourette (2008) principle of a justified security regulation is upheld only in the case of port facility A where $1 of investment in security results in a $7.13 reduction in residual security risk. In the other five cases, the security performance ratios are well below 1 and in the case of Port facility B it is particularly low at 0.0325. This suggests that the ISPS Code would not qualify as a justified regulation in the sense that Willis and LaTourette (2008) intended.

Contribution

The contribution of the research is threefold. First, the methods can be employed in the development of Greenfield sites to guide a CSO to implement a security system which best suits his/her requirements in terms of both residual security risk and security investment and to do so efficiently. Secondly, the proposed introduction of new port security technology with an enhanced performance in an existing port facility can be modelled to learn the extent to which the residual security risk might be reduced, for a new given level of security investment. Thirdly, a change in the background security threat to a port facility can be quantified in terms of a change to the residual security risk. CSOs can use this information to help them decide on a possible course of action to address the change in threat.

Areas of Further Research

One area for further research would be to collect empirical data on the change in performance of a port facility's security systems through the introduction of new technology or working practices. Another area for further research would be the application of the theory in the selection of a new security system for a Greenfield site. Consideration could be given to wider environmental, network-related and organisational risk sources for future research of this nature (see Juttner et al, 2003, for a discussion of supply chain risk sources).

CONCLUSION

The research has focussed on the field of port security and was based on an industry example. The existing literature has been examined and new definitions of security, port security, port security risk and port security risk management have been proposed. Furthermore, a model of port security risk has been developed, based on Willis et al's (2005) definition of terrorist risk.

The main research question considered how ISPS Code compliant port facilities can discover the efficient relationship between residual security risk and security investment. In order to address the main research question, it was broken down into two further research questions which addressed what it means for a port facility to be ISPS Code compliant and how the efficient relationship between residual security risk and security investment can be calculated. The latter was tackled by means of asking a further five questions concerning security threats to port facilities; estimated gross losses to the port facilities following prescribed security threats; the security systems present in the port facilities; the performance of the security systems in the face of the prescribed security threats; and the security systems' costs. The research methodology employed mixed methods, which included survey questionnaires to assess the six port facilities' security systems and costs; structured interviews with two of the company security officers for their subjective evaluations of the performance of the security systems; and an interview with a Lloyd's Underwriter of terrorism risks.

The research has intentionally not produced any new theory about port security but has shown how company security officers can assess whether a port facility's security systems are efficient. The was achieved by using portfolio optimization to construct an optimum portfolio drawn from the security systems in the different port facilities in order to arrive at the best solution for risk reduction for that port facility, in much the same way as one might construct a 'fantasy baseball team' drawn from the best players in a baseball league. The portfolio optimization approach produced the efficient solution for the relationship between risk and security investment drawn from all 216 possible combinations of security system portfolios from among the three security systems (access control, biometrics and detection) across the six port facilities.

The results of the research are generalizable to any ISPS Code compliant port facility or to any other type of node in the supply chain, such as a warehouse or logistics park, which consists of similar security systems and follows a similar security regime as that described in the ISPS Code. Furthermore, the research has produced two new port security ratios: the residual risk reduction : security expenditure ratio; and the residual risk : expected loss ratio. These ratios can be of use to port security personnel and company security officers when evaluating their security systems. The research contribution also includes a roadmap for developing security systems for Greenfield sites based on knowledge of existing security systems and the modelling of changes in background security risk and the introduction of new technology.

Finally, there is scope to extend the research to include many more types of risk in order to build a more comprehensive model.

REFERENCES

Anyanova, E. 2007. The EC and Enhancing Ship and Port Facility Security, *Journal of International Commercial Law and Technology*, Vol 2, 1

Arora, A., Hall, D., Pinto, A., Ramsey, D. & Telang, R. 2004. Measuring the Risk-Based Value of IT Security Solutions, *IEEE IT Professional* 6: 35-42

Aryasinha, R. 2001. Terrorism, the LTTE and the conflict in Sri Lanka. *Conflict, Security and Development*, Vol. 1, No. 2, pp.25-50

Baldwin, D.A. 2005. The Concept of Security in Diehl, P.F. (ed.) War. vol. 1, pp. 1-24, London: Sage

Bedford T. & Cooke, R. 2001, Probabilistic Risk Analysis: Foundations and Methods. Cambridge University Press

Benamara H, Asariotis R. 2007. ISPS Code implementation in ports: costs and related financing. In Bichou K, Bell MGH, Evans A. (eds). 2007. Risk management in port operations, logistics and supply chain security. Informa, London

Bichou K. 2004. The ISPS Code and The Cost of Port facility Compliance: An Initial Logistics and Supply Chain Framework for Port Security Assessment and Management. *Journal of Maritime Economics & Logistics.* 6 322–348

Bichou K., Evans A. 2007. Maritime security and regulatory risk-based models: review and critical analysis. In Bichou K, Bell MGH, Evans A. (eds). 2007. Risk management in port operations, logistics and supply chain security. Informa, London

Bichou, K. 2009. Security and risk-based models in shipping and ports: review and critical analysis. In OECD/ITF Roundtable 144. Terrorism and international transport: towards risk-based security policy. OECD/ITF Transport Research Centre

Bier, V., Y. Haimes, J. Lambert, N. Matalas, and R. Zimmerman. 1999. A survey of approaches for assessing and managing the risk of extremes. *Risk Analysis* 19(1): 83–94

Bigün, E.S. 1995. Risk analysis of catastrophes using experts' judgements: An empirical study on risk analysis of major civil aircraft accidents in Europe. *European Journal of Operational Research*, Vol. 87 pp.599-612

Broder, J. 2006. Risk Analysis and the Security Survey. Boston, 3rd Edition

Bryman, A. 2004. Social Research Methods. Oxford, 2nd Edition

Buzan, Barry. 1991. People, states and fear: an agenda for international security studies in the post cold-war era. New York: Harvester Wheatsheaf

Chopra, S. & Sodhi, M.S. 2004. Managing Risk to Avoid Supply Chain Breakdown. *MIT Sloan Management Review*

Christopher, M. (2005) "Logistics and Supply Chain Management", 3rd Edition, FT Prentice Hall

Closs, D. & McGarrell, F. 2004. Enhancing Security Throughout the Supply Chain. *IBM Center for the Business of Government Special Report Series*, April 2004

Dekker S, Stevens H. 2007. Maritime security in the European Union – empirical findings on financial implications for port facilities. *Maritime Policy and Management,* 34 (5) 485-499

Farrow S, Shapiro S. 2009. The benefit-cost analysis of security focussed regulations. *Journal of Homeland Security and Emergency Management*, 6 (1) Article 25

Fischer, R. J. & Green, G. 2004. Introduction to security. 7th ed., Boston: Butterworth Heinemann

Gaonkar, R. & Viswanadham, N. 2004. A conceptual and analytical framework for the managing of risks in supply chains. *Proceedings of the 2004 IEEE International Conference on Robotics and Automation*, April 26-May 1, Vol. 3, pp2699-2704

Gerencser, M., Weinberg, J. & Vincent, D. 2003. Port Security War Game. Booz Allen Hamilton

Greenberg, M, Chalk, P, Willis, H, Khilko, I & Ortiz, D. 2006. Maritime Terrorism: Risk and Liability. RAND Corporation Centre for Terrorism and Risk Management Policy

Gutierrez, X., Hintsa, J., Wieser, P. & Hameri, A-P. 2007. Voluntary supply chain security impacts: an empirical study with BASC members companies. *World Customs Journal*, Vol. 1, No. 2, pp31-48

Harrald, J., Stevens, H.W. & vanDorp, J.R. 2004. A framework for sustainable port security. *Journal of Homeland Security and Emergency Management* , Vol. 1 (2): Article 12.

Heimer, C. 1988. Social structure, psychology and the estimation of risk. *Annual Review of Sociology*, 14:491-519

International Maritime Organisation. 2003. International Ship and Port Facility Security (ISPS) Code. IMO: London

Juttner U, Peck H, Christopher M. 2003. Supply chain risk management: outlining an agenda for future research. *International Journal of Logistics: Research and Applications* 6 (4) 199-213

Kahneman, D. and Tversky, A. 1979. Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, Vol. 47, No. 2, pp. 263-292.

Kleindorfer, P.K. and Saad, G.H. 2005. Managing Disruption Risks in Supply Chains. *Production and Operations Management*. Vol. 14, No. 1, pp. 53-68

Lambert, J., Matalas, N., Ling, C., Haimes, Y. and Li, D. 1994. Selection of probability distributions in characterizing risk of extreme events. *Risk Analysis* 14 (5): 731–742.

Lewis, B., Erera, A. & White III, C. (2007) "Optimization approaches for efficient container security operations at transhipment ports", *Journal of the Transportation Research Board*, Vol. 1822, pp 1-8

Lichtenstein, S. Slovic P., Fischhoff, B., Layman, M. and Combs, B. 1978. "Judged Frequency of Lethal Events," J. *Exp. Psychol.*: *Human Learn. Memory* 4, 551-578

Lowrance, W.W. (1980) "The nature of risk", in Schwing, R.C. and Albers, W.A. (Eds) *How Safe is Safe Enough?*, Plenum Press, New York

March, J.G. & Shapira, Z. 1987. Managerial Perspectives on Risk and Risk Taking. *Management Science*, Vol. 33, No. 11, pp. 1404-1418

Markowitz, H. 1952. Portfolio Selection. *The Journal of Finance*, Vol. 7, No. 1, pp77-91

Maslow, A.H. 1942. The Dynamics of Psychological Security-Insecurity. *Journal of Personality*, Vol. 10, Issue 4, pp. 331-334

Miller, M.D. (1994) “Marine War Risks”, *Lloyd’s of London Press Ltd*, 2nd Edition

OECD. 2003. Security in Maritime Transport: Risk Factors and Economic Impact. Maritime Transport facility Committee, Directorate for Science, Technology and Industry

Nincic, D. 2005. The Challenge of Maritime Terrorism: Threat Identification, WMD and Regime Response. *The Journal of Strategic Studies*, Vol. 28, No. 4, 619-644

Parfomak P, Frittelli, J. 2007. Maritime Security: Potential Terrorist Attacks and Protection Priorities. CRS Report for Congress, 9 January 2007

Pinto CA, Talley WK. 2006. The Security Incident Cycle of Ports. *Maritime Economics & Logistics*. 8 267-286

Price, W. 2004. Reducing the Risk of Terror Events at Ports, *Review of Policy Research* 21 (3), pp329-349

Raymond, C.Z. 2006. Maritime Terrorism in Southeast Asia: A Risk Assessment. *Terrorism and Political Violence*, 18:2, 239-257

Rao, S. & Goldsby, T.J. 2009. Supply chain risks: a review and typology. *International Journal of Logistics Management*, Vol. 20, No.1, pp97-123

Robinson, P. 2008. Dictionary of International Security, Polity Press: Cambridge

Sheffi Y. 2001. Supply Chain Management Under the Threat of International Terrorism. *International Journal of Logistics Management*. 12 (2)

Speier, C., Whipple, J.M., Closs, D.J. & Voss, M.D. 2011. Global supply chain design considerations: mitigating product safety and security risks. *Journal of Operations Management*, Vol. 29, No. 7-8, pp721-736

Talas R, Menachof D. 2009. The efficient trade-off between security and cost for sea ports: a conceptual model. *International Journal of Risk Assessment and Management.* 13 (1)

UNCTAD. 2007. Maritime Security: ISPS Code Implementation, Costs and Related Financing. http://www.unctad.org/en/docs/sdtetlb20071_en.pdf. (3 August 2009)

Yates, J.F, Stone, E.R. (1992), "The risk construct", in Yates, J.F (Eds),*Risk Taking Behaviour*, Wiley, New York, NY, pp.1-25.

Williams, Z., Lueg, J.E. & LeMay, S.A. 2008. Supply chain security: an overview and research agenda. *International Journal of Logistics Management*, Vol. 19 No. 2, 2008

Willis H, LaTourette T. 2008. Using Probabilistic Terrorism Risk-Modelling for Regulatory Benefit-Cost Analysis: Application to the Western Hemisphere Travel Initiative in the Land Environment. *Risk Analysis* 28 (2) 325-339

Willis H, Morral A, Kelly T, Medby J. 2005. Estimating Terrorism Risks. RAND Corporation

Woo, G. 2003. Insuring against al-Qaeda. National Bureau of Economic Research Meeting

Yates, J.F, Stone, E.R. 1992. The risk construct. In Yates, J.F (Eds),*Risk Taking Behaviour*, Wiley, New York, NY, pp.1-25.

Yap, W.Y. & Lam, J.S. 2004. An interpretation of inter-container port relationships from the demand perspective. Maritime Policy & Management, 31:4, pp337-355

Zsidisin, G.A., Ellram, L.M., Carter, J.R. & Cavinato, J.L. 2004. An analysis of supply risk assessment techniques. *International Journal of Physical Distribution & Logistics Management*, Vol. 34, No.5, pp397-413

Appendix A – The graphs in figures 1 to 6 show the performances of the 216 security system portfolios in terms of residual security risk and security investment for Port Facilities A to F

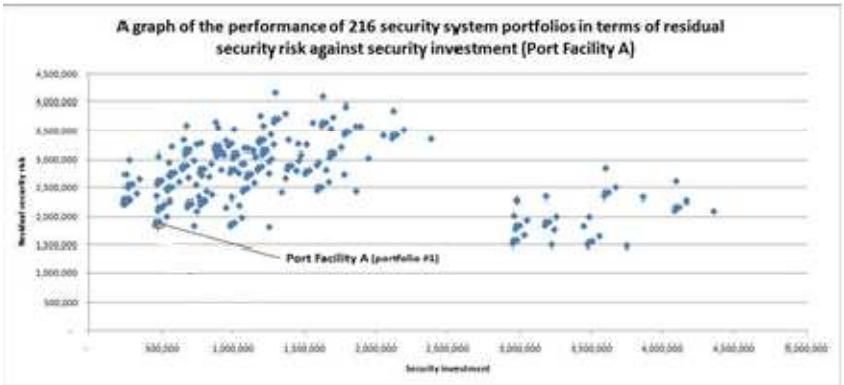

Figure 1: Optimum Portfolio Analysis: Port facility A

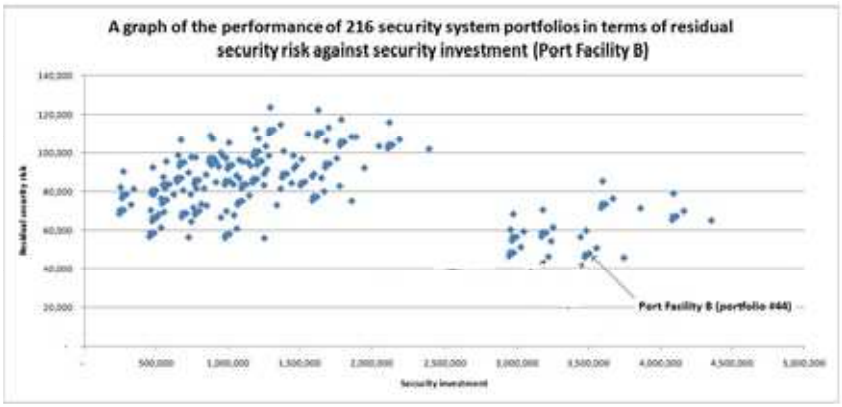

Figure 2: Optimum Portfolio Analysis: Port facility B

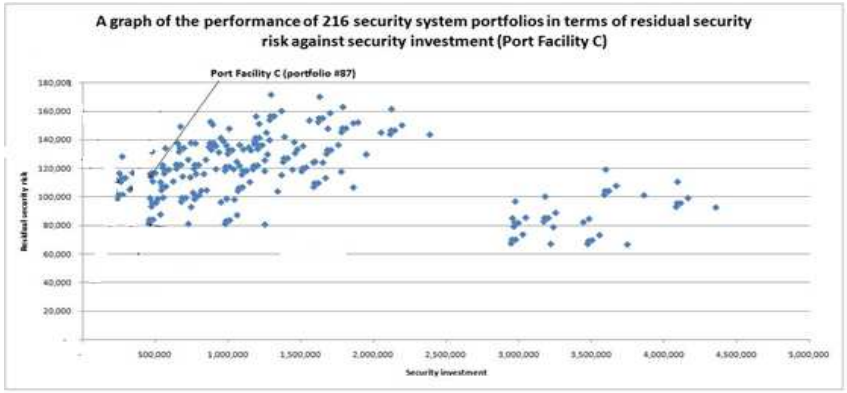

Figure 3: Optimum Portfolio Analysis: Port facility C

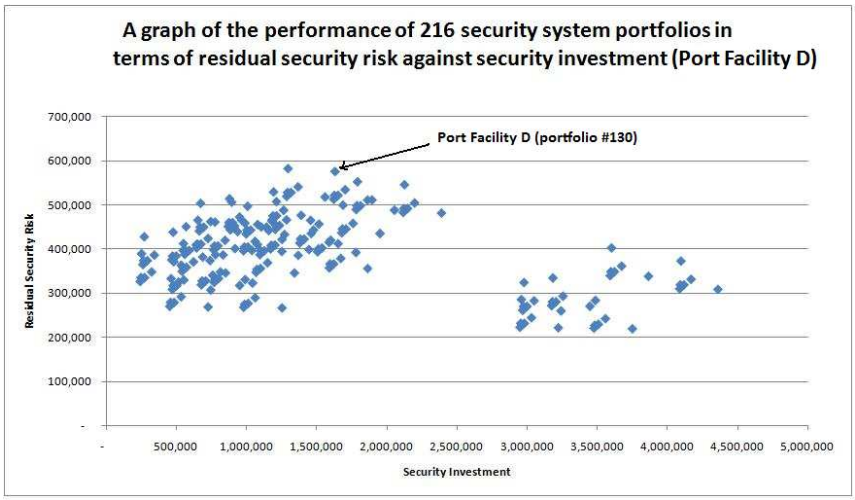

Figure 4: Optimum Portfolio Analysis: Port facility D

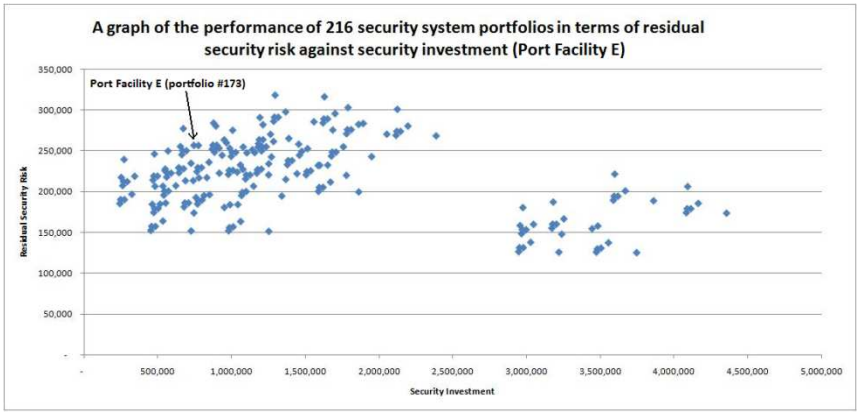

Figure 5: Optimum Portfolio Analysis: Port facility E

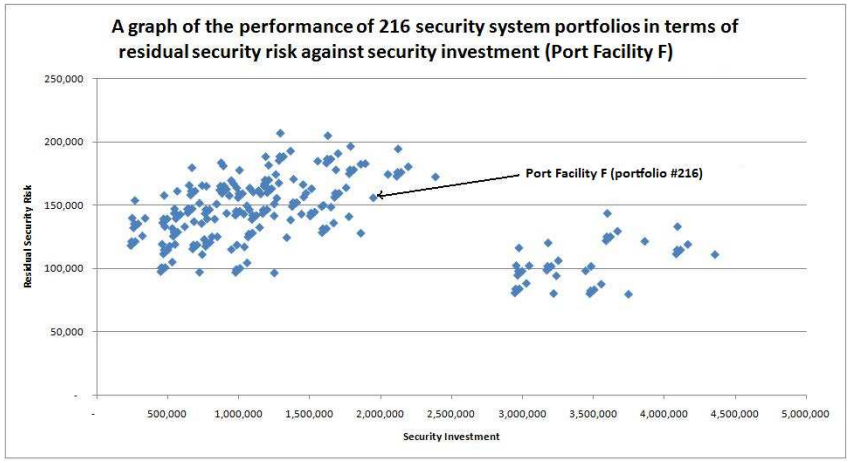

Figure 6: Optimum Portfolio Analysis: Port facility F