Designing a Centralized Training Academy for Maritime Security

Angelica Sogor
University of Miami, aangelicaa@sbcglobal.net

Follow this and additional works at: https://scholarlyrepository.miami.edu/oa_theses

Recommended Citation
https://scholarlyrepository.miami.edu/oa_theses/299
UNIVERSITY OF MIAMI

DESIGNING A CENTRALIZED TRAINING ACADEMY FOR MARITIME SECURITY

By
Angelica Sogor

A THESIS

Submitted to the Faculty of the University of Miami in partial fulfillment of the requirements for the degree of Master of Science

Coral Gables, Florida

December 2011
DESIGNING A CENTRALIZED TRAINING ACADEMY FOR MARITIME SECURITY

Angelica Sogor
The maritime industry is an economic activity that enables global trade and travel. However, the transportation network is threatened by security risks that seek to exploit vulnerabilities and cause damage to ships, interrupt the global supply chain network, and endanger the lives of crewmembers and passengers. While policies exist to aid in the prevention of attacks, these policies, alone, are insufficient to sustain global maritime domain security and awareness. Policies must be effectively enforced and complemented with highly trained crewmembers who have the knowledge and skills to efficiently prevent, detect, and respond to threats. This study analyzed maritime security policies and model courses to benchmark training requirements and create a topic development matrix for a centralized training academy for maritime security personnel. A course overview, syllabus, and learning objectives were created to reflect required and recommended security training components, with a focus on the cruise industry. This study concluded that a centralized training academy has significant benefits not only directly to the company where it is applied, but also to the maritime industry as a whole. Additional research would conduct evaluations of the academy and customize this curriculum for other companies engaged in ocean trade to enhance global maritime security and awareness.
I would like to thank Carnival Corporation & plc, who supported the research involved in this project. I would also like to thank my thesis committee: Dr. Liana McManus, Dr. Hans Graber, and Ms. Maria Estevanez. I greatly appreciate their support of my academic goals and the time they invested to reading and reviewing all of my products in this endeavor.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>LIST OF BOXES</th>
<th>vi</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIST OF FIGURES</td>
<td>vii</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td>viii</td>
</tr>
<tr>
<td>LIST OF ABBREVIATIONS</td>
<td>ix</td>
</tr>
</tbody>
</table>

## Chapter

1 INTRODUCTION AND LITERATURE REVIEW ................................................. 1
   1.1 A Need for Greater Global Maritime Security and Awareness ............ 1
   1.2 Background of International Policies for the Maritime Industry ...... 12
   1.3 Standards for Maritime Security Training .................................... 17
       1.3.1 Domestic (U.S.) ........................................................................ 17
       1.3.2 International ......................................................................... 19
   1.4 Current Security Training Methods in the Maritime Industry .......... 21
   1.5 Security Training at Carnival Corporation & plc ......................... 26
   1.6 Information and Action Gaps ...................................................... 29

2 GOALS AND OBJECTIVES ............................................................................. 33

3 SIGNIFICANCE AND LIMITATIONS ................................................................ 36

4 METHODS ........................................................................................................ 39
   4.1 Analysis of Standards and Policies at Domestic (U.S.) and International Levels ........................................................................................................... 39
   4.2 Analysis of Existing Training Curricula for Maritime Industries ...... 45
   4.3 Specific Needs of Carnival Corporation & plc’s Centralized Training Academy ................................................................. 47
   4.4 Design and Development of Carnival Corporation & plc’s Centralized Training Academy ................................................................. 49
   4.5 Pilot Study and Centralized Training Academy Evaluation .......... 50
   4.6 Cost Analysis of the Centralized Training Academy ..................... 51

5 RESULTS ......................................................................................................... 53
   5.1 Analysis of Domestic, International, and Other Standards and Policies ....................................................................................................................... 53
       5.1.1 Domestic ..................................................................................... 55
       5.1.2 International ............................................................................ 60
       5.1.3 Other ....................................................................................... 64
   5.2 Analysis of Existing Training Curricula for Maritime Industries ...... 67
List of Boxes

Box 1 – Case study analysis ........................................................................................................... 108
List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>Geographical expansion of Somali piracy</td>
<td>8</td>
</tr>
<tr>
<td>Figure 2</td>
<td>Summary data from analysis of Somali piracy in 2009</td>
<td>9</td>
</tr>
<tr>
<td>Figure 3</td>
<td>Trends in Somali piracy as related to spatial and temporal factors</td>
<td>9</td>
</tr>
<tr>
<td>Figure 4</td>
<td>Lower berth capacity and passenger carryings of the North American cruise industry from 2000-2010</td>
<td>10</td>
</tr>
<tr>
<td>Figure 5</td>
<td>Major international stakeholders in cruise industry security</td>
<td>16</td>
</tr>
<tr>
<td>Figure 6</td>
<td>Major domestic stakeholders in the maritime security domain</td>
<td>19</td>
</tr>
<tr>
<td>Figure 7</td>
<td>A flow chart depicting the design and development process of the centralized training academy</td>
<td>50</td>
</tr>
<tr>
<td>Figure 8</td>
<td>Carnival Corporation &amp; plc’s prominence in the global cruise market</td>
<td>105</td>
</tr>
<tr>
<td>Figure 9</td>
<td>The federal intelligence cycle</td>
<td>121</td>
</tr>
</tbody>
</table>
List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1</td>
<td>List of recent and historic attacks on cruise ships</td>
<td>10</td>
</tr>
<tr>
<td>Table 2</td>
<td>Summary of major international standards applicable to maritime security training</td>
<td>21</td>
</tr>
<tr>
<td>Table 3</td>
<td>Carnival Corporation &amp; plc operating lines, line headquarters, and line flag state registries</td>
<td>27</td>
</tr>
<tr>
<td>Table 4</td>
<td>Topic development matrix</td>
<td>44</td>
</tr>
<tr>
<td>Table 5</td>
<td>Summary of major policies reviewed</td>
<td>53</td>
</tr>
<tr>
<td>Table 6</td>
<td>Summary of major foreign standards and policies reviewed</td>
<td>67</td>
</tr>
<tr>
<td>Table 7</td>
<td>Course overview</td>
<td>78</td>
</tr>
<tr>
<td>Table 8</td>
<td>Learning objectives</td>
<td>82</td>
</tr>
</tbody>
</table>
List of Abbreviations

- AMSTEP – Area Maritime Security Training Exercise Program
- AWI – Asymmetric Warfare Initiative
- BMP4 – Best Management Practices for Protection against Somalia Based Piracy, Version 4
- CBP – Customs and Border Protection
- CG – Coast Guard
- CLIA – Cruise Lines International Association
- CIA – Central Intelligence Agency
- CSO – Company Security Officer
- CSI – Container Security Initiative
- CTPAT – Customs Trade Partnership against Terrorism
- CVSSA – Cruise Vessel Security and Safety Act
- DHS – Department of Homeland Security
- DOT – Department of Transportation
- EU – European Union
- FBI – Federal Bureau of Investigation
- FCCA – Florida-Caribbean Cruise Association
- IMB – International Maritime Bureau
- IMCO – Inter-governmental Maritime Consultative Organization
- IMO - International Maritime Organization
- ISM – International Safety Management Code
- ISPS – International Ship and Port Facility Security Code
• LRAD – Long Range Acoustic Device
• MARAD – Maritime Administration
• MARSEC Levels – Maritime Security Levels
• MSST – Maritime Safety and Security Team
• MTSA – Maritime Transportation Security Act
• Model Course 1.28 – IMO Model Course for Crowd Management, Passenger Safety and Safety Training for Personnel Providing Direct Services to Passengers in Passenger Spaces
• Model Course 1.29 – IMO Model Course for Proficiency in Crisis Management and Human Behavior Training Including Passenger Safety, Cargo Safety, and Hull Integrity Training
• Model Course 3.19 - IMO Model Course for Ship Security Officer Training
• MoU – Memorandum of Understanding
• NVIC – Naval Vessel Inspection Circular
• plc – public limited company
• PortSTEP – Port Security Training Exercise Program
• Ro-ro – roll on, roll off vessels
• SAFE Port Act – Security and Accountability For Every Port Act
• SAR – International Convention on Maritime Search and Rescue
• SOLAS – International Convention for the Safety of Life at Sea
• SRG – Security Review Group
• SSO – Ship Security Officer, also known as VSO
• STCW – International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers
• TSA – Transportation Security Administration
• TSCM – Technical Surveillance Counter-Measures
• TWIC – Transportation Worker Information Credential
• UK – United Kingdom
• UKMTO – United Kingdom Maritime Trade Operations
• U.S. – United States
• VSO – Vessel Security Officer, also known as SSO
• WMD – Weapons of Mass Destruction
1.1 A Need for Greater Global Maritime Security and Awareness

The fields of maritime security and maritime domain awareness have advanced in recent years, as maritime transportation has increased its presence in an increasingly globalized world. Security concerns have also received heightened attention following the terrorist attack on the USS Cole in 2000 and the terrorist attacks on the World Trade Center on September 11, 2001. Prior to September 11, main security objectives in the maritime industry centered around “smuggling, theft, illegal aliens, and drug trafficking,” as explained by former Central Intelligence Agency (CIA) Director James Woolsey; “…we have seen our own infrastructure used against us, the stakes have changed and seaport security has become a whole new world…The last time prior to September 11 that our own infrastructure was used against us by a foreign enemy, was when the British burned down the White House in 1814” (Wade, Jared).

Even as terrorism remains a dominant threat in the maritime industry, piracy has also emerged as a significant danger facing ships, particularly those traveling in areas at high risk for piracy. High risk areas threatened by Somali pirates include: the Gulf of Aden, the Arabian Sea, and the Northern Indian Ocean. These high risk areas and the recent geographical expansion of Somali-based piracy can be seen in Figure 1. Piracy trends are further impacted by weather patterns, notably the South West monsoon and the North East
monsoon; as winds and waves increase in intensity and size, piracy, at least in the noted high risk areas, decreases. As a result of decreased piracy in high risk areas impacted by monsoons, piracy can increase in other areas, including waters off Kenya and Tanzania. Although these established, and publicized, patterns help ships avoid pirates, the threat is still imminent, and these patterns do not exclusively encompass all attempted attacks or hijackings (United Kingdom Maritime Trade Operations). Because piracy is affected by both spatial and temporal considerations, existing policies may not be enough for companies and crews to fully be aware of their risks.

The *MV Maersk Alabama* is one ship that is, unfortunately, familiar with piracy. The ship encountered pirates twice in 2009, once in April, and once in November. In the April 2009 attack, Somali pirates hijacked the ship, and the ship’s Captain was held hostage for five days before the U.S. Navy successfully intervened. In the November 2009 attack, the ship was not hijacked because as pirates fired weapons, the ship, this time, was defended by an armed security team who responded to the attack with “gunfire and a high-decibel noise device” ("Pirates Attack U.S.-Flagged Maersk Alabama"). Because the ship learned from its first attack, it was prepared to defeat its next piracy encounter, which would not be its last, as the ship would meet with suspected pirates several more times. In September 2010, the *MV Maersk Alabama* was met by armed pirates in a skiff, who were effectively deterred by warnings of gunfire and acoustic weaponry from an armed security team aboard the ship ("Pirates Set Sights on Maersk Alabama Again, Maritime Group Says"). And in March of 2011, the *MV Maersk Alabama*
was again approached by a suspicious skiff, which was presumed to be filled with pirates looking to attack and hijack the ship. Fortunately, the ship successfully foiled another potential attack, also as a result of the armed security team, who fired the warning shots that caused the pirates to retreat ("Pirates Target the Maersk Alabama Again"). While Maersk was able to implement some best management practices to counter future pirate attacks, it had only done so after being the victim of a hijacking. As terrorism and piracy threats subsist, it is imperative that ships and crews take necessary measures, such as improved security training or the establishment of an additional security team onboard, to protect the ships, the crewmembers, and the shipping routes that proliferate trade and travel. Best Management Practices for Protection against Somalia Based Piracy, Version 4, represents a comprehensive list of precautionary measures and actions that companies and crew may implement to deter acts of piracy.

Specifically within the cruise industry, there was a terrorist attack on the ship *Achille Lauro* in the Mediterranean, in 1985. This attack shows how terrorism has progressively become more deadly since then; in that attack, only one passenger was killed, but that number might not be so low in 2011. After September 11, it became clear that “ships in ports, particularly large commercial cargo ships or cruise ships, could be attacked by terrorists.” Such attacks could harm an enormous amount of lives, considering that a cruise ship can hold an excess of 3,000 passengers, the majority of whom are typically U.S. citizens. Harm can be done to terrestrial and marine environments, which can be affected
by biological or chemical weapons and resulting pollution. Additional harm can impact port infrastructure and shipping channels; such destruction interrupting the maritime transportation system could halt world trade (Frittelli, John, F.).

Furthermore, cruise ships can be targets for large scale attacks because they “cater to large numbers of people who are confined to a single geographic space – which makes them ideal venues for carrying out assaults intended to maximize civilian casualties.” Whether a small or large scale attack was carried out on a passenger ship, it would likely generate media attention and a public following, and “this type of publicity is critical to the dynamics of any terrorist entity.” These and other factors can lead cruise ships to be potential targets for terrorist organizations, especially in consideration that security measures in the cruise industry differ from those in the aviation industry. Even though passenger screening for cruises has seen improvements since the September 11 attacks, it is still less thorough than that of the aviation industry; however, this is a generalization, and some cruise lines may adhere to more strict practices than what is required by the domestic cruise industry as a whole. Additionally, industry standards can vary among domestic and international ports; “many of the service employees who have access to ships at overseas docks may not have undergone any form of comprehensive background checking” (Greenberg, M., et al).

More recently, the cruise industry has also been impacted by threats of piracy, in addition to existing terrorism concerns. In November of 2005, two small boats approached a Seabourn Cruise Lines ship off the coast of Somalia. The
pirates in those boats used machine guns and rocket-propelled grenades to attack the ship, with the likely intention to board and hijack it. While the ship outran the pirates and avoided further attack, one crewmember was injured and the ship sustained minor, yet visible damages. Seabourn ships are on the smaller end, in terms of size and capacity, within the cruise industry, and this small size may have led to an appeal as a target. This particular ship, the Seabourn Spirit, was carrying a total of only 310 passengers and crew ("Cruise Liner Outruns Armed Pirate Boats"). However, larger ships face piracy threats as well. The Oceania Nautica is considerably larger than the Seabourn Spirit, but it also faced piracy in November 2008. Two small pirate boats suspiciously approached the cruise ship, but the ship avoided an attack with "evasive maneuvers and [acceleration] to its full speed." The Nautica held 1,048 passengers and crew at the time of the attempted attack, which took place off the coast of Yemen. After the incident, the company did not report plans to change travel routes, as doing so would not be practical ("Luxury Cruise Ship Outruns Pirates"). Although larger cruise ships that carry upwards of 4,000 passengers may not have the same vulnerabilities as much smaller ships do, these two attacks show that pirates will not discriminate against cruise ships. All cruise ships, especially those with physical vulnerabilities, such as small size, and those traveling near known areas of piracy, need to be aware of piracy, in addition to terrorism, as a prevailing security threat. Especially with consideration that avoiding these areas entirely is not feasible or sensible for cruise or cargo companies, ships and crewmembers need better preparation to avoid and mitigate security threats. Piracy data from
2009 including types of attacks, region of attack, and month of attack are illustrated in Figures 2 and 3. These figures, which show spatial and temporal trends in piracy, especially as related to the seasonal monsoons, can guide ships as to when and where attacks are most likely to take place.

Immediately following the horrific attacks of September 11 and the increasing trends of piracy, there was a surge in policymaking and a need for even greater technical innovation. While it is imperative to have a defined legal framework and supporting technology to aid in the prevention of a terrorist attack, these elements are only as strong as those whose duty it is to understand, implement, and enforce them. More specifically, it is of interest and importance to understand how this implementation and enforcement begins in the cruise industry, which, having transported 15 million passengers in 2010 and predicted to service 16 million in 2011, is a target for terrorism, as terrorists have already attacked sectors of the transportation network. As this industry grows, with an expected 26 new ships to join North American waters before 2015, global safety and security concerns also grow (“Cruise Industry Overview – 2011”). The growth of the North American cruise industry, and thus the increased potential for ships to be at risk of a terrorist or pirate attack, can be seen in Figure 4. An overview of historic and recent attacks on cruise ships is available in Table 1.

While this research focuses on maritime security threats, especially those within the cruise industry, it is worthwhile to briefly compare the aviation industry and the cruise industry, both of which are popular methods of personal travel. In 2010, the number of domestic and international passengers in the U.S. aviation
industry, as reported by scheduled flights, totaled 787, 324, 206 million (“Data Elements”). In comparison, the cruise industry carried 14, 820, 000 million passengers worldwide in 2010 (“Cruise Lines International Association”). It is important to note that the data for the aviation industry does not distinguish between personal and business travel. Within the U.S., both industries employ security measures and work with federal government agencies to protect the entire transportation system, including passenger safety and security. While air travel does receive more passengers on an annual basis and has been the receipt of more attempted and successful terrorist attacks, it is still interesting to look at the variance of security practices and procedures among the two different types of passenger travel. Although security procedures and screening practices may vary among port facilities and specific cruise lines, the Cruise Lines International Association (CLIA) notes:

Security measures are standard for cruise ships today and include passenger screening procedures similar to those found at U.S. airports including the use of metal detectors. Security procedures include the 100 percent inspection of all passengers, their carry-on baggage and luggage. Each crewmember holds a U.S. seafarers visa and has thus undergone a U.S. State Department background check prior to visa issuance. In addition, all crewmembers and guests are placed on an official manifest and may embark and disembark only after passing through a security checkpoint. Once a ship is underway, only documented employees and fare-paying passengers are on board. (“Cruise Lines International Association”)

Although it is interesting to compare passenger and cargo screening measures between the aviation and the cruise industries, there are possible benefits to the cruise industry employing measures that may fall short of practices in air travel. Enhanced (and possibly lengthy) screening procedures
can also negatively impact air travel; there are noted “economic damage[s] inflicted by the current inefficiencies in the passenger screening process [at U.S.
airports].” Ultimately, such inefficiencies can limit job creation and economic
growth (“U.S. Travel Industry Urges Improved Efficiency at Nation’s Airports”).

While this research focuses on security in the cruise industry, it is important to
note that developments, such a centralized training academy for maritime
security, should ideally aim to enhance ship security, without inconvenient,
impractical, or negative impacts to the passengers or industry as byproducts of
better security.

Figure 1 – Geographical expansion of Somali piracy; Source: European Union
Naval Force
Figure 2 – Summary data from analysis of Somali piracy in 2009; Source: United Nations Institute for Training and Research

Figure 3 – Trends in Somali piracy as related to spatial and temporal factors; Source: United Nations Institute for Training and Research
Figure 4 – Lower berth capacity and passenger carryings of the North American cruise industry from 2000 – 2010; Source: Cruise Lines International Association

Table 1 – List of recent and historic attacks on cruise ships; Source: www.cruisebruise.com

<table>
<thead>
<tr>
<th>Date</th>
<th>Type of Attack</th>
<th>Ship Line</th>
<th>Event Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.12.2011</td>
<td>Piracy</td>
<td>Acromas Holidays Ltd</td>
<td>- Pirates followed alongside the ship and attempted to board; ship increased speed and pursued evasive measures; pirates fell behind and did not board</td>
</tr>
<tr>
<td>4.25.2009</td>
<td>Piracy</td>
<td>MSC Cruises</td>
<td>- Reports indicate passengers were first to notice pirates boarding the ship and first to combat the attack (with patio chairs) before security personnel acted; pirates did not successfully board</td>
</tr>
<tr>
<td>12.4.2008</td>
<td>Piracy</td>
<td>German Transocean Tours</td>
<td>- Two suspected pirate boats were approaching the ship for an attempted attack; the Germany Navy prevented a successful boarding</td>
</tr>
<tr>
<td>Date</td>
<td>Type</td>
<td>Cruise Line</td>
<td>Event Description</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>12.3.2008</td>
<td>Piracy</td>
<td>Classic International Cruises Australia</td>
<td>Ship was reportedly surrounded by 29 small pirate boats; reports later said these small boats were local fishing vessels.</td>
</tr>
<tr>
<td>11.30.2008</td>
<td>Piracy</td>
<td>Oceania Cruises</td>
<td>A pirate skiff came within 300 yards of the ship and fired shots; a French helicopter responded to the attack and the pirates aborted the potential hijacking.</td>
</tr>
<tr>
<td>4.4.2008</td>
<td>Piracy</td>
<td>CMA-CMG</td>
<td>Small cruise ship was seized by pirates; no passengers were onboard at the time but the yacht and the crew were taken hostage for ransom; hostages and ship were freed 7 days later.</td>
</tr>
<tr>
<td>11.5.2005</td>
<td>Piracy</td>
<td>Seabourn</td>
<td>Pirates fired shots and grenades at the ship in a potential boarding of the ship; the ship outran the pirates and avoided further attack although the ship sustained minor damage and one crewmember was injured.</td>
</tr>
<tr>
<td>7.12.1988</td>
<td>Terrorism</td>
<td>Cycladic Cruises</td>
<td>Terrorists had concealed automatic weapons and hand grenades boarded the ship at Aegina and when it was several miles from shore, they killed 11 people and 98 people were injured.</td>
</tr>
<tr>
<td>1.23.1961</td>
<td>Terrorism</td>
<td>Companhia Colonial</td>
<td>Ship was seized by Portuguese rebels who infiltrated the luxury cruise ship and forced the ship to take a different course; 1 person was killed and several others were injured.</td>
</tr>
</tbody>
</table>
1.2 Background of International Policies for the Maritime Industry

Current international standards for maritime operations stem mostly from international conventions and codes of the International Maritime Organization (IMO), an agency of the United Nations. Prior to the establishment of the IMO, treaties and conventions were created and adopted with a piecemeal mechanism, which was most prominently seen through the formation of the International Convention for the Safety of Life at Sea (SOLAS) in 1914, as a response to the sinking of the RMS Titanic two years prior. Although SOLAS was a result of an incident with a passenger vessel, around this time, countries realized that even though shipping was such an international industry, the practices and procedures guiding it varied greatly from country to country and ship to ship. This led to the creation of the Inter-Governmental Maritime Consultative Organization (IMCO) in 1948. The agency entered into force in 1958, and in 1982, its name changed to the International Maritime Organization (IMO). IMO’s first conventions dealt mainly with safety issues, but as the maritime domain expanded and new concerns arose, IMO also dealt with issues of security, pollution, and specific regulations for cargo shipping. In 1978, due to the variance of practices among commercial ships, the IMO adopted the International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers (STCW), which was amended recently in 2010, with the Manila Amendments, as a response to current piracy threats (“IMO | International Maritime Organization”).
Also in 1978, the Hague Memorandum was developing among maritime interests in Western Europe. Although it was independent of the IMO, it led to important international practices on port state control. The Hague Memorandum was similar to STCW in its focus on shipboard living and working conditions, but right before it was to enter into force, there was an oil spill off the coast of France, which spurred motivation for something greater than the Hague Memorandum. This led to the Paris Memorandum of Understanding (MoU) on Port State Control, which was adopted in 1982. It originated with 14 members of the European Union, and it is now in force with 27 member countries. The Paris MoU enhances authority of port states, while complementing requirements and recommendations of the IMO. The Paris MoU gives port states the authority to conduct safety and security inspections, which are based off a risk profile analysis, in which passenger vessels are typically considered high risk (“Welcome to Paris MoU”). While the Paris MoU is specific to Europe and the north Atlantic regions, there are other MoUs that establish port state control in other areas of the world. They are: Tokyo MoU (Asia and Pacific regions); Acuerdo de Viña del Mar (Latin America); Caribbean MoU; Abuja MoU (West and Central Africa); Black Sea MoU; Mediterranean MoU; Indian Ocean MoU; and the Riyadh MoU (Gulf region) (“Port State Control”).

In the 1980s, maritime safety concerns grew into security concerns with hijackings of ships, notably the Achille Lauro in 1985. These events spawned response from the IMO with "Measures to Prevent Unlawful Acts Which Threaten the Safety of Ships and the Security of Their Passengers and Crews" in 1985
and “Measures to Prevent Unlawful Acts against Passengers and Crew On Board Ships” in 1986. Presently, these measures have been adopted into conventions and codes for stronger guidance. In November 2001, two months after the September 11 attacks on the United States, the IMO met and adopted a resolution, the “Review of Measures and Procedures to Prevent Acts of Terrorism Which Threaten the Security of Passengers and Crews and the Safety of Ships.” This resolution recalled and reviewed past conventions, measures, and resolutions to determine if something more than past IMO actions was necessary to combat new threats of terrorism. It was discovered that stronger regulations were needed, which led to the development of the International Ship and Port Facility Security (ISPS) Code in 2002. ISPS entered into force in 2004, and it is formally located in Chapter XI-2 of SOLAS (“IMO | International Maritime Organization”).

Even though terrorism concerns had not subsided much, concerns of piracy also arose in the first decade of 2000, which initiated the 2010 Manila Amendments to STCW. These amendments require training for seafarers in the event their ship is attacked by pirates (“IMO | International Maritime Organization”). Also in response to piracy threats, the United Kingdom Maritime Trade Operations (UKMTO), with support from many other industry organizations and interests, published the fourth version of Best Management Practices for Protection against Somalia Based Piracy (BMP4), in 2011. The guide consists of “suggested planning and operation practices for ship operators, and Masters of Ships transiting the high risk area.” With detailed instructions and procedures for
prior to entering a high risk area, during different stages of an attack, and post
incident action, these Best Management Practices allow for explicit fulfillment of
the somewhat vague 2010 STCW Manila Amendments (United Kingdom
Maritime Trade Operations).

Although ISPS is the major backbone of international maritime security
policy, it is complemented by IMO measures incorporated into SOLAS and
STCW, as well as by practices pursued by the European Union and the UKMTO.
Other conventions that are not directly applicable to this research, but are
important in the maritime safety domain include: the International Convention on
Maritime Search and Rescue (SAR) and the United Nations Convention for the
It should be noted that SUA cites specific actions, such as “the seizure of ships by
force; acts of violence against persons on board ships; and the placing of devices
on board a ship which are likely to destroy or damage it,” which can be
categorized as acts of piracy and/or terrorism. However, SUA seems to be more
concerned with the acts of crime or persons who commit them, rather than the
establishment of guidelines or training protocol to prevent or respond to such
actions (“IMO | International Maritime Organization“).

IMO conventions and codes are internationally applicable; however, they
are only fully adopted and implemented by member countries who are
signatories to the convention. Even still, IMO is not an agency charged with
enforcement duties, and the adoption and enforcement of policies rests on
market forces, economic incentives, and self-regulation within the maritime
industry. While other countries may have national specific maritime security training requirements, the IMO represents major international policies that are relevant in maritime security training ("IMO | International Maritime Organization"). These policies are also recommended and promoted by international stakeholders in the cruise industry, including the Cruise Lines International Association (CLIA) and the Florida-Caribbean Cruise Association (FCCA). Another international stakeholder is the International Maritime Bureau (IMB), which is a department of the International Chamber of Commerce. IMB works to protect against maritime crimes, with a current focus on preventing and reporting attacks of piracy ("International Maritime Bureau"). Figure 5 shows major international stakeholders in the maritime security domain, with a focus on the cruise industry.

Figure 5 – Major international stakeholders in cruise industry security
1.3 Standards for Maritime Security Training

1.3.1 Domestic (U.S.)

A visual representation of U.S. stakeholders in the maritime security domain is represented in Figure 6. Within domestic maritime territory, there exist a number of agencies that protect cruise ships, port security, and overall homeland security. Port security involves two major departments: the Department of Homeland Security (DHS) and the Department of Transportation (DOT). Under DHS are: the Coast Guard, the Bureau of Customs and Border Protection (CBP), and the Transportation Security Administration (TSA). These authorities have the most visible operations in preserving security at U.S. ports and in U.S. territorial waters. CBP can inspect ship crewmembers and passengers that are arriving at U.S. ports from foreign destinations. TSA, in partnership with the Coast Guard, implements the Transportation Worker Identification Credential (TWIC) system that maintains security in areas of ports that are high risk. The Coast Guard also preserves a security zone around ports, and continues this zone around cruise and cargo ships arriving at or departing from domestic ports. The Coast Guard also uses cutters and aircrafts to monitor coastal waters and infrastructure. DHS, as required by the Intelligence Reform and Terrorism Prevention Act of 2004, maintains a “terrorism ‘watch list’ for passengers and crew aboard cruise ships” (Fritelli, John, F.).

Under the DOT is the Maritime Administration (MARAD). While MARAD may not be a visible force at U.S. ports, they aid in development of model course frameworks that complement U.S. legislation. The major U.S. legislation, policies,
and regulations that apply to maritime security training are: the Maritime Transportation Security Act of 2002 (MTSA), the Security and Accountability for Every (SAFE) Port Act of 2006, the Cruise Vessel Security and Safety Act of 2010 (CVSSA), the Coast Guard Naval and Vessel Inspection Circulars (NVIC), and the Executive Order: Blocking Property of Certain Persons Contributing to the Conflict in Somalia or 2010. Much of this legislation has come about as a result of the September 11 attacks in the United States, and also due to the growing global concerns of piracy and terrorism.

Despite all these levels of security within U.S. territories, most cruise and cargo ships are not domestically owned, nor do U.S. citizens typically make up these ship crews (Frittelli, John, F.). In light of such situations, it becomes critically important how security training occurs. Because personal opinions, fears, and bias about maritime security can drastically differ by geographical region and culture, a standardized training system is necessary to bring all personnel the same basic levels of knowledge and awareness of international maritime policies and security practices. Standardized training can also reduce discrepancies of security practices and intelligence among developed and developing countries. Although developing countries “may not be able to afford the technology to improve their ports’ security,” centralized training would ensure that all ship personnel have equal access to knowledge that could enhance global maritime security, even though individual port infrastructure may vary (Frittelli, John, F.).
1.3.2 International

International standards for maritime security training rest mostly on conventions, codes, and model course frameworks produced by the IMO. The predominant common denominator among international maritime security policies is the implementation of the International Ship and Port Facility Code (ISPS), which is contained in IMO’s International Convention for the Safety of Life at Sea (SOLAS). ISPS is divided into two parts, Part A, which is mandatory for those who are signatories to the convention, and Part B, which contains additional recommendatory guidance. IMO members should implement and enforce Part A of ISPS. Some counties, such as the U.S., have adapted ISPS to legislation with other names, such as the MTSA. And some countries, such as
those in the European Union, have mandated that recommended sections of Part B are implemented and enforced as required policies. Even though ISPS provides common ground for international maritime security training, there are still discrepancies in how it is applied to training; ISPS may require what elements should be a part of ship security training, but how and to what extent the training is conducted is not standardized.

Additional international training standards stem from the 2010 Manila Amendments to IMO’s International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers (STCW). These amendments apply to IMO members and require training that prepares crews for threats of piracy. Similarly, the Philippine Overseas Employment Administration requires Mandatory Anti-Piracy Awareness Training for Seafarers. This awareness course is mandated for all Filipino seafarers, regardless of their shipping routes. Although seemingly exclusive to the Philippines, because that country provides an abundance of personnel within the maritime industry, this is a requirement that affects many shipping and cruise lines, and their respective companies and flag states, which creates a somewhat international requirement for piracy awareness, even for countries who are may not be IMO members but employ Filipino seafarers. These international standards are summarized in Table 2.
Table 2 – Summary of major international standards applicable to maritime security training

<table>
<thead>
<tr>
<th>Government or Organization</th>
<th>Legislation or Conventions Related to Maritime Security Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S.</td>
<td>• Maritime Transportation Security Act</td>
</tr>
<tr>
<td></td>
<td>• Cruise Vessel Security and Safety Act</td>
</tr>
<tr>
<td></td>
<td>• Security and Accountability for Every (SAFE) Port Act</td>
</tr>
<tr>
<td></td>
<td>• Coast Guard Naval and Vessel Inspection Circulars</td>
</tr>
<tr>
<td></td>
<td>• Executive Order: Blocking Property of Certain Persons Contributing to the Conflict in Somalia</td>
</tr>
<tr>
<td>IMO</td>
<td>• SOLAS, which contains ISPS</td>
</tr>
<tr>
<td></td>
<td>• STCW</td>
</tr>
<tr>
<td>Philippines</td>
<td>• Mandatory Anti-Piracy Awareness Training for Seafarers</td>
</tr>
</tbody>
</table>

1.4 Current Security Training Methods in the Maritime Industry

Existing research involving security in the maritime industry has analyzed how the U.S. Coast Guard “assessed risk in accordance with the DHS’s guidance and identified risks” in the cruise industry. This research also looked at protective actions taken by government agencies and ship operators to enhance security. Presently, TSA “creates and distributes security training courses for passenger vessel employees.” TSA guidance attempts to enhance attentiveness and develop responses to possible threats from ship personnel. TSA is also involved in a Visible Intermodal Prevention and Response program, which uses
technology, such as explosive detection devices, and manpower, such as behavior detection officers, to increase protective measures. Since 2006, this program has had 180 maritime operations (U.S. Government Accountability Office).

Similarly, DHS has authored reports through the Security Office of Inspector General that advise the Coast Guard “to perform a comprehensive review and analysis of the Maritime Safety and Security Team (MSST) program to ensure….maritime law enforcement and homeland security mission requirements in the current threat environment.” The MSST was created as an anti-terrorism response to the September 11, 2001 attacks, and these reports of the MSST showed that program “training content and curricula are standardized, [but] training delivery and availability of training assets are not.” In order to ensure that MSST is operating at its maximum potential, the report recommended that the Coast Guard continue to evaluate what amounts and types of staff and training best accomplish the missions of the program (Department of Homeland Security). This finding highlights the importance of education and training in the implementation of maritime security.

Another study sponsored by the Coast Guard looked at maritime operations through a social science perspective. This study investigated human factors in specific areas of security, such as manning, navigation, and training. Although this annotated bibliography addresses issues, key findings, and limitations of various studies of “application of human factors to the maritime industry,” security training is not the main focus. Among the variety of maritime
topics covered, one study resulted in finding the value of “careful training and implementation” before new technological advancements are used (Lee and Sanguist). The broad nature of the annotated bibliography, however, does not provide abundant understanding of maritime training specifically related to security.

Research done by Old Dominion University investigated the security incident cycle. The cycle is comprised of prevention, detection, response, and recovery phases. While this study finds that the prevention and detection phases have experienced considerable advances since the attacks of September 11, 2001, it focuses only on port security (Pinto and Talley). Cruise ships can have lengthy stays at ports, but their in-transit methods of sustaining security are also important, and thus require additional study. The rise of greater security needs and the implementation of new defense measures have also been explored, and additional research noted that “security measures implemented will be effective only as long as the people responsible for protecting the industry carry out their jobs efficiently” (Watt).

Research puts a strong emphasis on prevention as the most effective method of increasing maritime security;

Security experts argue that an effective solution must start with preventing undesired items from entering the maritime transportation network, because if some of these items — particularly nuclear weapons or dirty bombs — reach a U.S. seaport, they could be detonated before inspectors could find them. (Frittelli, John, F.)

Although this quote is in specific reference to container shipping, it can apply equally to cruise ships, which can also be used to transport illegal drugs,
weapons, and people. Research suggests “a layered approach with multiple lines of defense from the beginning to the final destination of a shipment” is the best preventative protection (Frittelli, John, F.). Again, applying this logic to the cruise industry, one of the lowest, but most important, layers is security training. With appropriate training, guards aboard cruise ships will be able to detect and protect against threats before such threats become an irrevocable and destructive attack. This implementation and efficiency can only come from the most proficient training, and the question remains, in the cruise industry, as to what type of training achieves this goal of maximum security.

The Maritime Transportation and Security Act (MTSA) of 2002 required “development of standards and curriculum to facilitate the education and training of maritime security personnel.” These developments can be applied to security training in the cruise industry, as they were designed with the intention to be used by “institutions and organizations that conduct maritime security education and training.” A report to Congress regarding the MTSA offered model course framework for the following positions: vessel security officer; company security officer; facility security officer; vessel personnel with specific security duties; facility personnel with specific security duties; military, security, and law enforcement; and general maritime security awareness. Each of the above models indicates the scope of the training, entry standards, course delivery options, teaching aids, legal references, and specific subject areas (MTSA Section 109 Implementation).
Another report to Congress addresses the Port Security Training Exercise Program (PortSTEP), developed by TSA. Fulfilling certain requirements under the MTSA, PortSTEP uses tabletop and field exercises to educate and prevent against terrorist attacks. Specific exercises have looked at threats of chemical, biological, and radiological nature, and different points of the maritime transportation network, including cruise ships, where these threats could become attacks. PortSTEP provides a holistic view as it integrates marine and terrestrial aspects of maritime commerce, including rail and trucking systems. In this same report, Area Maritime Security Training and Exercise Program (AMSTEP), developed by the Coast Guard, is also discussed. AMSTEP, similar to PortSTEP, fulfills requirements of MTSA by performing tabletop and field exercises, but it focuses more on land-based security near ports. Previous AMSTEP exercises include instances of “terrorist stowaways on an inbound hazardous cargo vessel, an explosion at a jet fuel receiving terminal, a suspicious package at a port facility…and explosion aboard an oil tanker in a shipping channel.” Additional training and exercises take place through the Asymmetric Warfare Initiative (AWI), which uses Coast Guard, Navy, and Federal Bureau of Investigation (FBI) resources to train and prevent against terrorist threats, including “hostage-taking and executions aboard a vessel in port” and “underwater explosive devices planted on multiple vessels in port” (Parfomak, Paul W. and Frittelli, John).

These reports to Congress offer extensive and informative suggestions to improving maritime security, and they emphasize the significance of security training, which highlights the value of this research. Despite certain training
requirements of U.S. legislation and international conventions, how training is implemented and whether training goes beyond minimal requirements can differ among and within the cruise and shipping industries. A centralized training academy, proposed by Carnival Corporation & Public Limited Company (plc), seeks to reduce these variances in security training curriculum design and implementation. Previous research offers a substantial starting point in designing curriculum for a centralized training academy, from which further research will identify which parts of existing model frameworks can be potentially used by Carnival Corporation & plc and what further information is required to complete Carnival's specific goals. This study of how the mechanisms behind security training are actually designed and applied in the maritime industry is still a relatively untapped area of research.

1.5 Security Training at Carnival Corporation & plc

Carnival Cruise Lines, which was formed in 1972, is the flagship brand of Carnival Corporation & plc. Carnival Cruise Lines bought several other operating lines in the late 1980s and 1990s. Carnival then formally adopted a corporation status and name in 1994, and it continued to expand. In 2003, Carnival Corporation and P&O Cruises united, and Carnival Corporation & plc became “one of the largest leisure travel companies in the world” (“Carnival Corporation & plc”).

Carnival Corporation & plc presently operates ten individual operating cruise lines, which plan and execute their security training fairly autonomously. The operating lines are: Holland America, Seabourn, Princess Cruise Lines,
Carnival Cruise Lines, P&O Cruises, Cunard, AIDA, Costa, Iberocruceros, and P&O Cruises Australia. Table 3 displays the operating lines, their locations of headquarter and the flags to which their ships are registered. Each operating line must conform to the minimum requirements developed by Carnival Corporation & plc, but the overall training development is a fragmented process that can create variances among the different lines. Although each operating line may have domestic and international regulations to comply with, they have individual training curricula, which may or may not extend beyond current industry requirements, and they each have different systems of executing the training.

Table 3 – Carnival Corporation & plc operating lines, line headquarters, and line flag state registries

<table>
<thead>
<tr>
<th>Operating Line</th>
<th>Headquarters</th>
<th>Flag States</th>
</tr>
</thead>
<tbody>
<tr>
<td>Holland America</td>
<td>Seattle, Washington</td>
<td>Netherlands</td>
</tr>
<tr>
<td>Seabourn</td>
<td>Seattle, Washington</td>
<td>Bahamas</td>
</tr>
<tr>
<td>Princess Cruise Lines</td>
<td>San Clarita, California</td>
<td>Bermuda</td>
</tr>
<tr>
<td>Carnival Cruise Lines</td>
<td>Miami, Florida</td>
<td>Bahamas, Panama</td>
</tr>
<tr>
<td>Carnival UK (P&amp;O Cruises and Cunard)</td>
<td>Southampton, United Kingdom</td>
<td>United Kingdom, Bermuda</td>
</tr>
<tr>
<td>AIDA</td>
<td>Rostock, Germany</td>
<td>Italy</td>
</tr>
<tr>
<td>Costa</td>
<td>Genoa, Italy</td>
<td>Italy</td>
</tr>
<tr>
<td>Iberos</td>
<td>Madrid, Spain</td>
<td>Italy</td>
</tr>
<tr>
<td>Carnival Australia (P&amp;O Cruises Australia)</td>
<td>Sydney, Australia</td>
<td>United Kingdom</td>
</tr>
</tbody>
</table>
Realizing that such fragmented training can result in discrepancies in knowledge of threats and responses to threats, Carnival Corporation & plc sought to standardize training among their different lines in one synchronized academy for all security personnel. If operating lines decide they have specific training, such as specific national legislation or concerns based on their ships’ destinations, to include in addition to the core training outlined by the Corporation, they will have the opportunity to supplement the academy with such additional training for their own personnel. The centralized training academy thus allows for a minimum standardized security education, while allowing operating lines to supplement this with additional training if necessary. This research aimed to analyze the design of the proposed centralized training academy by examining what aspects of international maritime law and policy are taught, how these topics are chosen among considerations of the geographically diverse nature of the cruise lines, and how the topics will effectively be taught to ensure understanding of regulations and compliance from personnel.

Because many “cruise lines are European-owned and fly either European or open registry flags,” policy and security training is an issue that covers international facets (Kite-Powell). Standardizing training among different cruise lines could supply a fleet of ship security personnel who possess increased global knowledge and awareness. If each line continues to operate independent security prevention, security guard training risks the possibility of being too region-specific and sheltering personnel from the ability of adapting to increasing demands of global protection and resilience from threats. A centralized training
The academy has the benefits of improving security and passenger experience on the ship of a Carnival Corporation operating line, as well as enhancing global maritime security. As stated by the president of the International Council of Cruise Lines, in reference to security concerns following September 11, “proper planning prevents poor performance;” Carnival’s centralized training academy aims to not only prevent poor performance, but also to ascertain excellence in performance and security (U.S. Department of Homeland Security and U.S. Coast Guard).

1.6 Information and Action Gaps

Through the literature review, numerous articles were found to discuss the background events and catalysts that have led maritime security to be a field of emerging significance. The literature review addresses key areas of concerns and cites specific ways that drug traffickers, human traffickers, and terrorists can use cruise and cargo ships as a means to inflict environmental, economic, or political harm. There is also abundant information on how domestic maritime policies have progressed since the terrorist attacks on the USS Cole and the attacks of September 11, 2001 and how these policy changes use technology and manpower to assert their effectiveness. Despite significant steps toward a more secure maritime domain, however, there are still areas of research in need of more information.

While there has been extensive research into enhancing port security and creating a supply chain of integrity for the maritime shipping network, there is a gap in research that analyzes how crewmembers are trained to comply with and
enforce policies and procedures, especially in the cruise industry, which transports more than 200 million people each year (U.S. Department of Homeland Security and U.S. Coast Guard). Because ship security personnel are entrusted with the duties of imposing regulations and standards, it is imperative that they have access to training in the knowledge, skills, and abilities their duties require. What constitutes this best training, how it should be designed, and how it should be carried out are areas of in need of exploration. Currently, there is a lack of information in the comparison of different security training methods presently used for cruise ship personnel, and there is a lack of action in trials and pilot studies of testing the application of different training programs. More specifically, different types of training procedures to be analyzed are whether an individual cruise or shipping line trains its security personnel or whether there is a centralized, corporate-wide training of multiple lines, and how these two different methods can affect security guard knowledge and performance.

Information and action gaps also include discrepancies of knowledge among different stakeholders. Private and government maritime industries, for example, may have different operational goals and different methods of providing a secure and resilient system. Even though private and government stakeholders in the maritime industry have different ends and means to these ends, they should all be afforded the same baseline knowledge of current security threats, ways to minimize these threats, methods of responding to the threats, and a
means to promote resilience following an attack. Maritime stakeholders can enhance global security by improving their individual security through common, shared knowledge.

Looking at a single cruise line or a corporation, composed of multiple cruise lines, can seem like small picture in comparison to the vast amount of cruise, cargo, and personal ships that make up the global maritime domain. Ascertaining the local and regional impacts of different security training methods for ship personnel, however, can have global benefits. Successful training academies can provide a framework for best management practices that can be altered and adopted by other cruise and shipping companies. Once the lack of information about the most effective security training practices is filled, research can delve further into an exploration of how positive changes in the cruise industry can have a multiplier effect and impact the global maritime domain.

Researching the design, curriculum, and implementation of a centralized security training academy is important because if successful, the academy can pave the way for new best management practices in the cruise industry, specifically, but also in the maritime industry as a whole. In today’s society, security measures and practices are not so secretive; what can improve the security of one company (or country) can be adopted by another company (or country), and each additional adoption of security can have a multiplier effect. Through the multiplier effect, one entity’s security improvements can improve the security of a physical region, or a part of an economic supply chain, both of which can result in greater international security. In this way, different stakeholders
benefit from sharing knowledge and best practices that will improve their protection from terrorist, piracy, or organized crime threats. In this specific research, because Carnival Corporation & plc is one of the largest in their industry, their corporate-wide security advancements have the potential to positively impact the cruise industry and the global maritime domain. Because of the potentially great benefits of this training academy, investigation of its design and development fulfill an interesting and important area of research that is currently deficient.
CHAPTER 2
GOALS AND OBJECTIVES

This project examined maritime policy and compliance from a corporate, private perspective, acknowledging that compliance can differ among stakeholders at public and private levels. It analyzed the multifaceted realm of maritime security, which incorporates environmental, economic, and legal constraints and considerations. The progression of security in the cruise industry from pre to post September 11, 2001 will also shed light on why security training is an important area of research. Through a history of events and attacks, the need for more stringent security arose and has become a topic of concern. The requirements and expectations for cruise ship security guards have increased, and this research of a centralized training academy aimed to positively change security guard training to reflect these heightened requirements and expectations. Thus, a major goal of this research was to design a training program that best prepares ship personnel for the vast array of global impending security concerns, in the financial and administrative confines of a corporation.

Because security can include protections that are physical, such as technology, and non-material, such as intelligence, another objective included identifying training components that covered both physical and non-material aspects of risks. For example, a potential training objective might be educating security guards in situational awareness, a form of information collection, that can provide crew preparedness for abnormal, and potentially threatening,
situations. Although background information has elicited a general progression of security threats from pre to post September 11, 2001, ongoing objectives of this research also included expanding upon documented threats to continually answer the questions of what threats the training academy proposes to mitigate and what different factors (policy, technology, education, etc) comprise security.

Specific academy objectives included obtaining a facility for the academy and designing a training curriculum applicable to all cruise ship security personnel of Carnival Corporation’s ten different cruise lines, headquartered in different countries with different geographical travel destinations. In choosing a facility, the major goal was matching up physical location needs, such as ample space to feed and lodge trainees. It was also important that the location facilitates classroom and field exercises recommended by the curriculum. Designing the curriculum required research of domestic and foreign maritime law and policy, with acknowledgment of different maritime environments at port, in territorial waters, and in the international high seas. Policy research had a goal of providing a global perspective, in addition to identifying what is legally required of the academy and what additional procedures and policies should be taught to fulfill the Corporation’s goal of having an effective training academy that desires to mitigate threats to maritime security.

While designing the academy itself, research objectives included looking at current training methods employed in the maritime industry and what, if any, other methods have been tested. The academy delivery was designed to consist of a potential combination of the following: hard copy manuals, PowerPoint
presentations, lectures, audio or movie supplements, interactive role-play in
simulations, field exercises, and/or a final exam. An additional objective included
looking at requirements and skill sets necessitated by security guards in other
arenas, like the military and law enforcement, and research incorporated some of
these factors into possible course components.

The design of the curriculum and how it is carried out in the academy,
which aims to be up and fully running sometime in 2012, aimed to apply maritime
policy to real world security issues, while taking into consideration constraints of
a private entity, like economic, environmental, and legal limitations. After
planning the curriculum and academy logistics, future research goals could
include assessing the effectiveness of this type of corporate-wide training in
comparison to previous practices by the individual cruise lines. Future goals and
objectives also include looking for a multiplier effect of how enhanced security on
a regional scale can potentially impact the global maritime domain. This study
can pave the way for supplementary research into the social side of security
training, such as comparisons of cruise ship security guards understanding of
policies and regulations from different training procedures, including personnel
perceptions of the academy’s effectiveness and their understanding and
preferences for various types of training programs, among others.
Security training in the cruise industry is an area of significance because of the world that exists today; without adequate protection from human traffickers, drug traffickers, pirates, and terrorists, the maritime domain would not be able to successfully facilitate international trade and travel to sustain the globalized economy that presently prevails. Although this protection can take place through human and technological means, it cannot reach its maximum effectiveness unless those whose duty it is to implement and enforce security measures understand and value its importance. Consequently, it is important to research new types of training methods with hopes of ensuring that legal frameworks and policies are most efficiently implemented.

This research is significant in its goals to explore maritime security as a broad and interdisciplinary topic, which encompasses not only passenger safety, but also relatively new security threats of terrorism and piracy. These threats not only compromise security, but they play a significant role in economic and environmental terms. Security threats can present themselves as biological or chemical weapons that have the intention of posing threats to human life and safety; however, a large scale attack with biological or chemical weapons can pollute and negatively impact the composition of ocean waters and marine organisms. Additional environmental concerns that can affect ship navigation and port operations include invasive species introduced from ballast water and
endangered species. While these are mostly logistical concerns, changes in a ship’s route or operations could require heightened awareness for security risks and threats. Because of an overlap among different factors and concerns, this research showed that training (and improved maritime security) has additional benefits applicable to the global maritime domain. Improved security training can also improve crew responses to actual threats and attacks; faster response times and better decisions allow for greater resilience of the industry to recover and return to normal operating procedures, without a large economic burden from a halt in day to day port or cruise operations.

Research limitations include the difficulty to assess the effectiveness of the training academy; the academy will not be fully operational until at least months after its design. If a pilot study of this training academy is able to take place during the course of this research, the study will be a controlled experiment to some degree, and this may not be entirely representative of real world situations or outcomes. Curriculum design and execution may be physically limited by facility size, location, and ability to conduct field and hands-on exercises. Moreover, despite extensive planning, the lifetimes of the curriculum and of the academy are uncertain; because law and policy can change rapidly (as evidence by sweeping changes in security precautions following September 11, 2001), the existence of such an academy and its success is undefined.

Limitations also arise when considering different levels of intelligence and different financial capabilities of public and private stakeholders. This specific research was limited to available information of security threats based on public
information accessible through the worldwide net and those available from Carnival Corporation & plc. Some information available to the Corporation, which helped form the academy training, was for “Official Use Only.” Also, in terms of intelligence availability, the federal government may have increased access to security information compared to local government, state government, and private corporations; this can limit what types of threats can be protected against. Specifically within the study of Carnival Corporation & plc, there are regulations that prohibit this research from disclosing some detailed information to the public. If the academy is a success, which is dependent on its debut after the conclusion of this research, there may be limitations to the feasibility of its application to and adoption by other industries and countries. In a more general perspective, limitations to global maritime security include the voluntary treaties of the IMO. Because IMO membership is voluntary, there are countries that have not ratified every IMO convention, which limits the distance that security, crew, and vessel regulations extend; this means that much of global maritime security still rests within state governments and their commitment to reducing security threats.
CHAPTER 4
METHODS

The research took place at Carnival Corporation & plc U.S. headquarters, located at 3655 NW 87th Avenue, Miami FL, 33178. Research was also reviewed at a Security Review Group (SRG) meeting in Newport, Rhode Island. Research included the utilization of online and hardcopy resources to design academy curriculum. Assessment of potential locations of academy facilities located in India and the Philippines, with a goal of one academy in each country, was implemented; research and assessment of the facilities were not a major objective of this study. Potential facility sites in the Philippines were located in Manila and Subic Bay, and potential sites in India were located in Mumbai.

4.1 Analysis of Standards and Policies at Domestic (U.S.) and International Levels

Training curriculum research reviewed relevant policy and literature review, including data publicly available from the maritime industry. Domestic (U.S.) policies reviewed were: the Maritime Transportation Security Act (MTSA), the Cruise Vessel Security and Safety Act (CVSSA), the Security and Accountability for Every Port Act (SAFE Port Act), the Coast Guard Naval and Vessel Inspection Circulars (NVIC), and the Executive Order: Blocking Property of Certain Persons Contributing to the Conflict in Somalia of 2010.

Although not exclusive to the maritime industry, this research also investigated general skill sets and specific security duties required and
recommended of security guards in other industries. The U.S. organizations and agencies researched for such information were: the New York State Office of Homeland Security: Preparedness Training Catalog for Law Enforcement; the U.S. Department of State: Security Overseas Seminar; the U.S. Department of State: Advanced Security Overseas Seminar; the U.S. Military; U.S. Department of Defense; and the U.S. Department of State: Foreign Service Officer Qualifications. An additional piece of legislation, again not specific to the maritime industry, reviewed in its domestic security applications was the Federal Information Security Management Act of 2002.

International policies reviewed were standards developed either by an international organization, like the IMO, or standards that had an international scope of application, such as best management practices for the global maritime industry. The policies this study reviewed include: the International Convention for the Safety of Life at Sea (SOLAS); the International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers (STCW); the International Ship and Port Facility Security Code (ISPS); Measures to Prevent Unlawful Acts against Passengers and Crew On Board Ships; and Measures to Prevent Unlawful Acts Which Threaten the Safety of Ships and the Security of Their Passengers and Crews. Other policies briefly reviewed but not focused on because of their limited applicability in security aspects include: the United Nations Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA), International Convention on Maritime Search and Rescue (SAR), and the United Nations Convention on the Law of the Sea
(UNCLOS). These conventions were not extensively analyzed because their focus on security was limited; more specifically, SUA, even though it addresses specific actions that threaten ship safety and security, did not further expand on training practices to circumvent unlawful actions.

Additional domestic, foreign, and international practices reviewed include: the U.S. Coast Guard Marine Safety Manual; TSA Maritime Security/Transportation Security Training; TSA Port Security Training Exercise Program (PortSTEP); Coast Guard Area Maritime Security and Exercise Program (AMSTEP); FBI Guide to Cruise Line Crime Scene Preservation; Paris Memorandum of Understanding (MoU) on Port State Control; European Union Regulation No. 725/2004; Best Management Practices of Protection against Somalia Based Piracy – Version 4 (BMP4); Inter-American Port Security Training Program: Regional Course on Port Security for Caribbean Countries; the Philippine Overseas Employment Administration: Mandatory Anti-Piracy Awareness Training for Seafarers; and India’s Ship Security Awareness Course.

This study specifically identified components of these laws and policies that are required for maritime security training, components that are recommended, and components that are optional; this categorization is further described later in this section. To begin, each policy was outlined and its major requirements and topics of concern were broken out in the outline. After each policy was outlined, the policy components were compared and contrasted with one another as a way to compile a comprehensive list of all components, whether they were required or recommended by policy, model course
frameworks, or stakeholders. These components were organized by a combination of the following: which policy or stakeholder developed, requires, recommends, and/or actively applies the component.

The policy and stakeholder categories were divided into: IMO, ISPS, U.S., EU, and other. IMO consisted of different IMO conventions, measures, and model courses. It also consisted of BMP4, which although not created or distributed by the IMO, was categorized there because of its international scope. ISPS was broken out separately from IMO because of its extreme significance to maritime security. The U.S. consisted of MTSA, CVSSA, SAFE Port Act, NVICs, model courses from these policies, and other U.S. agencies, though not specific to the maritime domain, such as the U.S. Department of Defense and U.S. Department of State. The EU consisted of policies from the UK, the Netherlands, and Italy; the Paris MoU; and EU Regulation NO 725/2004. The final category, labeled “Other,” consisted of non-EU flag states (including Panama and the Bahamas), Filipino requirements, Indian maritime policies, and the Inter-American Port Security Training Program. This section was specific to this research, and it is reflective of training facility sites and flag states used by Carnival Corporation.

The comprehensive list of training components, a result of policy and model course comparisons, was formatted into a table that depicted the component and where it is regulated and/or recommended, as defined by the categories previously described. This table formed the topic development matrix, which would then be used in developing a course syllabus. The topic
development matrix is visible in Table 4, and it lists all the training components as required or recommended by policy and model course frameworks. The potential training components were then broken into a list format which identified core, recommended, and optional training components for potential use in Carnival’s curriculum. Core components were used by 4-5 of the five categories; recommended components were used by 3 of the five categories; and optional components were used by 1-2 of the five categories.

Core elements were automatically included into the curriculum as course topics, while non-required elements were further reviewed in order to determine whether or not they should be a part of the curriculum. Recommended training elements potentially provided for greater security, but because a longer course syllabus created a longer academy, the cost of adding recommended or optional elements needed to be justifiable. This research also aided in policy analysis, which determined how policy strengths and requirements were incorporated into a training curriculum, while identifying policy weaknesses.

Relevant legislation and policy as a part of curriculum research and design provided a more informed background of why security is needed and how security duties have progressed over time. In addition to applicable domestic and international regulations, a review of background and historical events, such September 11th, the attack on the USS Cole, and the attack on the Achille Lauro, gave insight into the motivation behind the academy and provided for use as possible case study analysis in the curriculum. Event analysis aimed to consider known organized crime, political unrest, previous maritime terrorist attacks, and
acts of piracy. Historic and current event analysis, coupled with domestic legal framework and international convention standards, helped shape training and provided for a widespread global perspective. Legally mandated requirements, such as regulations of the MTSA, provided the backbone for the topic development matrix, which was augmented by specific requirements from operating lines’ flag states, as well as the locations of the academy facility. Ship registry included the following flag states: the Netherlands, the Bahamas, Bermuda, Panama, the United Kingdom, and Italy. This topic development matrix was reviewed and edited to ultimately form a detailed academy syllabus, which was reflective of the constraints of the facility, as well as time considerations.

Table 4 – Topic development matrix

<table>
<thead>
<tr>
<th>Topic</th>
<th>IMO</th>
<th>ISPS</th>
<th>EU</th>
<th>US</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal issues</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>ISPS</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Threat identification and mitigation</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Definitions and clarifications of duties</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Watchstanding and patrols</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Searches and inspections</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Ship security assessment and plan</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Port facility security</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Drills and exercises</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Criminal response</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>procedures</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Crowd management</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Self defense</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Documentation:</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>incident reporting and</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>record keeping</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information and</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>intelligence gathering</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>and exchange</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information security,</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>confidentiality, and</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sensitivity</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Piracy</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hostage survival</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Radiation protection</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 4.2 Analysis of Existing Training Curricula for Maritime Industries

Model course frameworks reviewed include: the MTSA Model Course Frameworks, CVSSA Model Course 11-01; IMO Model Course 1.28: Crowd Management, Passenger Safety and Safety Training for Personnel Providing Direct Services to Passengers in Passenger Spaces; IMO Model Course 1.29: Proficiency in Crisis Management and Human Behavior Training Including Passenger Safety, Cargo Safety, and Hull Integrity Training; and IMO Model Course 3.19: Ship Security Officer.

Current security training manuals and syllabi used by the operating lines also aided in the development of the training syllabus. The operating lines who

The review of the above materials helped to determine suggested time frames for specific course topics, opportunities for supplemental course materials, and opportunities for practical training. Materials were analyzed for their strengths and weakness, and design incorporated the strengths in the academy curriculum and proposed to reform potential weaknesses. These frameworks also gave insight into additional training practices that may not be legally mandated, but were categorized as recommended or optional because they provided for a prepared and knowledgeable security crew. Course frameworks were used to determine appropriate theoretical and practical mediums for course instruction and potential methods for evaluation of security
personnel comprehension of material. All materials, including models stemming from legislation, and current syllabi of the operating lines, were analyzed for their strengths and weaknesses.

Analysis of current suggested training techniques and methods, within Carnival Corporation and in the maritime industry as a whole, were explored in order to pursue best management practices. To further seek out best management practices, investigation of skill set requirements among security guard positions outside of the maritime industry provided a broad view of available practices and resources for adaption to Carnival’s academy. Although not all of the skill sets and requirements in non-industry related training pertained to the academy’s projected curriculum, some of these factors could be used to enhance the recruitment process for security positions. Additionally, table-top learning in comparison to field exercises was analyzed with respect to each topic of training, in order to determine which topics were best instructed in which medium.

4.3 Specific Needs of Carnival Corporation & plc

Carnival Corporation & plc needed one academy facility located in the Philippines and one located in India. Because the Philippines and India are countries with large marine and naval cultures, Carnival Corporation & plc obtains a majority of their ship security personnel from these two countries. It was most logical to have a training facility where the security personnel originate from, and it was likely to be less expensive than a facility located in the U.S. In choosing a location to conduct the training, facility options were evaluated based
on the following: quality of local instructors and businesses, ability to let Carnival provide its own instructors and curriculum, spatial capacity to lodge and feed personnel, ability to conduct field exercises, and feasibility of these activities. Because the locations of the facilities will be neither Corporate nor operating line headquarters, research also examined if the Philippines and India have specific maritime security training requirements. Carnival Corporation & plc aimed for the centralized training academy to be about one week (five business days) in duration. Additional operating line-specific training planned to occur immediately following the academy for an extra three to five days, as needed. The total time spent at the training facility was estimated to be one to two weeks, but it was ultimately dependent on the length of the academy syllabus.

The curriculum for the centralized training academy also incorporated suggestions and feedback from the Security Review Group (SRG), which is comprised of Company Security Officers (CSO) from every operating line and chaired by the Corporation’s Director of Maritime Security. The SRG, especially during their meeting on September 15-16, was a resource for information, review, and discussion. At this meeting, present curriculum research, in terms of benchmarking domestic, foreign, and international maritime regulations and recommendations, was presented and reviewed. Comments were obtained about additional policies to research, and the meeting, as a whole, helped to provide further insight for curriculum consideration.
4.4 Design and Development of Carnival Corporation & plc’s Centralized Training Academy

Curriculum research was accomplished following these steps: (1) development of a rationale for training, (2) determination of necessary knowledge and skill sets for security guards, (3) identification of tasks for security guards and training objectives, (4) domestic and international policy and model course framework analysis, (5) creation of a topic development matrix, (6) formation of a detailed session plan, and (7) a review of products accomplished at each step by the SRG. A visual representation of these steps can be seen in Figure 7. The topic development matrix can be seen in Table 3. Curriculum research entailed the creation of a comprehensive list of required training policies, as mandated by domestic and international law. In addition to these legal requirements, additional research resulted in a list of other possible training requirements that are not legally mandated, but could allow for an efficient training academy that meets the Corporation’s expectations of enhancing ship security. Training aimed to extend beyond the minimum regulations that are mandated by legislation or international conventions; an all-encompassing training curriculum considered and adopted additional recommended topics with the goal of producing security personnel who have the abilities to detect, deter, and respond to security threats and incidents.
4.5 Pilot Study and Centralized Training Academy Evaluation

A pilot simulation of the academy intended to be conducted if time and resources were permitting, and the execution and outcome of the simulation would then be analyzed to ensure the proposed academy is fulfilling Carnival’s expectations. The pilot simulation aimed to run a few security personnel through the academy; ideally, the pilot simulation should encompass the entire duration of the training academy, but if this is not possible, at least one training day should be simulated. A pilot study would allow for a preliminary evaluation of the centralized training academy to answer the questions:

Figure 7 – A flow chart depicting the design and development process of the centralized training academy
1. Are the logistics of the academy practical?

2. Are the training topics and course objectives easily understood by personnel?

3. Do field exercises and lectures adequately complement their respective curriculum topic?

4. Does the academy fulfill the needs of the Corporation’s goals and a general need to enhance maritime security?

5. Is this academy an appropriate match for Corporate and operating line resources?

Other potential areas of academy evaluation include: a comparison of corporate and individual operating line training methods and the assessment of prospective regional, industry, and global impacts of a centralized training academy in the maritime domain.

4.6 Cost Analysis of the Centralized Training Academy

Because of the proprietary nature of the centralized training academy, a generalized analysis looked at costs and benefits of the entire global maritime domain. General considerations applicable to the maritime industry included looking at logistical benefits of training that takes place at a centralized academy, in comparison to training onboard a ship, which would represent on the job training. Because a centralized security training academy could apply to shipping lines, cruise lines, or ports, the analysis generalized the benefits of such a program, although it sought out a specific example that would have detailed figures to aid in understanding potential benefits. A cost analysis was important
to consider as both passengers and businesses have choices among which cruise or shipping lines they use. Because the civilian maritime industry does have commercial interests, it is important to evaluate whether choices, such as a centralized security training academy, are effective uses of industry resources.

A cost analysis for a centralized training academy could consider the major components of the program, which are the facility and the curriculum. The location of the academy should be analyzed to consider its abilities and costs to facilitate: theoretical and practical training elements; the option of a company supplying their own instructors and materials; and the capabilities of lodging and feeding students. These costs are likely to vary based on the amount of students attending the academy, the length of the course, and the type of field exercises conducted. For example, a facility may have certain security equipment onsite, but may need to specially order additional equipment or systems. Another option for future consideration is whether to add additional training offered at the same academy. Examples of additional training include: Ship Security Officer (SSO) training and refresher training. These additions would require further analysis of costs and benefits.
CHAPTER 5

RESULTS

5.1 Analysis of Domestic, International, and Other Standards and Policies

Table 5 summarizes major domestic, international, and foreign policies reviewed, including where they are applied and key notes about their application or contents.

Table 5 – Summary of major policies reviewed

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Abbreviation</th>
<th>Place of Application</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maritime Transportation Security Act</td>
<td>MTSA</td>
<td>U.S.</td>
<td>Mandatory implementation of ISPS</td>
</tr>
<tr>
<td>Cruise Vessel Security and Safety Act</td>
<td>CVSSA</td>
<td>U.S.</td>
<td>Focus is on criminal activities</td>
</tr>
<tr>
<td>Security and Accountability for Every Port Act</td>
<td>SAFE Port Act</td>
<td>U.S.</td>
<td>Limited applications to cruise ships</td>
</tr>
<tr>
<td>Coast Guard Naval and Vessel Inspection Circulars</td>
<td>NVIC</td>
<td>U.S.</td>
<td>Give recommendatory guidance; not U.S. law</td>
</tr>
<tr>
<td>Coast Guard 33 Code of Federal Regulations</td>
<td>CFR</td>
<td>U.S.</td>
<td>Discusses MARSEC Levels</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>-----------------------------------------------------------------</td>
</tr>
<tr>
<td>Executive Order: Blocking Property of Certain Persons</td>
<td>U.S.</td>
<td></td>
<td>Full force of enforceable law; highlights the need for anti-piracy</td>
</tr>
<tr>
<td>Contributing to the Conflict in Somalia of 2010</td>
<td></td>
<td></td>
<td>measures</td>
</tr>
<tr>
<td>International Convention for the Safety of Life at Sea</td>
<td>SOLAS</td>
<td>International</td>
<td>Contains the ISPS Code</td>
</tr>
<tr>
<td>International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers</td>
<td>STCW</td>
<td>International</td>
<td>Contains the 2010 Manila Amendments which require training in preparation of piracy</td>
</tr>
<tr>
<td>International Ship and Port Facility Security Code</td>
<td>ISPS</td>
<td>International</td>
<td>Contained in SOLAS; Part A of the code is mandatory and Part B is recommendatory</td>
</tr>
<tr>
<td>Paris Memorandum of Understanding of Port State Control</td>
<td>Paris MoU</td>
<td>27 European Countries</td>
<td>Enhances port state control for ship inspections, detainment, and banning</td>
</tr>
<tr>
<td>EU Regulation No 725/2004</td>
<td>European Union</td>
<td></td>
<td>Mandates parts of ISPS’s recommendatory Part B</td>
</tr>
<tr>
<td>Mandatory Anti-Piracy Awareness Training for Seafarers</td>
<td>Philippines and International</td>
<td></td>
<td>Required for all Filipino seafarers regardless of ship’s route</td>
</tr>
</tbody>
</table>
### 5.1.1 Domestic

The MSTA and CVSSA were extensively examined, noting their key components and requirements. The major relevant requirements of the MTSA are: conducting vulnerability assessments for port facilities and vessels; developing security plans to mitigate identified risks for the national maritime system, ports, port facilities, and vessels; developing the Transportation Worker Identification Credential (TWIC), a biometric identification card to help restrict access to secure areas to only authorized personnel; and establishing a process to assess foreign ports, from which vessels depart on voyages to the U.S. The first two requirements (vulnerability assessments and security plans) are especially important because they come from the ISPS. Some major relevant requirements of the CVSSA are: maintenance of video surveillance on passenger vessels and crew training in the prevention, detection, preservation, and reporting of criminal activities in the international maritime environment.

The SAFE Port Act was not as heavily analyzed because it was found to apply more to port facilities and cargo ships than passenger vessels. The major relevant applications were the implementation schedule of TWIC and the role of CBP. Other policies reviewed include the Coast Guard 33 Code of Federal Regulations (CFR), the Coast Guard NVIC 03-07, and the Executive Order: Blocking Property of Certain Persons Contributing to the Conflict in Somalia of 2010. The CFR discusses Maritime Security (MARSEC) Levels and port-facility-vessel communications; the 03-07 NVIC gives guidance on TWIC.
implementation; and the Executive Order gives directives for those who may be affected (such as passenger ships traveling in high risk areas) by piracy.

Each piece of domestic policy researched had strengths and weaknesses. A prominent strength of U.S. legislative policies, laws, and presidential executive orders is their ability to be enforced by the U.S. government and its respective agencies. More specifically, MTSA provides a mandatory domestic implementation of the IMO’s ISPS Code, through Section 109, “Maritime security professional training.” Although the legislation itself can be considered vague in its requirement of minimum standards that should be afforded to maritime security personnel, it gains strength where it requires, no later than six months after the MTSA is enacted, that the Secretary of Transportation develop a model course framework that depicts the standards and curriculum the law is referencing. The Secretary delegated these responsibilities to MARAD, who appointed the course development to the U.S. Merchant Marine Academy. The MTSA model course framework will be analyzed independently, but its existence as a means to help companies and ships comply with the law is seen as a strength.

The CVSSA is strong in its listing of specific measures ships and crewmembers should undertake to enhance passenger safety and security. Examples of these specifics include: ship rails at least 42 inches above the cabin deck; rooms equipped with a means of visual identification (such as peep holes); and rooms with security latches and time-sensitive key technology. The CVSSA also supports technology, if available, to aid in detection of passengers who may
have jumped or fallen overboard and to aid in communication operations, such as with an acoustic hailing device, in high risk areas. For the prevention and detection of criminal activities, the Act requires the maintenance of a video surveillance system; and for the response to criminal activities, the Act requires specific procedures, if and when criminal and sexual attacks occur. Similar to the MTSA, the CVSSA charged the Secretary to develop specific training plans that comply with the new legislative requirements. The CVSSA model course framework will be analyzed independently, but it again shows strength in its ability to transform legislative requirements into specific training curriculum for easier application in the industry.

The SAFE Port Act has strengths in its detailing of specific measures on how to enhance port and cargo security. The Act cites specific measures to be taken, such as the formation of TWIC, the creation of interagency operational centers, the Container Security Initiative (CSI), and the Customs Trade Partnership against Terrorism (CTPAT). These specific measures prevent the Act from being a series of vague requirements of enhanced security, without plans to execute enhanced security. A notable weakness of the SAFE Port Act is its limited applications to cruise ships. While cruise lines and ship security personnel do have communications with port facilities, the SAFE Port Act focuses on container security for the shipping industry. Specific port facility security plans, such as TWIC and background checks, have the opportunity to improve the security of cruise operations, but ship personnel, the majority of whom are not U.S. citizens, are not likely to fully understand TWIC because it is
beyond the realm of their assigned duties. Although the port facility security measures in this act do not specifically reference the cruise industry, they do offer a starting point for standardization of security policies at all U.S. ports, and such standardization can offer spillover effects. If U.S. ports are safer, perhaps cruise ships arriving at and departing from those ports will also be more safe and secure, as they try to comply with more stringent standards.

NVICs are not U.S. law, and they are not enforceable. Despite this pronounced weakness, NVICs offer recommendatory guidance, sometimes on how to comply with industry regulations, which are enforced by law. NVICs have strong internal benefits within the Coast Guard and other enforcing bodies; non-compliance with a NVIC indicates a potential non-compliance with maritime law, and thus can guide Coast Guard efforts to heighten their awareness of suspicious parties in non-compliance. NVICs are not specifically security or training related, as these are concerned mainly with issues of vessel construction, manning requirements, and special hazards.

Executive orders, which come via the President of the U.S., have the full force of enforceable law. The particular executive order researched was the Executive Order: Blocking Property of Certain Persons Contributing to the Conflict in Somalia of 2010. This was researched as an element of piracy, a threat which poses potential danger to ships traveling in high risk areas. In this research the law represents its strength by justifying the need to train seafarers for all risks and threats, including recent ones such as piracy. However, while all U.S. legislation has the potential to be strong with the ability to be enforceable in
terrestrial waters, it has limitations in the international realm of the maritime domain. Ships are likely to prioritize their flag state procedures, which may vary from U.S. law.

Additional domestic research included investigation into standards for security guards outside of the maritime industry. Research yielded several training topics that had not appeared widely in other research but could be considered for incorporation into the academy’s curriculum. These training topics were: suicide bombing prevention and awareness; counterintelligence; foreign intelligence; hostage survival; information technology security; and general skills and qualities required for Foreign Service officers. These topics came from research into the following agencies and programs: the New York State Office of Homeland Security: Preparedness Training Catalog for Law Enforcement; the U.S. Department of State Security Overseas Seminar and Advanced Security Overseas Seminar; Technical Surveillance Counter-Measures (TSCM) used by the U.S. Military and U.S. Department of Defense; review of the Federal Information Security Management Act of 2002 as implemented by the U.S. Department of State; and the U.S. Department of State Foreign Service Officer Qualifications. Many of these measures had strengths in their general applications to security domain, however, limitations as to how they could be effectively implemented in the curriculum and applied in the maritime domain were potential weaknesses for the purpose of this research, as well as when considering the potential cost of lengthening the academy.
5.1.2 International

Following review and analysis of domestic law, research then examined international regulations for the maritime industry. Although there are a plethora of conventions and codes, research was narrowed to those policies specific to security, however sometimes the distinction between safety and security was blurred. The major international policies applicable to security are: SOLAS, which includes ISPS; STCW; the Paris MoU; additional IMO measures which were later incorporated to conventions; and BMP4. Other policies reviewed and not deemed extremely applicable to security training objectives of this research were: SAR; the International Safety Management (ISM) Code; International Regulations for Preventing Collisions at Sea; and SUA.

The major relevant requirement of SOLAS is the ISPS Code. Part A of ISPS is required, and Part B is recommendatory implementation measures of Part A. The functional requirements of Part A are: the gathering, assessing, and exchanging information; maintenance of communication protocols; prevention of unauthorized access to ships and restricted areas; prevention of unauthorized weapons, incendiary devices, or explosives; establishment of security levels; a Declaration of Security; a Ship Security Assessment; a Ship Security Plan, based on assessments; record keeping and including a means for alarm in event of a threat or incident; appointment of a CSO and a SSO; training, drills, and exercises, related to security plans and procedures; and verification and certification for ships. The specific security levels in accordance with ISPS are: (1) Normal operating level of minimum appropriate protective measures; (2)
Heightened risk of a security incident, with additional protective security measures; and (3) Probable or imminent risk of a security incident with further specific protective security measures for a limited period of time.

The major relevant requirements of STCW are: provisions on port state control and the 2010 Manila Amendments, which require crew training for preparation against piracy. The major relevant components of the Paris MoU are the rights of inspections by port states and the classification of passenger vessels as high risk. The relevant guidelines of IMO Measures to Prevent Unlawful Acts against Passengers and Crews on Board Ships and Measures to Prevent Unlawful Acts Which Threaten the Safety of Ships and the Security of Their Passengers and Crews are presently incorporated into ISPS. The relevant guidelines of BMP4 include: ship risk assessment; reporting procedures; company and ship master planning; ship protection measures; and guidelines for response during an attack.

The IMO’s conventions that pertain the most to maritime security, SOLAS and STCW, have similar strengths and weaknesses. Both are strong in the vast international realm they cover, although they are only as strong as the countries that choose to adopt and enforce them, since the IMO lacks regulatory powers. Both conventions also appear to acknowledge the overlap between safety and security issues; treating both issues as necessary measures to sustain the wellbeing of a cruise ship can be a strength, but only if the distinct differences of risks and threats of safety and security issues are further analyzed. However, because ship, passenger, and crew safety has been an issue in international
discussion since 1914, SOLAS is not the only piece of policy that needs to be considered. IMO has developed many other codes and conventions, such as SUA, SAR, and ISM, which apply mainly to safety concerns. This leaves ship owners and those who design maritime security training courses with a plethora of international policy to review. Extensive regulations and recommendations, in addition to overlap of conventions that deal with safety and security issues, are potential weaknesses, in consideration of the time and effort it takes to research all existing IMO materials. SOLAS can be particularly perplexing in that its name indicates it deals with safety at sea, but it also includes the ISPS code, which is focused on security.

When analyzed independently of SOLAS, ISPS is strong in its two divisions: Part A, which is mandatory, and Part B, which is recommendatory guidance. ISPS clearly indicates what ships and companies need to do to enhance security, and it enhances strengths of some non-specific requirements by recommending specific methods in Part B that fulfill Part A’s necessary obligations. Because of its overwhelming presence in facilitating port and ship security, perhaps it would be more beneficial if ISPS was separate from SOLAS. IMO’s additional and supplementary materials, such as its measures and resolutions, have mostly been incorporated into other codes and conventions; this can again be confusing as to why these measures or resolutions continue to stand as independent documents when, conceptually, they are not so.

International policies outside of the IMO, mainly the Paris MoU and BMP4, have strength in their ability to show that the IMO is not the only international
force, albeit the main one, to develop maritime policies. While the Paris MoU is specific to European countries, other MoUs have been developed and adopted to enhance port states authorities of inspections; these MoUs are specific to the geographic region of their signatories. Like IMO conventions, they are only as powerful as their design if they are implemented and enforced as such. Because there are different, geographically based, versions of MoUs on port state control, this lack of standardization in an international world of trade and travel can be a potential weakness, especially for ship companies or cruise lines that are not confined to one specific region of the world.

BMP4, which is supported by many stakeholders in the maritime industry, is successful in terms of its outreach and education of piracy tactics in high-risk areas. It describes what factors are likely to lead to a successful attack, in comparison to what ship and crew measures should be taken before and during transit that can prevent a successful attack. It is very specific in its nature, and it is a comprehensive compilation of best practices in the maritime domain. BMP4 also provides a detailed way for ship companies to comply with the vague requirements of anti-piracy training under STCW’s 2010 Manila Amendments. Best industry practices, published and disseminated, can successfully prevent piracy attacks and enhance global maritime security. Because piracy is constantly evolving, and geographically expanding, best management practices need to be dynamic. It is also important for those who implement BMP4 to know that it was established based on known patterns, but it does not imply piracy tactics are static or that implementing BMP4 will completely prevent any attacks.
5.1.3 Other

Other maritime policies and legislation needed to be researched for the flag states in which Carnival Corporation & plc’s ships are registered. The following flag states were researched regarding relevant information about their implementation of ISPS and the possibility of additional maritime policies: the Bahamas, Panama, the United Kingdom (UK), the Netherlands, and Italy; Bermuda was grouped with the UK. The locations of the academy facilities, the Philippines and India, were also researched for their respective maritime policies. The Bahamas, Panama, the UK, the Netherlands, and Italy all actively implement ISPS. The UK, via Bermuda legislation, also follows the Maritime Security Act of 1997. The UK also abides by the Aviation and Maritime Security Act of 1990 and the Terrorism Act of 2000, in addition to procedures and legislation specific to criminal activities. Countries of the European Union also are required to comply with the EU Regulation No 725/2004. India does not have additional legislation, but it practices a Ship Security Awareness Course that covers ISPS and the threat of piracy. The Philippines do have a specific requirement directed by the Philippine Overseas Employment Administration; the requirement is for Mandatory Anti-Piracy Awareness Training for Seafarers, regardless of a ship’s proposed destination.

Most of the flag states that Carnival Corporation & plc ships are registered with do not have additional maritime security legislation beyond ISPS. Bermuda’s Maritime Security Act of 1997 criminalizes offenses to ships that jeopardize safety and security, such as hijackings, destruction of ships, or navigation
hazards. The Act also discusses Bermuda-specific restriction zones and searches in harbor. While this act may clarify safety and security concerns, it is unlike ISPS in its lack of requiring specific measures taken by the crew and ship to enhance awareness and protective measures. The UK also implemented the Aviation and Maritime Security Act of 1990 and the Terrorism Act of 2000. The Aviation and Maritime Security Act gives powers to the Secretary of State, such as requesting information and conducting searches, to prevent safety and security threats to passenger ships. It specifies acts, such as hijackings, which are threats to ships or fixed platforms, but again unlike ISPS, it does not require explicit procedures to be undertaken by the ship’s crew. The Terrorism Act is not maritime specific, and its focus is to define terrorism and to extend police powers when threats are perceived. Since this Act, the UK has developed several other acts that further define and seek to prevent terrorist acts. None of these additional acts have been specific to the maritime industry, but are they implemented onboard UK-flagged vessels to prevent terrorism and provide appropriate agency contact and responses if and when they occur. These pieces of UK legislation seem to exist mostly to specifically identify and criminalize certain threats to vessels, but their purpose does not seem to be establishing specific regulations or recommendations for crews to protect against the illegal acts. These acts, however, do give the UK power to search ships as a means to ensure safety and security, and this can be seen as policy strength.

The EU Regulation No 725/2004 was developed to mandate parts of ISPS that, through the IMO, are only recommendatory guidance, rather than strict
regulations. As mentioned previously, ISPS is divided into mandatory regulations in Part A and suggestive guidance in Part B. This EU regulation takes certain sections in Part B and makes them mandatory for the European community. This policy is able to enhance security in European waters, and because the new regulations are taken from Part B of ISPS, which is designed and written in an unambiguous way, they are not vague or open to extreme interpretation. Although the new regulations may be implemented slightly differently on passenger and cargo ships, they offer another level of standardization in the maritime industry, for ports and ships. However, this standardization only applies to the EU, and there still exist variances in global methods to enhance maritime security.

The final piece of foreign legislation analyzed is the requirement of anti-piracy training for all Filipino seafarers, regardless of their destinations. The Philippine Overseas Employment Administration developed this requirement, and it applies to this research because Carnival Corporation & plc receives a large amount of security crew from the Philippines, and it was also chosen as a potential site to facilitate the centralized training academy. There is a brief course outline available for demonstrating training topics would be compliant with the mandatory anti-piracy training. It does not go into much detail, but it outlines key topics and subtopics that should be addressed, with respect to piracy. Some of these topics include an introduction, planning prior to transit, procedures when the ship is in-transit, contingency plans if attacked, and post-incident responses and actions. These specific topics pave the way for this general regulation to be
implemented in the industry, although it is not as detailed as BMP4. Because the Philippines produce many seafarers in the maritime industry, this regulation positively impacts many cruise and shipping lines. A summary of these foreign policy results can be found in Table 6.

Table 6 – Summary of foreign standards and policies reviewed

<table>
<thead>
<tr>
<th>Policy</th>
<th>Place of Application</th>
<th>Maritime Specific</th>
<th>Crime</th>
<th>Terrorism</th>
<th>Piracy and/or Hijackings</th>
<th>Extensions in Authority</th>
<th>ISPS, Part B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maritime Security Act of 1997</td>
<td>Bermuda</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Aviation and Maritime Security Act of 1990</td>
<td>United Kingdom</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Terrorism Act of 2000</td>
<td>United Kingdom</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Regulation No 725/2004</td>
<td>European Union</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Mandatory Anti-Piracy Awareness Training</td>
<td>The Philippines and all Filipino seafarers</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Notes: Crime includes onboard crimes, crimes at sea, and crimes at port; Extensions in authority include enhanced police and/or port authority powers, such as searches and inspections; ISPS Part B does not refer to Part B in its entirety, but those sections of Part B referred to in Regulation No 725/2004

5.2 Analysis of Existing Training Curricula for Maritime Industries

Existing training curricula in the maritime industry was analyzed for strengths and weaknesses as it was reviewed for possible incorporation into the
syllabus design for the centralized training academy. The training curricula from the operating lines of Carnival Corporation & plc will not be individually analyzed in this research; because of the secure and classified nature of the documents, specific analysis for strengths and weaknesses cannot be done without compromising the security of the materials. Unlike the MTSA, CVSSA, and IMO model courses, the training materials of the operating lines were not publically available documents.

As a result of MTSA, there are various model course frameworks available for industry use and adaptation. Because there are so many, however, it can be difficult for a company to ensure they are picking a model course framework that provides enough basic awareness without adding too much additional information that would increase the length of the course and, subsequently, the cost of the course. The different MTSA model courses available are: Maritime Security Awareness; Maritime Security for Military, First Responder, and Law Enforcement Personnel; Maritime Security for Facility Personnel with Specific Security Duties; Maritime Security for Vessel Personnel with Specific Security Duties; Vessel Security Officer; Refresher Course for Vessel Security Officer; and Guidelines for Maritime Security Training Course Providers.

All of the MTSA course materials, excluding Guidance for Maritime Security Training Course Providers, have the same basic components and format. The format is: Introduction; Course Framework; Course Outline; Detailed Teaching Syllabus; Instructor Manual; and Evaluation. Because of their matching formats, course providers could easily pick and choose different topics from the
course models and incorporate them into a course unique to the providers’ needs. Furthermore, because these and three other IMO model course (Ship Security Officer, Company Security Officer, and Port Facility Security Officer) have all been developed by the same entity, the U.S. Merchant Marine Academy, they can all easily be read, reviewed, edited, and re-constructed in a similar and straightforward method, since their formats are similar. While these similarities are a strength, they can also be a weakness as a course provider has to allocate extensive time to deciphering nuances among the courses to choose the course, or parts of different courses, that are most needed.

Another strength of the MTSA model courses, and again for the three aforementioned IMO model courses, is the designation of ship and port facility security training. Although a course provider for shipboard personnel may not need training models for port facility personnel, the ability to access both ship and port personnel duties and responsibilities, as defined by the MTSA and ISPS Code, can allow for comprehensive understanding among trainers and trainees as to who is responsible for what. The access to ship and port security training models can illustrate how both ship and facility personnel have similar goals of attaining and maintaining security. Although there are differences in how to implement ship and port security measures, communications, and information exchanges, the ability for each side to know and understand the other’s duties and goals can better help them both to achieve more efficient and effective threat mitigation. Another benefit of the MTSA model courses, with respect to their design, is the development, in a tabular format, of concise competences, with
noted methods for demonstrating such competences and criteria for their evaluation. This table can help instructors, as well as students, clearly identify the purposes and expected outcomes of training.

Most of the MTSA courses build on one another; the series begins with general Maritime Security Awareness and advances to Vessel Security Officer (VSO) training. One course, however, that contained a training component that was unique to research thus far was Maritime Security for Military, First Responder, and Law Enforcement. The distinct training subject area was: Maritime, Intermodal, and Supply Chain Conditions and Operations. The subject area had six sub-sections, including hazardous materials security. Perhaps this subject area is an assumed knowledge of trainees for the other MTSA courses, but its background could provide additional support to basic courses, such as Maritime Security Awareness. It should, however, probably be omitted from advanced courses, like VSO training, as experienced seafarers and security personnel are likely to have this general information. Another, though subtler, difference in the course for military and law enforcement was the separation of crowd and crisis management; crisis management was broken into its own subsection, independent of crowd control. Including this distinction in a course for ship security personnel could enhance their training, with considerations of security incidents taking place at sea, where panic and crisis could ensue, without the immediate availability of military or law enforcement.

The VSO and VSO Refresher courses both have the same weaknesses: the reference to the U.S. TWIC program. While comprehensive knowledge,
understanding, and enforcement of the TWIC program is imperative at U.S. port facilities, it may not be applicable to all cruise or cargo ship crewmembers, even those with identified security duties. While docked at a U.S. port, personnel and security guards check passenger and visitor identification, as required, but this does not necessarily require understanding of TWIC. Furthermore, within the realm of the centralized training academy for Carnival Corporation & plc, not all of their operating lines or ships call at U.S. ports. It may behoove crew that frequently arrive at and depart from U.S. ports to have a general understanding of TWIC, but even then it may not be necessary because it extends outside of their designated duties. This analysis found that TWIC implementation is not necessarily a pertinent aspect of training for operating lines and ships that do not regularly travel to the U.S. References to the National Incident Management System and the National Response Framework, both specific to the U.S., may also have similar weaknesses of not having relevance to a corporate-wide training academy for companies with a focus on global, not domestic, operations.

The CVSSA mode course framework offers extensive information for training crew in the applications of the law’s new safety and security requirements. Some of the law’s requirements are technology dependent or otherwise related to the ship’s security plans and systems. The model addresses how guards should be trained in the appropriate use of security systems and equipment, including the importance of retention of data, video, and images. The retention of data, as well as proper communication pathways, allows crews to notify the proper authorities and to be prepared for U.S. requirements if and
when authorities, such as the FBI, investigate crimes aboard the ship. This model also offers extensive information for prevention, detection, investigation, and reporting of criminal activities. It has a detailed methodology of what to do when entering a scene and how to properly detect, collect, and preserve different types of evidence. However, the model course framework is limited in its usefulness to train personnel in security concerns, such as terrorism, that extend beyond common criminal activities. Furthermore, because the model is specific to U.S. legislation, its applicability to an operating line that does not cater to the American population may be limited. Consequently, the model course was very helpful in designing the portion of the syllabus that details specifically with criminal activities, but it did not provide much help elsewhere in the syllabus design.

Three model courses of the IMO were reviewed and evaluated. They were: Crowd Management, Passenger Safety and Safety Training for Personnel Providing Direct Services to Passengers in Passenger Spaces (Model Course 1.28); Proficiency in Crisis Management and Human Behavior Training Including Passenger Safety, Cargo Safety, and Hull Integrity Training (Model Course 1.29); and Ship Security Officer (Model Course 3.19).

Model Course 1.28 addressed issues with both passenger and roll-on/roll-off (ro-ro) ships, which are designed to transport vehicles as cargo in addition to passengers. This dual purpose is a positive for the varying sectors of the maritime industry, but it was a slight negative for the purpose of this research, as the review had to be careful whether guidelines applied to all passenger vessels
or specifically to ro-ro vessels, which are not used by Carnival Corporation & plc.

Another weakness for this research was the amount of focus Model Course 1.28 gave to topics that were more safety, rather than security, based. However, safety concerns and training topics are reflective of STCW, and thus positively reflect IMO’s policy goals. This course also gave specific case studies, with a description of what happened and lessons learned from the experience, in addition to referencing case studies in describing how some of the IMO’s policies were created. These features are helpful in relating regulations and policies to real-world events. As a whole, Model Course 1.28 provided detailed and supporting course materials, which could provide the basis for an effective course, but not the entire basis for a course devoted solely to maritime security.

Model Course 1.29, which also addressed passenger vessels, ro-ro vessels, and safety concerns had similar strengths and weaknesses as Model Course 1.28 in this respect. Another strength for the maritime industry was this course’s appreciation of operational logistics, such as cargo loading and embarkation processes. However, for a maritime security course, general port and ship operations will be addressed in terms of security roles, responsibilities, and communications, rather than explicit logistical functions. The human behavior element of this course was a notable strength, as it addressed the need for understanding motivations of passengers and other personnel, which can impact procedures in the event of an emergency. Specific mention was made regarding stress and panic, and the irrational behavior and thoughts that can result from such feelings. Model Course 1.29 also had an important strength in its
requirement of national and international regulations to be implemented with drills and exercises. This acknowledgement supports all global stakeholders, as opposed to an IMO course focusing solely on IMO regulations. Model Course 1.29, however, had some conceptual similarities as Model Course 1.28; perhaps it would be more efficient to combine the two courses as one unit, rather than two separate, yet similar, units.

Model Course 3.19 was the most applicable to this research because it focused solely on security, specifically the role and responsibilities of the SSO. The course was detailed, and its focus on safety was minimal. Because this course did not require trainees to have specific entry prerequisites, parts of this course could be used for another security training course (although maybe more advanced than basic) that was not exclusive for a SSO. Model Course 3.19, in the instructor manual, also referenced security threats and attacks that occurred outside of the maritime industry. While heavy focus on operational logistics of those threats may not be applicable, the lessons learned and methods to prevent such attacks from occurring on ships could be helpful, in addition to the reinforcement of security as global concern that spans many industries.

As an additional general strength, all of the IMO model courses reviewed for this research had similar structures and formats; course providers could easily combine elements of each course into a unique framework tailored for their specific needs. Furthermore, all of the courses reviewed contain IMO and
international background information that sets the stage for why these courses were developed and how they can prevent future safety or security disasters in the maritime industry.

5.3 The Design and Development of the Centralized Training Academy

5.3.1 Facility

The final facility decisions are pending Corporate visits to the Philippines and India and the SRG’s vetting of the facility visits and resulting evaluations.

5.3.2 Curriculum and Course Delivery

The research aimed to initially identify what is legally required of the academy and what is recommended, in order to include both elements in a curriculum that successfully implements Carnival’s goals. This was accomplished through policy analysis, and the creation of a topic development matrix (located in Table 4), which was one of the foundational elements off which to base course topics. Analysis of model course frameworks also contributed to delineating course topics. The preliminary versions of a course overview and learning objectives are in Tables 7 and 8, respectively. The detailed syllabus cannot be publically circulated due to security concerns and its proprietary nature, but a condensed syllabus is located in Appendix E.

The foundational part of the course applicable to all operating lines of Carnival Corporation & plc is about six days in length, which is reflective of theoretical and practical training elements. At a later point, operating lines will have the option to create their own individual sections of line-specific topics. The course delivery contains two major components: theoretical and practical
training. The theoretical training, which served as the foundation for the entire academy, was established through lectures, given via PowerPoint presentations. The practical training complemented the theoretical training by reinforcing concepts and engaging student participation. Some methods of practical training incorporated include: staged scenarios of security threats and/or incidents; role-playing scenarios to encourage understanding incidents from different perspectives; hands-on training with equipment and systems; and practice of correct reporting measures via communication pathways and documentation forms. The following topics are likely to be accompanied with practical training: the Role of Onboard Security Guards; Information Collection and Reporting; Security Administration; and Transformation of Policies into Procedures.

Additional course supplements may include the following: independent study exercises; audio or visual materials; student hand outs of key Corporate or international policies; quizzes; and a final cumulative exam.

Additional research indicated that administering a final cumulative exam at the conclusion of the course would be most effective if it were preceded by smaller quizzes or assessments. The assessments prior to the final exam would encourage student engagement and would reduce the number of students who do not actively engage themselves in course material until immediately prior to a final exam (Rust, C.). In relation to the centralized training academy, the clear division of course topics would allow for a quiz or assessment to follow each
topic. Furthermore, some topics can be grouped together (such as topics that fall under a category of prevention), which would also allow slightly larger assessments based of multiple course topics.

Research also indicated that independent studies can be most effective for students when they have sufficient access to necessary materials, and when an assessment of the task will follow. More specifically, students have been shown to actively support “assessment measures to incentivize weekly readings” and “mechanisms that provide greater access to learning materials” (Lemanksi, C.). Because trainees at the centralized training academy will be given all supplementary materials and because there are possibilities to add smaller assessments prior to a final exam, an independent study exercise can be a time-efficient method to promote student engagement with the curriculum in addition to lecture and field exercises.

The benefits of practical training as a supplement to theoretical training were reaffirmed by research that indicated “practical training increased students’ understanding of theoretical knowledge and their motivation to study” (Katajavuori, N., Lindblom-Ylanne, S., and Hirvonen, J.) While practical training is required by STCW regulations V/2 and I/14, results showed that adding components of interactive exercises fulfills more than an international requirement; practical training fulfills Carnival’s aims to provide highly skilled and thoroughly trained security crewmembers that have demonstrated abilities to mitigate security risks. The practical training elements incorporated into the centralized training academy sought to not only diversify the structure of the
course, but also to further connect students with a comprehensive knowledge of
course topics by encouraging interest and motivation through interactive
participation.

Table 7 – Course overview

<table>
<thead>
<tr>
<th>Subject Area</th>
<th>Hours</th>
<th>Day</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Introduction</td>
<td>1.0</td>
<td>1</td>
</tr>
<tr>
<td>1.1 Course overview</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2 Introduction of participants and facility</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3 Course conduct</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.4 Competences to be achieved</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.5 The Company</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.6 Current global threats and patterns</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.7 Cruise ship and port operations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Threat Overview</td>
<td>3.0</td>
<td>1</td>
</tr>
<tr>
<td>2.1 Crime</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2 Terrorism</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.3 Piracy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.4 Civil unrest</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5 Trends of current global threats</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Maritime Security Policy</td>
<td>1.5</td>
<td>1</td>
</tr>
<tr>
<td>3.1 Relevant international conventions and codes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.2 Relevant U.S., E.U., and other legislation and regulations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.3 Flag state requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.4 Definitions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.5 Legal implications of action and/or non-action</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4. ISPS
Security Roles and Responsibilities
4.1 Contracting governments
4.2 Recognized security organizations
4.3 The company
4.4 The ship
4.5 Port facility
4.6 Ship Security Officer
4.7 Company Security Officer
4.8 Port Facility Security Officer
4.9 Fleet and Port Security Auditor
4.10 Security coordinator
4.11 Security supervisor
4.12 Security guards
4.13 Shipboard personnel with specific security duties
4.14 Port facility personnel with specific security duties
4.15 Other personnel
4.16 Actions required by different security levels
Ship Security Assessment
4.17 Risk assessment methodology
4.18 Assessment tools
4.19 On-scene security surveys
4.20 Security assessment documentation
Ship Security Plan
4.21 Purpose
4.22 Contents
4.23 Confidentiality issues
4.24 Implementation
4.25 Maintenance and...
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Attendance</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. The Role of Onboard Security Guards</td>
<td></td>
<td>24.0</td>
<td>2-4</td>
</tr>
<tr>
<td>5.1 Screening</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.2 Watch Standing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.3 Crime Scene Preservation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.4 Dispute Resolution</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.5 Surveillance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.6 Threat identification, mitigation, and response</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Shoreside Security</td>
<td></td>
<td>1.5</td>
<td>5</td>
</tr>
<tr>
<td>6.1 Countries, flag states, and ports visited by Carnival Corporation &amp; plc</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.2 Countries and/or ports with high security standards</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.3 Countries and/or ports with low security standards</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.4 Importance of ship security independent of port security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Protecting the Ship</td>
<td></td>
<td>2.0</td>
<td>5</td>
</tr>
<tr>
<td>7.1 ISPS and MARSEC security levels</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.2 Flag states</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.3 Contracting governments</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Drills and Exercises</td>
<td></td>
<td>1.5</td>
<td>5</td>
</tr>
<tr>
<td>8.1 Emergency procedures and contingency planning</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.2 Security drills and exercises</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.3 Assessment of drills and exercises</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. Information Collection and Reporting</td>
<td></td>
<td>2.0</td>
<td>5</td>
</tr>
<tr>
<td>9.1 Basic</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.2 Advanced</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.3 Information and communication security</td>
<td>9.4 Information Technology (IT) security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>10. Security Administration</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.1 Written and verbal communication skills</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.2 Documentation and record keeping</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.3 Monitoring and control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.4 Security audits and inspections</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.5 Reporting non-conformities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>11. Transformation of Policies into Procedures</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.1 Crime</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.2 Terrorism</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.3 Piracy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.4 Civil unrest</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Course Review</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Evaluation</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>48</td>
<td>7</td>
<td></td>
</tr>
</tbody>
</table>
Table 8 – Learning Objectives

<table>
<thead>
<tr>
<th>Course Topic</th>
<th>Learning Objective</th>
<th>Methods of Achievement</th>
<th>Methods of Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Introduction</td>
<td>A. Knowledge of Company structure and organization</td>
<td>• Comprehension of nautical terms and ship layout</td>
<td>Assessment from evidence obtained from approved training and/or examination</td>
</tr>
<tr>
<td></td>
<td>B. Understanding of the unique nature of cruise ships</td>
<td>• Understanding of various stages of cruise ship travel: in port; in territorial waters; and in international waters</td>
<td></td>
</tr>
<tr>
<td>2. Threat Overview</td>
<td>A. Knowledge of threats to cruise security</td>
<td>• Knowledge of historical events</td>
<td>Assessment from evidence obtained from approved training and/or examination</td>
</tr>
<tr>
<td></td>
<td>B. Knowledge of global threat trends and patterns</td>
<td>• Knowledge of trends and patterns of current threats, especially criminal activities, terrorism, piracy, and civil unrest</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C. Identification of weaknesses/issue s in case studies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Maritime Security Policy</td>
<td>A. Knowledge of major international regulations</td>
<td>• Awareness of key maritime security policies</td>
<td>Assessment from evidence obtained from approved training and/or examination</td>
</tr>
<tr>
<td></td>
<td>B. Knowledge of the primary international regulatory code</td>
<td>• Understanding of basic differences among the role of shipboard security guards and government authorities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C. Knowledge of applicable U.S. law</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>D. Understanding of relationship among U.S. law and international regulations</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 4. ISPS | A. Understanding of the primary role of ISPS  
B. Understanding of the requirements and applications of major ISPS sections | • Understanding of the specific roles of the port state, the port facility, and the shipboard security personnel  
• Understanding of appropriate actions required by ISPS security levels  
• Creation of emergency procedures and plans, including a Ship Security Assessment, Ship Security Plan, and Declaration of Security | Assessment from evidence obtained from approved training and/or examination  
Demonstration of practical ability to fulfill required components of ISPS |
| --- | --- | --- | --- |
| 5. The Role of Onboard Security Guards | A. Understanding of the roles and functions of shipboard security guards  
B. Ability to effectively screen and conduct searches of passengers, their effects, and the ship  
C. Ability to effectively patrol and monitor the ship’s interior and exterior  
D. Ability to preserve onboard crime scenes | • Knowledge of techniques used to circumvent security measures  
• Recognition of behavioral patterns of persons likely to pose a threat  
• Implementation of active watchstanding and patrols  
• Understanding of crime scene entry procedures, | Assessment from evidence obtained from approved training and/or examination  
Demonstration of practical ability to screen passengers, their belongings, and their behavior  
Demonstration of practical ability to control restricted areas |
| 6. Shoreside Security | A. Understanding of the strengths and weaknesses of shoreside security  
B. Understanding of the interaction between ship and | Understanding of variances in shoreside security at different ports traveled by Carnival Corporation & | Assessment from evidence obtained from approved training and/or examination  
Demonstration |
|---|---|---|---|
| E. Ability to resolve disputes, control crowds, and exercise self-defense  
F. Ability to conduct surveillance as means of maintaining ship/port interface security  
G. Ability to identify and respond appropriately to weapons, explosives, and drugs | evidence collection, and investigation  
- Awareness of victim and witness sensitivity  
- Display of appropriate behavior, bearing, and disposition  
- Implementation of correct crew/guest gangway procedures  
- Heightened awareness for suspicious activity and nonconformities  
- Ability to recognize and respond to weapons, drugs, dangerous substances, and explosives/devices | and access points  
Demonstration of practical ability to preserve crime scenes and collect evidence  
Demonstration of practical ability to control crowds and aggressively hostile passengers  
Demonstration of practical ability to conduct security surveillance  
Demonstration of practical ability to: identify weapons, drugs, dangerous substances, and explosives/devices |
<table>
<thead>
<tr>
<th></th>
<th>shore security personnel</th>
<th>plc</th>
<th>of practical ability to conduct proper security measures shoreside</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>C. Identification and understanding of the discrepancies among strong and weak shoreside security</td>
<td>Ability to enact proper security procedures when at ports of call</td>
<td></td>
</tr>
<tr>
<td>7. Protecting the Ship</td>
<td>A. Understanding of how to apply roles of different elements (ISPS, port state, and government) to protect ship security</td>
<td>Ability to interpret and apply security levels and warnings to a ship</td>
<td>Assessment from evidence obtained from approved training and/or examination</td>
</tr>
<tr>
<td>8. Drills and Exercises</td>
<td>A. Identification of different types of drills and exercises B. Understanding of the value and importance of drills and exercises</td>
<td>Knowledge of ship emergency procedures and contingency plans Participation in drills and exercises</td>
<td>Assessment from evidence obtained from approved training and/or examination Demonstration of participation in security drills and exercises</td>
</tr>
<tr>
<td>9. Information Collection and Reporting</td>
<td>A. Understanding the importance of information collection and information security in maintaining ship security</td>
<td>Ability to effectively collect and report security information Ability to communicate sensitive and confidential information appropriately</td>
<td>Assessment from evidence obtained from approved training and/or examination Demonstration of practical ability to collect and exchange information</td>
</tr>
</tbody>
</table>
| 10. Security Administration | A. Understanding basic written and verbal communication skills | • Effective written and verbal communication skills  
• Knowledge of proper communication routes  
• Accurate reporting, documenting, and logging of information, nonconformities, and incidents | Assessment from evidence obtained from approved training and/or examination  
Demonstration of practical ability of effective communication and documentation skills |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>B. Understanding of proper documentation and reporting processes</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>C. Understanding of security audits and inspections</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 11. Transformation of Policies into Procedures | A. Understanding of how policies, procedures, and standards are transformed into plans and actions for specific criminal, terrorism, piracy, and civil unrest threats and incidents | • Comprehensive knowledge of all applicable policies and regulations  
• Ability to implement and enforce industry and Corporate procedures to prevent and mitigate threats | Assessment from evidence obtained from approved training and/or examination  
Demonstration of practical ability to maintain secure ship environment, onboard and within ports |
5.4 Pilot Study

Due to the limited timeframe of this internship, a pilot study and further evaluation of the academy was not able to take place.

5.5. Cost Analysis of the Centralized Training Academy

Analysis looked at the costs and benefits of centralized security training within the maritime industry as a whole because many shipping or cruise lines currently practice on the job training that may differ slightly from ship to ship, or line to line under a single corporation. When analyzing the perceived benefits of both training methods, however, the centralized training academy has significant benefits that current training methods may not have. Because onboard training is conducted by individual lines, there is no standardization among the training of security personnel, despite that all lines and personnel that may administratively operate under a single corporation. The centralized training academy is an obvious solution to this fragmented process, and it ensures that all ship security personnel are afforded the same basic foundational knowledge of threats and mitigation measures.

Another issue with on board training is the lag time between when a new guard boards the ship and when their security job might actually begin. In addition to receiving security training on the job, new personnel may have additional, non-security related, duties that occupy their time; these additional duties can deter from an effective learning environment and detract from the amount of time a trainee is able to focus on their training materials. At the centralized training academy, the only student focus is security training, and this
process also allows new guards to begin their security duties as soon as they board a ship, upon successful completion of the academy. Because of these significant factors, the benefits of a centralized training academy, in terms of better logistics and standardization among all security personnel, can prove to be invaluable for a company that operates multiple cruise or cargo lines.

The cost analysis also looked at estimated costs of security incidents in the maritime domain, in addition to the financial costs of running the academy, although the explicit costs of running this specific academy were not disclosed for proprietary reasons. In the maritime domain, security risks and threats are also costs; if a security threat becomes an attack, there will be a financial cost attached. Whether the cost is the repair of a ship or equipment; reimbursement of passengers for the experience; adding new physical ship security measures; or the lost revenue while a ship or port is out of commission; security risks and threats can and will have financial costs. Although the details of such costs can only be speculated until an attack occurs, they needed to be considered in a cost/benefit analysis.

It is difficult to accurately quantify the costs of attacks on ships, as there can be many direct and indirect costs, some of which can be difficult to measure. The following estimates will focus on an attack of piracy, as an example of a significant security threat in certain waters. Major direct costs of piracy include: “ransoms, insurance premiums, the costs of re-routing to avoid piracy regions, deterrent security equipment, naval forces, piracy prosecutions, and anti-piracy organizations.” Looking even deeper at some of these direct costs, it is
interesting to note that “[t]he total cost of ransom is estimated to be around double the value actually paid to pirates,” as a result of additional elements, which can encompass: “the cost of negotiations, psychological trauma counseling, repair to ship damage caused while it is held captive, and the physical delivery of the ransom money, often done by helicopter or private plane.” When calculating an estimate for the direct costs of ransom money alone, these costs for the years 2009 and 2010, with the doubling factor calculated, is estimated to be $830 million. Looking at the direct cost of implementing enhanced ship security measures, estimates range from $363 million to $2.5 billion, per year. Because there are a variety of security measures and these measures may further vary on ship size, type, and capacity, this figure has a wide range of estimation (Bowden, A., et al).

Beyond direct costs that can be estimated to a certain degree, there are indirect costs of piracy (and other security threats) that are not able to be calculated or estimated as easily. Indirect costs from a macroeconomic perspective include: “effects on regional trade, fishing, and oil industries, food price inflation, and reduced foreign revenue.” These effects can be difficult to quantify as “it [is] too difficult to scientifically disaggregate the effects of piracy from general instability and state failure in countries harboring pirates.” Beyond these indirect costs, there are also additional costs and concerns regarding the human element in the maritime domain; injuries, deaths, and counseling all have additional costs. After approximating some major direct and indirect factors, the total estimated cost of piracy is $7 to $12 billion per year, which is reflective of
conservative assessments to minimize the overinflating of values. This specific figure, however, does not include any potential environmental costs resulting from an attack, such as the accidental spilling of oil or fuel into the water. Furthermore, it is important to note that while these figures provide for some preliminary calculations to be included in a cost analysis of a centralized training academy, data is limited by what attacks and their resulting effects are actually reported in the industry. As much of the maritime industry is profit motivated and most ships run on tight schedules, some ships or companies may not report attacks of piracy as the owners may not want “bad publicity or the ship to be delayed by an investigation.” While cost/benefit analyses can benefit the industry and those who research maritime security threats, there is an underlying potential issue that “[p]iracy is downplayed by both governments and industry for both political and commercial reasons” (Bowden, A., et al).

Although a terrorist attack may be logistically different than that of piracy, it is plausible to assume that some of the direct and indirect costs of terrorism are similar. A terrorist attack on a ship would not likely result in demands for ransom (and thus would eliminate some direct costs); however, because terrorist attacks can result in more human fatalities, more physical damage to a ship, and more media attention, there may be additional costs for consideration in an analysis. Furthermore, a terrorist attack (which may occur at a port while piracy is more likely to occur in coastal waters) can also generate costs of port closures and costs of disruptions in a domestic supply chain, if a container ship or a container terminal at a port is targeted.
When analyzing costs more specific to the cruise industry, it can still be difficult to obtain exact figures of direct and indirect costs that result from significant security incidents. There is, however, some data available to investigate the financial costs a company incurs when they are forced to remove a ship from the water and into a dry dock. It is important to note that this example looks at operational concerns, rather than security concerns. The costs to dry dock a ship can vary based on the extent of operational damage or maintenance needed, whether or not the ship prematurely ended a cruise, and whether or not the dry docking negatively impacts future cruises. As a result of a mechanical issue (a drive bearing failure), a Celebrity Cruise Lines ship was forced to dry dock. Identified costs included: “refunds of all prepaid tickets for [a] cancelled cruise, plus issuing vouchers for a free cruise to ticket holders.” These and other costs to Celebrity Cruise Lines added up to $14 million per instance of dry docking. In this particular example, Celebrity had filed a law suit against the maker of the faulty mechanical elements, and an initial settlement awarded Celebrity $36 million (Carr, B.). The cost to dry dock as a result of operational malfunctions is not cheap, but this specific example does not encompass a variety of other costs and concerns associated with an attack of terrorism or piracy on a ship. Additional costs of a security related incident can also include: compensation to injured or killed crewmembers or passengers; more extensive or complete damage to a ship; and the resulting public perception of the maritime industry as exploitable by terrorists and pirates.
Although there is a cost for ship security crewmember training and costs for ships to employ physical security measures, the benefits of a centralized training outweighed the costs of associated security risks, which the academy aims to mitigate. The ultimate purpose of a centralized training academy is to have quality training that outweighs security risks, and costs associated with such risks. In specific respect to piracy concerns, investing in training that has long term prevention and mitigation benefits will surpass costs associated with an attack: ransom, ship damage, compensation for passengers or crewmembers, the amount of time a hijacked ship is out of operation, increased insurance premiums, and a resulting negative public perception. Furthermore, in comparison to onboard training, the academy will provide a better environment for theoretical and practical learning without any lag time once the guard is aboard a ship; a corporate-wide standardization of curriculum, in conjunction with a more effective atmosphere will provide training that is better than the current onboard training system. This enhanced training experience has perceived benefits of better trained crewmembers, who will more aptly engage in risk mitigation, and more efficiently respond with resiliency in event of an attack.

More generally, when looking at the costs incurred by stakeholders to comply with new policy regulations in the maritime industry, the costs to establish an academy can also be considered short-term sacrifices, while the enhanced security gained from policy implementation does not have an expiration date. At a corporate level, a cruise or cargo line may feel pressure from market forces to adapt readily to new, regulated or recommended, policies. As a means to sustain
and increase their customer base, these private industries can advertise their enhanced security features and compliance as a method to promote the safe, secure, and reliable services they are selling. Security measures ensure the integrity of containers for imports or exports, and such security measures are valued in a globalized economy, where risks and threats are also international concerns. Economic and trade incentives can also prevail in the global maritime world; where port state authorities can exercise their control of searches and inspections, ships may find it advantageous to comply with regulations before being detained or banned from a port. Economic incentives, as a mechanism to increase demand within market forces, are thought to drive compliance with security regulations as a means for countries to continue trade.

Especially in the globalized world of today, countries might have incentives to take preemptive measures to comply with maritime policies than to risk detention, banning, or trade sanctions, which are costs that could exceed costs of compliance. Furthermore, the costs for maritime stakeholders to comply with IMO regulations are short term costs, while the perception of benefits extends into the long term. IMO regulations, especially the ISPS Code, also offer some level of standardization for ships and ports worldwide to have some security similarities; these similarities can also act as benefits to allow a ship to arrive at and depart from a port with more ease, thus staying on business schedule, than if ports and ships did not comply with the same set of security regulations.
The following example will detail a potential security attack in the maritime industry, the potential costs of the attack, and the potential ways enhanced maritime security training could have prevented or mitigated the attack. A large commercial ship is carrying a volatile fuel into the Port of Los Angeles. As the ship nears the port, a suspected terrorist who was hiding in the ship makes himself known and detonates the fuel. The ship explodes, and although no immediate damage is done to the port, many ships must re-route to other ports along the Western coast of the U.S as a result of security concerns of additional terrorists in the immediate area of the Port of Los Angeles. Due to the rerouted traffic, many other ports on the West coast become congested, as they attempt to adapt with the unexpected increase in port operations. The Port of Los Angeles has been completely closed as the Coast Guard works to mitigate a mess in the offshore waters and the FBI works to investigate the suspected terrorist attack. An estimated cost of the port closure alone is approximately “$1 billion per day for the first five days, rising sharply thereafter.” While this estimate is based off a labor-management dispute, not a terrorist attack, for ports along the West coast, not specifically the Port of Los Angeles, it is a potential estimate for the economic consequences of shutting down a port (Frittelli, J.). A suspected terrorist attack could further increase the costs needed to supply investigation teams and hazardous cargo clean up teams, in addition to lasting immaterial costs of negative public perceptions of the maritime industry as terribly vulnerable to security threats.
There may not be any conclusive and permanent measures to prevent an attack that aims to exploit the vulnerabilities of the maritime transportation network, but it is plausible to believe that if ship security personnel receive improved training at facilities devoted solely to maritime security, some attacks may potentially not be successfully executed. For example, if crewmembers were trained in behavioral screening, perhaps they would have noted suspicious vehicles or persons at the ship’s point of origin and notified port facility personnel. Port facility personnel then may have been able to investigate the suspicions, which could have deterred and prevented unauthorized persons from approaching or boarding the ship. If crewmembers were traveling from a port with lax security procedures or did not notice any suspicious individuals while in port, perhaps training in proper watchstanding and patrols of controlled areas and access points could have increased the likelihood of a stowaway being discovered more rapidly, before an attack took place. Even if a suspected terrorist managed to elude these preventative measures and the ship’s crewmembers did not have time to react upon identification of the attacker, port security personnel who received ample training could effectively and efficiently temporarily cease all operations to engage in a comprehensive inspection of the port, in search for suspicious persons, vehicles, or devices. With theoretical and practical training of proper communication pathways and proper search techniques, there is the possibility that even if a port required closure, comprehensive security training
could reduce the impacts, costs, and length of any closures, allowing the port to resume operations more quickly than if port personnel had insufficient preparation in responding to an attack.
CHAPTER 6
DISCUSSION

6.1 Enhancing Security within the Civilian Maritime Industry

This research aimed to explore maritime security concerns from a corporate perspective. Because a large company in the maritime industry can be made up different branches from different countries, there may be variations in interpretations and implementations of company regulations that are developed with a goal of standardization. These differences can be attributed to varying cultural and geographical backgrounds, as well as differences in an individual’s maritime experience. These differences, however, can also be positive aspects, as they provided for discussion, rather than a situation where one person from a corporation makes decisions for all the different branches of the company to blindly agree to. In this respect, the dynamic and diverse nature of the maritime industry can be further compounded by cultural and geographical diversity as well. Because the international maritime industry is comprised of container shipping, oil tankers, and cruise ships, there is some understanding as to why some policies and regulations take a seemingly vague standpoint. While domestic or international policy should not be entirely ambiguous, there needs to be some room for different interests to interpret and adapt regulations as they best apply to their practice, and sometimes, only those interests can make such decisions for themselves.
Also from a business standpoint, cruise and shipping lines have to answer to administrative superiors, such as a Chief Executive Officer, and customers demanding satisfaction. Factoring in costs and public perception, much deliberation goes into decision-making. Enhancing security, through additional crewmembers, more extensive crew training, or hard measures onboard, costs money. These costs need to be justified such that the perceived benefit of mitigating risks is greater than the financial cost to do so. Protective measures that would be noticeable to passengers also need to be evaluated, in addition to cost, for their effects on public perception. Simply put, the maritime industry cannot scare their customers away with security measures that cause more anxiety than they do reassurance of a safe and secure service.

Along the lines of public perception, public communication, especially about security threats and responses, is a line that a business needs to walk carefully. In the cruise or aviation industries, for example, there are general safety and security messages, warnings, and pamphlets for people to listen, read, and comprehend at their own discretion. If on a cruise ship, or airplane, and a potential threat arises, crewmembers need to assess the validity of a threat in order not to falsely worry or scare passengers. To avoid a “cry wolf” scenario, companies want to make sure if they are alerting passengers it is for a legitimate reason so as to refrain from desensitizing passengers to real risks. Although the topic of public communication is often dealt with by some form of a public relations sector, the concept of maintaining a certain public perception, often by means of trustworthy and accurate communications, can be a constraint for a
company as they deal with deciding when, and how to, appropriately warn customers of increased security risks and mitigation measures.

When designing a maritime security training course, curriculum contents and course delivery need to be purposeful. More specifically, course logistics of potential consideration were: whether independent study should be considered as part of the curriculum; what, if any, type of evaluation was conducted; what materials could be used to supplement lectures; and if practical training was an effective use of time and resources. Because these factors could affect the efficiency of the course and the cost of the course, decisions made could not be arbitrary. As a means to have an academy that was logistically effective and worthy of the related costs, research sought to find studies, for or against, those important considerations. The course content itself was supported by research of domestic, foreign, and international maritime policies, and the justification for course logistics, as supported by additional research of certain practices in the field of education, showed that the design of a security training course needed to be supported by sound research and background information.

6.2 Defining Security Risks and Threats

Some threats to maritime security seem to be apparent ones, such as stowaways, drug smuggling, crime, terrorism, and piracy. This research, however, aimed to delve deeper than these threats by continually evaluating what risks the centralized training academy aimed to mitigate. Along this train of thought, different cruise or cargo lines may have different threats they perceive to need most protection against, and these differences can be attributed to different
ports of call and different travel routes. For example, piracy is not a major concern for ships making roundtrips originating from Miami and traveling into the Caribbean, but drug smuggling is. Furthermore, security threats can be commonly thought of as physical attacks, like an armed robbery or a bombing, but security threats can also be immaterial risks, such as the leaking of classified information. While immaterial risks can lead to physical attacks, they are also somewhat separate vulnerabilities that need to equally be protected against.

Because security is a multifaceted area and a comprehensive training academy would seek to give all threats due diligence, there is support as to why certain course components, such as information gathering, information security, and situational awareness, were necessary even though they may not result in visible increases of security measures.

In expanding on the definition of security threats, another research challenge was to connect security with the physical maritime environment. Threats such as Weapons of Mass Destruction (WMD), biological weapons, and chemical weapons could pose significant dangers to human and environmental health if there was a large-scale attack. Looking into environmental impacts from security measures was also an area of interest. While some security systems, such as metal detectors, are relatively simple and do not have an obvious impact on the environment, there are other technologies that may affect the environment. For example, Long Range Acoustic Devices (LRADs) can be used as a crowd control mechanism or as a measure to alert an approaching boat when they are encroaching in a ship’s secure area. For the latter measure, this
can help define if an approaching boat has malicious intentions; if they do not respond to warnings, the cruise ship can prepare itself for a potential security threat, like a pirate attack. Because LRADs can produce sounds that greatly exceed safe decibel levels for humans, they can cause pain and possible hearing damage, depending on what level they are operated at and for how long. If there are birds or marine organisms near the ship when these devices are deployed, it is reasonable to wonder what, if any, negative effects they could have on an animal’s hearing, which can impact a marine organism’s ability to echolocate and can impact other internal physiological functions.

In summary, maritime security is a dynamic environment, and what risks and threats that define security and its related mitigation measures are constantly being re-written. Specifically in the U.S., terrorism is a broad area of concern that requires a multitude of protective measures. Every time that a new mechanism of terrorism, such as a shoe bombing or hijacking threat, occurs, security regulations, especially in the aviation industry, need to be reviewed and often re-written. In this way, the maritime industry needs to understand and adapt to the dynamic nature of security to truly maintain successful protection measures against every new risk and threat that arises. Especially in consideration of the cruise and cargo industries, where ships can constantly be in transit, it is essential to take the time, and money, to outfit ships with hard protective measures and trained crewmembers to keep up with the dynamic nature of security. Because the course materials for the centralized training academy aim to have a dynamic nature to respond to changes in needs of Carnival
Corporation & plc and emerging threats within the global maritime domain, this training program complements the dynamic needs of maritime industry.

### 6.3 Benefits and Multiplier Effects of the Centralized Training Academy

The major local perceived benefit of the centralized training academy is that the crew of Carnival Corporation & plc ships will receive improved training, as a result of the standardization and comprehensive nature of the curriculum. Improved training will lead to safer and more secure ships; the trained crew will complement the physical measures, such as technology, and when both the physical and human elements of security are in sync, the ship, its crew, and its passengers, will be recipients of the enhanced mitigation methods. However, to be open minded and realistic about security, a threat or attack could still arise despite extensive protection. In the event of an attack, a perceived benefit of the academy is that, as a result of thorough theoretical and practical training, crewmembers will respond appropriately to enhance the ship’s resilience. Such action and resilience can either combat an attack entirely, or at least reduce the economic and environmental impacts that will ensue.

The local benefits enhance the security of each ship, but because Carnival Corporation & plc makes up such a large part of the cruise industry (as evidenced in Figure 8) there can be global benefits of the academy as well. The cruise industry itself, as a result of Carnival’s large involvement in it, may be safer and more secure. But if other cruise lines, and even shipping lines, adopt Carnival’s training strategy as a best practice in the maritime industry, the potential global benefits expand from a multiplier effect. As each cruise or
shipping line employs a training academy as a means to standardize and improve crew training, the effect of this research and Carnival’s product, multiplies into a global enhancement and awareness of the maritime domain. Even if the idea of a centralized training academy is not immediately adapted in the maritime industry, there is the potential that the idea itself will incite conversations among stakeholders. Discussion of maritime security training practices in itself can lead to heightened awareness of the dynamic nature of security threats, and heightened awareness of the global maritime domain is one step closer to enhanced security, in comparison to no changes in awareness of at all.

Furthermore, before entire nations or regions of the world can consider enhancing security at their ports or on ships of their flag state, there have to be smaller, more local examples of the effectiveness of new security initiatives. While Carnival Corporation & plc may not seem like a large section of the entire international maritime domain, the effectiveness of a centralized training academy for one company can hint at its applications and effectiveness for larger maritime businesses and port states to adapt such a process and curriculum for their security personnel. Starting small can have larger benefits in the future; for example, “the ‘Think Globally. Act Locally’ slogan, popular with the environmental movement, applies equally well to developing a stable security environment that enables global, regional, and national prosperity.” In this respect, improved awareness and security has to start somewhere in order to expand anywhere. Just as security risks and threats can be localized but have international impacts
as a result of today’s global economy, risk mitigation and protective measures can have the same impact, even though the globalized impacts of security may be slower to emerge than the impacts of attacks (Martoglio, C. and Morgan, J.).

BMP4 applies not only internationally required security regulations, but it also applies industry recommended practices to prevent and deter piracy. Furthermore, the specific nature of BMP4’s guidance allows for greater comprehension of the threat and practical implementation of mitigation measures. With the perceived benefit of Carnival’s training academy and its curriculum, having efficacy and applicability similar to BMP4, it can be applied not only to other cruise and shipping lines, but perhaps also to port facilities to train their security personnel as well. While best industry practices offer room for tailored variations for adoption, they have an underlining theme of enhancing existing methods to elicit a multiplier effect that will have benefits. In this case, enhanced maritime security training, as a best management practice supports existing policy, while aiming to extend the scope of awareness and action beyond minimum requirements.
More specifically in the cruise industry, a centralized training academy will better prepare ship crewmembers against all threats, including attacks of piracy. In 2009, Somali pirates attacked the MSC Melody, with 1,500 passengers onboard. Although the ship was not successfully boarded or hijacked, there are varied reports about what security measures were actually implemented onboard prior to and during the attack. The ship was traveling “far off the coast of Somalia,” but it should have planned and executed preventative measures prior to entering waters with known piracy threats. One report does not detail specific actions taken by the ship, but notes that the pirates “retreated after the Israeli security officers aboard the cruise ship returned fire” (“Italian Cruise Ship Fires on Somali Pirates”). Other reports indicate that ship passengers, not
crewmembers, were the first to notice the pirates, and they resorted to throwing ship furniture overboard to prevent pirates from boarding. After passenger action, the ship security personnel became aware of the situation and took action, which foiled a successful attack (“Attack on the MSC Melody: Passengers Fought Pirates with Tables and Deck Chairs”).

While the specifics vary among accounts of the attack on the MSC Melody, this incident can provide a possible case study analysis, for students to apply their acquired knowledge to real life occurrences in the cruise industry. A case study analysis would provide students with a realistic example of what can happen in the industry and how a centralized training academy can mitigate an attack. Extrapolating on an attack can create potential scenarios for students to apply their abilities and engage in a discussion or practical exercise. Based off a piracy attack similar to that which may have occurred on the MSC Melody, a case study template is provided in Box 1.

Although preventative actions cannot definitively preclude attacks that are driven by necessity and intense aggression, this scenario supports that comprehensive security training, which supplements requirements with best practices available in BMP4, is the only way to actively mitigate an attack and its potential impacts. Without knowledge of and ability to apply preventative and mitigation measures, there is the risk of a successful attack. It may not be likely that a small group of pirates would seek to hijack a large cruise liner carrying upwards of 3,000 passengers, but there are other imminent dangers that face cruise ships. Passenger and crewmember lives, in addition to the ship’s
structural integrity, are at risk if armed pirates assault a ship with heavy gunfire and grenades. While pirates may not hijack an entire ship if they are able to board, they may kidnap several passengers, for ransom, whose lives would be at great risk.

Comprehensive training would also incorporate post-event procedures, since proper reporting and communications can improve the ability of documented events to be used for future case study analysis. Without proper reporting and documentation, a company and the public can accumulate varying accounts of what happened, such as in the case of the MSC Melody, where it may be uncertain whether or not passengers were forced to compensate for inactive security guards. Misunderstandings and miscommunications, during and after a security incident, can affect what events, and how those events, are reported within a cruise line, as well as to international media. Websites, such as blogs, may not be as credible as news networks; and passenger accounts may be skewed by emotions. It is imperative that companies train security guards not only to detect, prevent, and mitigate any incidents, but also to objectively report and document them, with standardized forms and procedures. Through the analyses of the following fictitious scenario and the documented attack on the MSC Melody, it is clear that a centralized training academy has the potential to produce guards who are able to aptly detect and respond to threats, while maintaining passenger safety, in international waters.
This template enables students to identify strengths and weaknesses in security preparedness using a piracy attack scenario, some details of which are based on reported events.

1. Event description:

A cruise ship with 1,500 passengers is traveling through waters that are at high risk for piracy. Security guards are on the ship, but they are not actively engaged in appropriate duties that would be pertinent to travel in high risk waters. There is no heightened awareness, no additional watchstanding and patrols, nor are guards stationed and ready to utilize an LRAD, fire hoses, or foam monitors to deter the boarding of the ship. Instead, the security guards are only engaging in moderate awareness and vigilance, in addition to personal socializing. Two small boats begin to approach the ship, but they go undetected by distracted, oblivious, and untrained guards. Passengers who are lounging in a deck area begin to hear and sense suspicious activity. As passengers verify their suspicions, they see the two small boats very close to the ship; so close in fact that a few pirates have begun attempts to board the ship.

Panicked passengers, realizing their lives are in imminent danger, resort to throwing the deck furniture overboard to prevent the pirates from boarding. As the commotion escalates in intensity and noise, ship security guards become aware of the situation; they communicate the situation to the Ship Security Officer (SSO), who communicates with the Captain. The ship increases speed and employs evasive maneuvers, such as traveling in a zigzag pattern. The passengers, though now mustered in a safe zone, prevented the pirates from boarding, while guards engaged the fire hoses and foam monitors to continue the deterrence. The two boats, unable to board the cruise ship, have ceased their efforts and are no longer pursuing the ship. There are no immediate damages to the ship and there are no injuries to passengers or crewmembers; however, the ship and the Company will have to address the issue of poorly trained security guards, whose incompetence directly caused increased risk of injury and death to passengers.
2. Security gaps:

Ship security guards did not have sufficient or efficient training in what procedures are to be implemented prior to and during travels in high risk waters. There was a clear lack of: active patrols of the ship’s decks, increased visual surveillance, and preparedness to engage in anti-piracy measures if suspected pirates were discovered. Security guards also did not rapidly prevent passenger interaction with the threat once the incident was recognized, as they hurriedly joined the efforts to deter boarding.

3. Needed security protocols to address security gaps:

Prior to entering high risk waters, security guards should have had a briefing that would remind them: how the threat of piracy may affect cruise ships, how increased vigilance is imperative to early detection of threats; what types of behavior and patrols constitute increased vigilance; and what additional measures and procedures should be taken in the event there is an imminent threat of an attack by pirates.

As a result of heightened awareness, security guards would have been more likely to detect suspicious boats before they approached and attempted to board the ship. Guards would have immediately reported the threat to the SSO, who would correspond with the Captain, who would then report the threat to the relevant shoreside and naval authorities in the area. The Captain, and all security personnel, would then communicate the potential threat with the passengers, who would be required to muster in a safe zone, where they would not be in as much immediate danger as if they were directly fending off armed pirates.

As the ship engaged in evasive maneuvers and the pirates were no longer threatening the ship, all security personnel would have the proper training to communicate such updates with the passengers, in addition to enact crowd control measures, if needed. The proper post-incident reporting and documentation procedures would occur, along with procedures for government or military intervention, if needed. The guards would then return to their designated duties, including the maintenance of awareness and vigilance.
4. Training to effectively implement security protocols:

The following training topics, in theoretical and practical form, would be imperative to the prevention and mitigation of this proposed piracy attack:

- **Threat Overview**: provides a basic outline of major security threats to the maritime industry, including in what ways piracy is most likely to affect a cruise ship, in addition to current trends and patterns of piracy

- **Maritime Security Policy**: outlines major relevant domestic, international, flag state, and Company requirements and recommendations; the following policies require student awareness, understanding, and application: STCW (2010 Manila amendments), a national regulation of the Philippines, and BMP4

- **The Role of Onboard Security Guards**: details the major duties and responsibilities of guards when they are onboard a cruise ship; relates duties to specific risks and threats; subtopics in this section, such as Watch Standing and Surveillance, are imperative to detecting threats, especially suspicious vessels, in international waters

- **Drills and Exercises**: seeks to reinforce the importance of practice and preparation for all security risks and threats, even when no incidents or attacks have recently occurred on the ship

- **Transformation of Policies into Procedures**: represents the culmination of the course; this is where all of the newly acquired knowledge and skills are applied and transformed into actions; this topic utilizes case study analysis and practical exercises to foster prevention and mitigation procedures, beginning with detection and concluding with post-event procedures, such as documentation
6.4 Limitations and Shortcomings

6.4.1 Research and Academy

A research limitation was the time, four months from August to December 2011, allotted to the internship with Carnival Corporation & plc, in comparison to the expected installation of the centralized training academy, which was projected to be fully operational in 2012. The time frame limits this research to providing only a preliminary security training syllabus for use by Carnival Corporate & plc. Because this research was not conducted by an expert in maritime or security fields and because of the administrative processes at a corporation, the preliminary research and deliverables pave the way towards a functional course syllabus, but they are not entirely representative of the final product. As a result of time limitations, a shortcoming of the analysis of the benefits of the academy is the failure to see the academy in its entirety, from conception to installation. The conception of the academy had mostly occurred prior to August 2011, although through the research, design, and development of it, there were still ideas and details left to the purview of this research. This research, however, did not have the opportunity to fully analyze the execution of the academy or to analyze whether all perceived benefits came to fruition. A factor of the academy that could impact these perceived benefits is the experience and abilities of the course instructor. A course instructor with a background in the maritime security field would be most prudent in the academy achieving its goals. An element of instructor experience, beyond an academic and professional background, is the instructor’s practical knowledge of cruise
ships and realistic onboard processes. Furthermore, understanding of all potential benefits is limited by the academy’s possible expansion. The initial design of the academy, to train new crewmembers with security duties, has the potential to expand with additional purposes, such as advanced training, SSO training, and refresher training. Again, how these changes could affect benefits of the original research is uncertain.

Another limitation of this research and the academy is that the security training course is mostly ship-specific. While a comprehensive security training course also deals with in-port situations and facility communications, operations, and security, the academy is limited in how it can aid in protection once passengers disembark from the ship. Independent of the academy, ship personnel are limited to the control they have of passengers in port facilities or on shore excursions. Because shore excursions are a part of the cruising experience and passengers are entitled to their free will, even the most well trained crew on a ship cannot fully protect passengers if they decide to venture into cities with crime, civil unrest, or terrorism threats. In these circumstances, the perceived benefit comes from guards who have enhanced communication skills, in addition to information gathering and exchange skills. Better trained ship personnel can heighten passenger awareness and educate passengers about potential threat information prior to debarkation of the ship.

A logistical limitation to port and ship security is the process of a ship tendering at certain ports or harbors, which cannot physically accommodate a large cruise ship. In such a case, a ship will anchor in a bay, and small boats
manned by the ship’s crew tender back and forth from the harbor to transport passengers aboard the ship. Although this can be left to the concern of specific ports or ships, it can still be a general issue of concern for the cruise industry as a whole. Security issues may arise when there are no hard security measures, such as X-ray machines or metal detectors, on shore before persons board the tendering boat. Once the passengers disembark the tender and enter the cruise ship, there are security measures and crew that screen passengers and their effects. However, there are still small spatial and temporal gaps in which a criminal or terrorist could exploit the distance before these screening measures occur. On shore, however, there are ship crewmembers checking identification of passengers, and it is within the short timeframe before a person boards a tender, that comprehensive security training can be crucial. Because there are no physical screening processes, crewmembers should be extensively trained in screening behavior and dispositions of persons likely to post a threat to security, in order to compensate for a lack of physical screening processes. Although it may be possible for some ships to independently tender their own security equipment and systems to a port or harbor before tendering passengers to the ship, this may not be approved or allowed by certain port authorities. Even if it is allowable for a ship to deploy their equipment on shore, it may not be logistically sensible or feasible to do so if a ship is only docked for a few hours. Whether or not a ship is able to deploy its own equipment on shore while the ship remains docked in a bay, there are still possibilities for increased security concerns when the tendering process is required. Because of such situations, there is even more
support for security guards to receive quality training in physical screening processes, as well as intelligence gathering and behavioral screening.

The subject of tendering also raises a more general issue of ports that, with or without the need to tender, do not have adequate security measures, trained personnel, or active enforcement of regulations by authorities. There are ports that do not provide, or do not allow a cruise line to provide, security equipment and systems on land to screen passengers and their belongings before boarding the ship. Even if screening takes place immediately on board, such as with tendering, there still exist spatial and temporal gaps for security risks to become attacks. While a centralized training academy can train crews to be especially vigilant in ports that practice lax security procedures, even the mostly highly skilled crewmembers are not impervious to risks and vulnerabilities. While this obvious limitation in hard security measures, such as a protective border around a ship and passenger screening, can be prevented by calling only at ports that comply with strict security measures, it may not be realistic, for a cruise or shipping line to only travel to the most safe and secure ports in the world, as business would be significantly limited.

6.4.2 Policy

A major policy critique is the often vague and open-to-interpretation nature in the way regulations are written. It should be duly noted this does not apply to all law and policy, but the ones that will be specifically mentioned in this particular discussion. An example of ambiguity as a weakness is present when looking at the 2010 Manila Amendments of the STCW; the amendments call for anti-piracy
training, but are somewhat vague in how that training can or should be accomplished. Although the amendments do include mentions of piracy, as it relates to existing ship procedures and plans, in standards of competences for Ship Security Officers, it does not detail what anti-piracy techniques or activities should take place. In this instance, BMP4 can fill in the gaps for companies and Ship Security Officers, but not every training topic can be supported by such explicit guidelines if there are no best management practices for all security concerns. In policies without additional materials to support and guide implementation and enforcement of regulations, there can be many interpretations, even misunderstandings, of what the policies truly call for.

In consideration of the vast nature of the global maritime industry, however, there may be some purpose as to why policies are written with seemingly obvious shortcomings. It may not be practical for a policy to be idealistic and conceptually apply to all cruise lines and shipping lines, given the variances in ship structure, purposes of voyages, geographical origins and destinations, and security risks and threats faced by different ships and in different regions of the world. Can a policy realistically and accurately cover regulations and recommendations that acknowledge and embrace all these differences in the industry? An effective policy is probably not going to be that detail oriented. Although vague text can be a shortcoming, it is likely done purposefully to require a minimum level of security standards and procedures in the industry, without prescribing specific plans that would be unable to be effectively and efficiently executed in the diverse nature of the maritime domain.
International regulations may be especially broad in order to allow application to a varying degree of cultures, locations, threats, economies, and governments.

Whether policy is internationally broad or domestically specific, it needs effective and realistic strategy to complement its conceptual structure. Furthermore, policy is only as effective as its implementation and enforcement. Policy supplements, such as free model course frameworks, can aid in successful implementation. Enforcement will likely come from government or law enforcement agencies with specific duties, such as the U.S. Coast Guard, but self-regulation and internal industry enforcement can also support policy implementation. A weakness and limitation to domestic (U.S.) policy, however, is the trend for cruise ships to be registered with flag states other than the U.S. and for domestic policy to no longer have enforceable strength once a ship, regardless of the flag, is not in U.S. territorial waters. Once ships reach the international high seas, there are great policy limitations, as the ship is bound by its flag state requirements, not U.S. law.

As for the IMO, its conventions, regulations, and recommended practices only apply to those who are signatories to the convention. The IMO is not a regulatory body, and it cannot actively babysit signatories to ensure their practices coincide with their signatures. At the international level, implementation and enforcement rests more within port state authorities exercising control, through searches and inspections. This implementation is supported by Port State Control Memorandums of Understanding, such as the Paris MoU. Support from other stakeholders, such as CLIA and FCCA, can further encourage
enforcement of international maritime policies, although those non-governmental organizations are also absent from regulatory powers.

Another weakness of policy, specifically security related policy, is its reactionary, as opposed to proactive, nature. This blends into the next topic of limitations, which looks at the general field of security, but the focus here remains somewhat on policy. Security policy seems to be limited by what risks and threats exist, as defined by known attacks or known attempted attacks. This may be because policymakers do not possess the same creativity, or need for it, as terrorists, for example; or, this may be because without concrete evidence of why a supposed incident is to be seriously considered a threat to security, it is difficult to fund and support seemingly irrelevant policy. The phrase “Don’t fix what isn’t broken,” could also apply; if current policy, shaped from historical events, is sufficient for current risks and threats, why would policymakers seek to change it for potential, yet nonexistent, threats? Because this research did not look into the politics behind policymaking, the “why” behind a reactionary approach cannot be accurately attributed to any single factor, but nonetheless, this conservative approach is a limitation to security regulations. This also begs the question, which further blurs the line separating policy limitations from the field of security limitations, of whether it is even possible to be cognizant, and thus have protection against, every possible security risk and threat from criminals to terrorists. Again, this research does not try to answer that question, but rather acknowledge it and acknowledge the limitations it can impose on policy. These policy limitations can then limit industry knowledge and security standards, which
would also ultimately limit the effectiveness of a centralized training academy, if such an academy aimed only to satisfy minimum industry requirements. In such a case, the perceived benefits of the academy are not maximized if the policies and regulations the curriculum is based off are not comprehensive and proactive in their nature.

6.4.3 General Study of Security

A limitation to security policy and security in general is the thought process that associates risks and threats coming from external sources. On an airplane, it is the passengers, entering from outside the aviation industry, that are typically thought to harbor threats jeopardizing a safe flight. On a ship, it is, again, typically passengers, vendors, stowaways, or other small vessels who externally enter the industry that are viewed as obvious risks to safety and security. This thought process is empirically supported by historical and recent events, which have shown threats typically do come from outside an industry by those either directly attacking from the outside (attack on the USS Cole) or by those attempting to infiltrate the system from the outside (September 11th attacks). This thought process, then, is not incorrect by any means, but it is, like the issue of defining security threats, limiting in its perspective. Unintentionally being blinded to any threats, whether criminal or terrorist, that could arise from company personnel or ship crewmembers can be a limitation to studying security and imposing measures to mitigate threats.

Whether in the aviation or maritime arena, there are limitations to the study of security, especially when one without extensive experience in the field
conducts research. Specifically, there are limitations to the U.S. federal intelligence cycle, and where a private industry fits into that cycle. The cycle is visually represented in Figure 9. The cycle begins with planning and direction, which come from interests and concerns most pertinent to the President and the Executive Branch. Tasks are initiated with persons who actively collect raw information, which is then processed and analyzed. Results of analysis are disseminated and sometimes turned into intelligence products that then continue the cycle, if new or continuing tasks are planned and initiated (Noricks, D.).

What types of information the federal government collects may have more general and national purposes than looking at any private industry, let alone a specific cruise line. In this respect, private industries and corporations are not implicitly part of the federal intelligence cycle. If specific threats are discovered, this information will be disseminated to the appropriate entities; however, industries ultimately need their own intelligence cycles to engage in active information collection and to avoid limitations that exist as a result of information classification levels within the government. A major limitation to the study of security in a particular industry, such as the maritime domain, is that the industry generally does not have its own active information collectors, and the industry is then limited by what second-hand information they receive and analyze. While informal processes may exist for industry information exchange and communication, there is no specific government intelligence collection for the civilian maritime industry (Noricks, D.). This limitation, of discrepancies among the federal intelligence cycle and the business intelligence cycle, supports
advanced training methods for cruise ship security guards to develop a sense of situational awareness of their environments and develop threat identification skills, as a way to provide a company with accurate information within the maritime domain.

While agencies like the United Nations, and specific bodies such as the IMO, can create and execute security plans and procedures, these agencies and their respective processes cannot be the only driving forces to enhancing global security. Policy implementation and effectiveness rests greatly on industry and government initiative and action. Ships who abide by the ISPS Code can enhance their safety and security when calling at ports who also abide by the ISPS Code, but in order to truly improve international maritime security, all ships, all ports, and all governments need to follow security standards, specifically those set forth by the IMO, for the sake of standardization. Policies, regulatory or recommendatory, and a compilation of best industry practices are surely important directives in sustaining security and proliferating international trade and travel, but they cannot be the ending points; their effectiveness ultimately rests on the port states and governments whose duty it is to enforce regulations and perhaps even develop policies that exceed the minimum international standards.
Figure 9 – The federal intelligence cycle; Source: Carnival Corporation & plc
CHAPTER 7
CONCLUSIONS AND RECOMMENDATIONS

7.1 Conclusions of Research Goals and Objectives

Terrorism most vividly incites thoughts and memories of the September 11, 2001 attacks on the U.S., but terrorism’s reach is not exclusive to the aviation industry. The attack on the USS Cole showed that terrorism can affect the maritime industry, but threats in the global maritime domain extend even beyond terrorism. Threats include historic concerns of onboard crime, drug trafficking, and stowaways, but piracy has recently emerged as a threat that in some ways is comparable to terrorism and requires additional security measures than those that are currently sufficient for onboard crimes. Furthermore, the attack on the Seabourn Spirit and the attempted attack on the Oceania Nautica show that pirates can and will threaten cruise ships, in addition to cargo ships. While physical measures, such as a ship’s size, speed, and available technology, can aid in the detection and prevention of attacks, ship security personnel need to have training that elicits the following: an understanding of current threats; an appreciation for maintaining security; a knowledge of international and relevant foreign maritime policy; and a comprehension of how plans, procedures, and equipment can be used to prevent, detect, and respond to threats. Improved training methods can also enhance resilience and minimize impacts if a security incident occurs. Carnival Corporation & plc’s plan for a centralized security training academy fulfills these objectives by not only standardizing security on all
of their operating lines’ ships, but also by providing the international maritime industry with ships and crewmembers who have better resources to mitigate threats and maintain secure travels.

The purpose of this research was to analyze existing law, policy, and regulations in domestic, foreign, and international maritime domains and review existing model course frameworks for maritime security training, some of which come from laws and policies, and some of which come from existing training curricula used in the cruise industry. The results of the policy and curriculum analyses benchmarked key training components that are required, recommended, or optional for the goals of Carnival Corporation & plc’s centralizing training academy, which sought to enhance the quality and process of security training for shipboard crew on all of the Corporation’s ten operating lines. In order to improve the current training process, the centralized training academy will lodge and educate trainees at facilities located in India and the Philippines. These facilities will provide a better learning environment that is exclusive to the academy’s training purposes, which will allow trainees to concentrate solely on security duties and be ready, without delay, for their first shipboard deployment. The facilities also aided in enhanced quality of training by allowing theoretical curriculum to be easily complemented with practical and hands-on training.

This research yielded a preliminary curriculum for potential use at the centralized training academy, and the potential training materials will continue to be vetted by the Corporation’s Director of Maritime Security and the SRG prior to
the academy’s successful establishment. Because of the months of research and analyses that have gone into the curriculum, in addition to the various parties who thoroughly reviewed the materials, the training materials were reflective of a comprehensive strategy to produce maritime security personnel that have the ability to reduce security threats onboard Carnival Corporation & plc’s ships.

Based on a preliminary analysis of the purpose of the centralized training academy and its projected curriculum, it appears to fulfill Carnival Corporation & plc’s goals. The perceived benefits of the academy exceed the current benefits of standard onboard training procedures within the maritime industry. Maritime industries are also likely to find that the development of a centralized training academy is an effective use of their resources; even though financial costs may outweigh the costs of current onboard training, a centralized training academy has short and long term benefits that exceed those of standard training methods. In the short term, ship security personnel are able to begin their assigned duties immediately once they board a ship, without the delays of on the job training. In the long term, ship security personnel can reduce security risks, while having the knowledge and skills to quickly and effectively respond to an attack; proper responses and actions can save lives, in addition to reducing the economic and physically destructive impacts of an attack. Although this conclusion, like the cost/benefit analysis, represents initial findings that should be reviewed after the academy is fully instituted, results of this research indicate that the centralized training academy fulfills Carnival’s objectives and has potential for industry applications to enhance global maritime awareness and security.
7.2 Recommendations for Future Research

In addition to pursuing the proposed pilot simulation of the academy, recommendations for a follow-up of this research include monitoring the remaining developments of the centralized training academy and periodic reviews of the academy once fully functional to maintain that the perceived benefits come to fruition and outweigh the benefits of onboard training methods. Follow up research could include an additional study to compare the academy’s actual benefits with perceived benefits, which could entail periodic auditing of the course, course instructors, student performance, and student evaluations of the course. These follow ups would not only ensure the academy is fulfilling its original goals, but they could also show where modifications can further improve the academy structure or content. Future developments or academy additions can include the installation of advanced training, such as SSO training and refresher training courses.

Specific follow up research could include a study that investigates how the results of the academy compare to previous, onboard training methods. Such a study could develop an evaluation to determine differences between student knowledge from onboard training methods and the academy. An evaluation could consist of a written exam, oral exam, and/or practical demonstration of required knowledge and skills. This evaluation should test security personnel in three phases: immediately after (onboard or academy) training is completed; a midterm phase; and a final phase. By the final phase of the evaluation, all security personnel should be able to demonstrate near 100% accuracy and completion of
their duties; however, this study would aim to show whether the initial and midterm assessments validate that personnel who received training at the academy, as opposed to on the job training, achieve required knowledge and skills at a faster pace.

This evaluation process represents a way to quantify the time it takes for a security guard to reach a level of effective independence in their roles and responsibilities. If this study were to find that the academy does in fact provide security guards who understand and fulfill their duties with more ease and accuracy, then the academy’s benefits of producing highly skilled guards in an effective manner is validated. As a measure to ensure reliability and legitimacy of security guard evaluations as accurate measures of the academy’s assessment, evaluations should be conducted by impartial parties, such as the auditors from the Maritime Policy and Compliance department of Carnival Corporation & plc, as opposed to someone from the guard’s operating line. Furthermore, an ideal execution of this study would ensure that the guards selected from onboard and academy training methods are a random sample that is reflective of guards in all of the ten operating lines.

Other industry applications for this centralized training academy and other opportunities for maritime security training research include: adaptation for shore side security crew for cruise and cargo lines; adaption for port security personnel, with courses for general port security, port security personnel with focus on cruise ships, and port security personnel with focus on cargo ships; and adaption by an agency, such as a joint effort among the U.S. Coast Guard, TSA, and CBP
to create and mandate standardize training for all security personnel at U.S. ports, with the option for each location to have additional port-specific training.
Works Cited


October 2011.


Appendices

Appendix A - Timeline of Key Academic and Internship Dates and Deliverables

<table>
<thead>
<tr>
<th>Item Description</th>
<th>Date (2011)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Begin internship</td>
<td>August 8</td>
</tr>
<tr>
<td>Comprehensive exams</td>
<td>August 8 and 11</td>
</tr>
<tr>
<td>Committee meeting</td>
<td>August 11</td>
</tr>
<tr>
<td>Summary report of policy research</td>
<td>August 22</td>
</tr>
<tr>
<td>Committee meeting</td>
<td>September 9</td>
</tr>
<tr>
<td>SRG meeting and presentation</td>
<td>September 15</td>
</tr>
<tr>
<td>First thesis draft (proposal + methods + results)</td>
<td>September 30</td>
</tr>
<tr>
<td>Second thesis draft (+ discussion)</td>
<td>October 7</td>
</tr>
<tr>
<td>Third thesis draft (+ conclusion and recommendations + appendix)</td>
<td>October 16</td>
</tr>
<tr>
<td>Draft of thesis defense</td>
<td>October 31</td>
</tr>
<tr>
<td>Announcement of defense</td>
<td>October 31</td>
</tr>
<tr>
<td>Final defense presentation and practice run</td>
<td>November 7</td>
</tr>
<tr>
<td>Thesis defense and committee meeting</td>
<td>November 14</td>
</tr>
<tr>
<td>Final thesis submission to committee</td>
<td>November 25</td>
</tr>
<tr>
<td>Last day of internship</td>
<td>December 8</td>
</tr>
<tr>
<td>Deadline to submit thesis to University of Miami</td>
<td>December 14</td>
</tr>
<tr>
<td>Graduation</td>
<td>December 15</td>
</tr>
</tbody>
</table>
Appendix B – Final Presentation for SRG Meeting

Benchmarking of Maritime Security Training Requirements for the Centralized Training Academy

Angelica Sogor
September 15, 2011

Contents
- Historical Overview
- Significant International Policy and Stakeholders
- Comprehensive List of Training Topics
- Core Security Training Topic Categories
- Recommended Security Training Topic Categories
- Optional Security Training Topic Categories
Historical Overview

- 1948: Convention in Geneva which established the Inter-Governmental Maritime Consultative Organization (IMCO), as a specialized agency of the United Nations
- 1958: IMCO came into force, with its first meeting in 1959; the name changed to the International Maritime Organization (IMO) in 1982
- 1982: the Paris Memorandum of Understanding on Port State Control was adopted and entered into force

- 1985: IMO Measures to Prevent Unlawful Acts Which Threaten the Safety of Ships And the Security of Their Passengers and Crews, Resolution A.584(14)
- 1986: IMO issued MSC/Circ.443 on Measures to Prevent Unlawful Acts against Passengers and Crews On Board Ships
- 2010: Manila amendments to the STCW Convention and Code
Significant International Policy and Stakeholders

- Significant International Policy
  - IMO – Consists of SOLAS, STCW, Additional Measures, Model Courses, and Best Management Practices for Piracy
  - ISPS

- Stakeholders
  - EU – Consists of United Kingdom, The Netherlands, and Italian regulations; Paris MoU
  - U.S. – MTSA, CVSSA, SAFE Port Act, Coast Guard Naval and Vessel Inspection Circulars (NVIC), other agencies, and Model Courses
  - Non-EU Flag States – Consists of policies from the Philippines, Panama, the Bahamas; Indian maritime policies; and the Inter-American Port Security Training Program

<table>
<thead>
<tr>
<th>Topic</th>
<th>IMO</th>
<th>ISPS</th>
<th>EU</th>
<th>US</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal issues</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>ISPS</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat identification and mitigation</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Definitions and clarifications of duties</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Watchstanding and patrols</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Searches and inspections</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Ship security assessment and plan</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Topic</td>
<td>IMO</td>
<td>ISPS</td>
<td>EU</td>
<td>US</td>
<td>Other</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----</td>
<td>------</td>
<td>----</td>
<td>----</td>
<td>-------</td>
</tr>
<tr>
<td>Port facility security</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Drills and exercises</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Criminal response procedures</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Crowd management</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Self defense</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Topic</th>
<th>IMO</th>
<th>ISPS</th>
<th>EU</th>
<th>US</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documentation: incident reporting and record keeping</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Information and intelligence gathering and exchange</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Information security, confidentiality, and sensitivity</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Piracy</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Hostage survival</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Radiation protection</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Core Security Training Topic Categories

1. Technology
2. Definitions and Clarifications of Duties
3. Piracy
4. Ship Security Assessment and Plan
5. Documentation: Incident Reporting and Record Keeping
6. Information and Intelligence Gathering and Exchange
7. ISPS
8. Searches and Inspections
9. Legal Issues
10. Port Facility Security
11. Drills and Exercises
12. Crowd Management
13. Threats Identification and Mitigation

Recommended Security Training Topic Categories

1. Radiation Protection
2. Criminal Response Procedures
3. Watchstanding and Patrols

Optional Security Training Topic Categories

1. Self Defense
2. Hostage Survival
3. Information Security, Confidentiality, and Sensitivity
Appendix C – Photos from the Piracy Attack on the Seabourn *Spirit*

Damage that internalized in a cabin

Damage that internalized in a cabin
External damage

External damage
External and internal damage

Pirates who attacked the ship

Source: all photos received from Carnival Corporation & plc
Appendix D – Model Course Frameworks Analyzed in This Research

The MTSA model course frameworks are available for download at the following website:


The CVSSA model course framework is available for download at the following website:


IMO model courses are available for purchase directly from the IMO’s website:

http://www.imo.org/Publications/Pages/Home.aspx

Appendix E – Preliminary Condensed Syllabus for Carnival Corporation & plc

Condensed Syllabus

1. Introduction

The Introduction briefly explains the course and relates its purpose to the future duties and responsibilities of the trainee. The overview, facility description, and expected conduct reveal the course logistics. The competences to be achieved details what tangible results are expected from the trainees after the conclusion of the course. A brief overview of the Company and maritime operations relevant to the cruise industry provides basic background information for students.
1.1. Course overview

- Purpose: to provide security awareness and implement effective security operations onboard
- Describes course topics and their importance
- Review of timeline; with one 15 minute break in the morning, a one hour lunch break, and another 15 minute break later in the afternoon
- Course delivery: mix of theoretical and practical methods; lecture, complemented with scenario/role-playing, group discussions, and hands on/interactive training
- Supplies and lectures provided to students

1.2. Introduction of participants and facility

- Determination of experience levels

1.3. Course conduct

- Mandatory attendance unless absence approved in advance
- Only light refreshments allowed in classroom
- Questions, comments, etc welcomed at appropriate times
- Consequences of failure/non-completion and course completion certificate

1.4. Competences to be achieved

- Introduction
  - Knowledge of Company structure
  - Understanding of the unique nature of ships
- Threat Overview
  - Knowledge of threats to cruise security
  - Knowledge of global threat trends and patterns
  - Identification of weaknesses/issues in case studies
- Maritime Security Policy
  - Knowledge of major international regulations
  - Knowledge of the primary international regulatory code
  - Knowledge of applicable U.S. law
  - Understanding of relationship among U.S. law, international regulations, and Corporate policies
- ISPS
  - Understanding of the primary role of ISPS
  - Understanding of the requirements and applications of major ISPS sections
- The Role of Onboard Security Guards
  - Understanding the roles and functions of shipboard security guards
  - Ability to effectively screen and conduct searches of passengers, their effects, and the ship
- Ability to effectively patrol and monitor the ship’s interior and exterior
- Ability to preserve onboard crime scenes
- Ability to resolve disputes, control crowds, and exercise self-defense
- Ability to conduct surveillance as a means of maintaining ship/port interface security
- Ability to identify and respond appropriately to weapons, explosives, and drugs

- Shoreside Security
  - Understanding of the strengths and weaknesses of shoreside security
  - Understanding of the interaction between ship and shore security personnel
  - Identification and understanding of the discrepancies among strong and weak shoreside security

- Protecting the Ship
  - Understanding of how to apply threat warnings and security levels to actively protect the ship

- Drills and Exercises
  - Identification of different types of drills and exercises
  - Understanding of the value and importance of drills and exercises

- Information Collection and Reporting
  - Understanding of the importance of information collection and information security in maintaining ship security

- Security Administration
  - Understanding of basic written and verbal communication skills
  - Understanding of proper documentation and reporting processes
  - Understanding of security audits and inspections

- Transformation of Policies into Procedures
  - Understanding of how policies, procedures, and standards are transformed into plans and actions for specific criminal, terrorism, piracy, and civil unrest threats and incidents

1.5. The Company
- Describes the structure of the company

1.6. Cruise ships and port operations
- Unique nature of maritime trade and travel
  - Consideration of varying threats and responses while at high seas, in territorial waters, and at ports
- Basic nautical definitions
- Differences between a cruise and a passenger ship
- Differences between air and cruise travel
- Intermodal nature of transportation
  - Cruise ships and shore excursions
- Port operations, port communications, and secure/restricted areas around a ship in port
- Guidance on the access of public authorities, emergency response services, and pilots on board ships
- Provides awareness of the larger context in which threats and risks exist
- Basic knowledge and understanding of Port Facility Security Plan (PFSP) and Port Facility Security Officer (PFSO)

2. Threat Overview

A historical perspective and discussion of current threats offer background for the “why” behind this course. This section identifies major threats to safe and secure cruise ship operations. It summarizes incident statistics and discusses underlying motivations and results of notable incidents in the maritime domain. Along with case studies for specific types of threats, this section also provides an overview of direct or indirect economic consequences of an attack to further instill an appreciation for optimal and secure cruise and port operations. In this section, events will be briefly discussed in order to determine what lessons current security guards can learn. As the course nears its conclusion, these events will be revisited with the objective of trainees applying policies and skills to these real world situations.

2.1. Crime
- Differences between onboard and shore side crimes
- Example

2.2. Terrorism
- Background
  - Different types of threats:
    - The use of a small watercraft to cause damage to or destroy a larger ship
    - The use of a ship to cause damage to or destroy a channel or port facility
    - The hijacking of a ship (which may differ from a piracy scenario)
    - The uses of explosives, including suicide bombers, Improvised Explosive Devices, and Weapons of Mass Destruction
- Terrorist mindset, motivations, and methods
- Examples:
  - Hijacking of the Achille Lauro (1985)
  - Mumbai bomb blasts (1993)
  - Attack on the USS Cole (2000)
o Explosion onboard the Limburg (2002)
  o Attack on the M Star (2010)

- Prevention and detection
  o Importance of awareness and vigilance for things like suspicious behaviors and dangerous substances
- Response and reporting
  o Awareness of multiple attacks, such as on first responders, and multiple attackers

2.3. Piracy
- Background
  o Definition and geographical expansion
  o The pirates
  o Piracy in the cruise industry
  o Costs
- Trends and patterns
  o Effects of monsoons
- Strategies, targets, and equipment used
- International response and industry initiative
  o BMP4
  o IMO, STCW Manila Amendments
  o Government response from the Philippines
- Examples:
  o Hijacking of the MT Petro Ranger (1998)
  o Hijacking of the MV Alondra Rainbow in (1999)
  o Hijacking of the MV Inabukwa (2001)
  o Hijacking of the MT Han Wei (2002)
- Interaction with armed guards onboard
- In transit
  o General planning, company planning, ship master planning, voyage planning, self protective measures and maneuvers
  o Group transit procedures, speed, vigilance, and lookout
- If attacked
  o Contingency plan, ship security alert system, AIS, and evasive maneuvers
- If boarded
  o Overview of hijacking and hostage situations
- In event of military action
- Post incident
  o Reporting, debriefing, and counseling

2.4. Civil unrest
- How civil unrest could affect port operations and/or shore excursions
- Example

2.5. Trends of current global threats
Crime (physical and sexual assaults), terrorism (bombs, hijackings, suicide bombings, and lone wolf terrorists), piracy and armed attacks, contraband smuggling, cargo theft, collateral damage, civil unrest, suicide bombings, theft over $10,000, and stowaways and refugees

Need for heightened awareness

General processes and goals of:
- 1. Before threat: prevention and detection
- 2. During threat: mitigation and response
- 3. After threat: recovery and resilience

However, need to consider that responses of recovery often originate from plans and procedures that were established far before the threat surfaced; thus, it is also important to consider the integration of resiliency with prevention because preventative measures can encourage resilience even if they do not prevent an attack

3. Maritime Security Policy

Maritime Security Policy aims to further expand on introductory background of historical and current security threats and patterns by relating events to the policies that exist today. While an overview of applicable security policies is given, focus will be on ISPS, which is of great significance in the maritime industry. Basic definitions will be given, to aid in understanding of policy requirements. Legal implications of action/non-action address the importance of security personnel to understand their position in following policy requirements, without acting under authority of government or enforcement agencies.

3.1 Relevant international conventions and codes
- International Maritime Organization (IMO)
  - Convention on the Standards of Training, Certification, and Watchkeeping of Seafarers (STCW)
  - Convention for the Safety of Life at Sea (SOLAS)
  - The International Ship and Port Facility Security (ISPS) Code
  - The rapidity with which IMO acted to enhance maritime security following September 11 attacks
- United Kingdom Maritime Trade Operations (UKMTO)

3.2 Relevant U.S., E.U., and other legislation and regulations
- U.S.: MTSA and CVSSA
- E.U. Regulation #725 and Paris MoU
- Other: Philippines
3.3 Flag state requirements

3.4 Definitions
- Legal definitions
- Federal Bureau of Investigation (FBI)
- Reportable crimes in 46 U.S.C. Section 3507 (g)(3)
- Ship Security Officer/Vessel Security Officer
- Company Security Officer
- Ship Security Plan
- Port facility
- Ship/port interface and maintaining this security
- Ship to ship activity
- Port Facility Security Officer
- Designated Authority
- Recognized security organization
- Declaration of Security
- Security incident
- Security level
  - ISPS and MARSEC levels

3.5 Legal implications of action and/or non-action
- Identifies the legal limits of authority and the obligations of personnel with security duties
- Maritime jurisdiction law: understanding legal and jurisdictional boundaries as they relate to criminal activity/security incidents in the maritime environment, including the high seas and territorial waters
- No one is being trained to act as an agent of the government

4. ISPS

ISPS is the backbone for international maritime security policy. Its instruction is broken down into the following blocks: Security Roles and Responsibilities; Ship Security Assessment (SSA); and Ship Security Plan (SSP). Security Roles and Responsibilities introduces the role and function of onboard security guards, specifically as related to requirements of ISPS, and differentiates their duties from that of other involved parties. The Ship Security Assessment invokes an understanding of risks and vulnerabilities, which aim to be minimized in the Ship Security Plan. With comprehensive understanding of how the plan is implemented, the entire security staff can effectively work together, with awareness of how their individual roles result in a combined effort to enhance ship security.

Security Roles and Responsibilities

4.1. Contracting governments
• With respect to SOLAS and ISPS
• Exercise of port state control by different governments
  o Crew, ship, and passenger inspections by port facility personnel
• Required to ensure completion of a Port Facility Security Assessment for each of the port facilities within its territory
• Required to ensure Ship Security Assessments, Ship Security Plans, Port Facility Security Assessments, and Port Facility Security Plans are protected from unauthorized disclosure
• Should take amount of general and specific threat information into consideration when setting the security level (I, II, or III)
• Should provide contact details for government officers that a SSO, CSO, or FPSO can report security concerns to
• Should issue appropriate identification documents to government officials entitled to board ships or enter port facilities
• Should recommend that ships traveling within its territorial waters implement advised security measures
• Favorable treatment should not be given to ships who fly a flag that is not an IMO member

4.2. Recognized Security Organizations (RSO)
• Identifies the extent of its function
• How they can take on related activities of the contracting government
• Especially important for CSOs and FPSOs
• May advise or provide assistance to The Company or port facilities in developing security assessments and plans
• RSOs should be evaluated for their competencies

4.3. The company
• Responsibilities with respect to:
  o Ensuring Master has documents on board related to the crewing of the vessel and its employment, and the International Ship Security Certificate
  o Ensuring the SSP contains a clear statement emphasizing Master’s authority
  o Designating a CSO and SSO; ensuring they have support to fulfill their duties
  o Required to provide the Master of the ship with information to meet the requirements of the Company, such as: ship management companies, manning agents, contractors, etc.

4.4. The ship
• Compliance with SSP per set security level
• Implement safe manning provisions, including hours of rest, while still making sure the ship is sufficiently and efficiently manned
4.5. Port facility
- Compliance with ISPS
- Shall act upon security levels set by the administration within whose territory it is located
- Should be communication among the port facility, the Company Security Officer, and the Ship Security Officer for the Port Facility Security Plan; if there is no Port Facility Security Plan, another point of contact should be arranged to provide shore side security assistance/measures
- Communications of when a ship is denied entry to or expelled from a port

4.6. Ship Security Officer (SSO)
- Designation of a SSO
- Duties and responsibilities of SSO

4.7. Company Security Officer (CSO)
- Designation of a CSO
- May act as CSO for one or more ships provided the responsibility is clearly identified
- Several persons may be a CSO if responsibilities are clearly identified
- Duties and responsibilities of CSO

4.8. Port Facility Security Officer (PFSO)
- Designated for each port facility
- A person may be PFSO for one or more port facilities
- Duties and responsibilities of PFSO

4.9. Fleet and Port Security Auditor
- Reports to Director of Fleet Security

4.10. Security Coordinator

4.11. Security Supervisor

4.12. Security guards

4.13. Shipboard personnel with specific security duties
- Members of the ship’s crew may be assigned security duties in support of the SSP

4.14. Port facility personnel with specific security duties
- Personnel other than the PFSO may be assigned security duties in support of the PFSP

4.15. Other personnel
May have a role in the enhancement of maritime security

4.16. Actions required by different security levels

- 3 ISPS levels
  - Level 1: normal; the level at which the ship or port facility normally operates
    - Control of access to the ship
    - Screening all persons and their effects for weapons and dangerous devices
    - Designation of Restricted Areas
    - Screening of ship stores and luggage
    - Monitoring the security of the ship
  - Level 2: heightened; the level applying for as long as there is a heightened risk of a security incident
    - Increased security patrols
    - Increased access controls
    - Increased over-the-side lighting to see areas alongside the ship
    - Increased screening of people, luggage, and stores
    - Increased restrictions for visitors
  - Level 3: exceptional; the level applying for the period of time when there is the probable or imminent risk of a security incident
    - Continuous security patrols
    - Over-the-side lighting in all areas
    - Underwater inspections
    - Visitors refused onboard
    - Security searches of the ship
    - Posting of personnel at entrances to restricted areas
    - Stopping the loading of stores
    - Evacuation of the ship, if warranted

- Lists the security measures and procedures at the 3 security levels required to:
  - Ensure performance of all ship security duties
  - Control access to the ship
  - Control the embarkation of persons and their effects
  - Monitor restricted areas
  - Monitor deck areas and areas surrounding the ship
  - Coordinate security aspects of handling cargo and the ship’s stores
  - Ensure that security communication is readily available
  - Can be complemented with an in-class discussion and creation of a checklist detailing the appropriate generic actions given various conditions

Ship Security Assessment (SSA)
4.17. **Risk assessment methodology**
- Identifies weaknesses and vulnerabilities in physical structure, personnel protection systems, processes, or other areas that may lead to a security breach; suggestions for mitigation of these risks through developments and updates of the SSP
- Basic principles of risk assessment in day-to-day operations
- Regular inspections of the ship
- Assessments of risk, vulnerability, and threats
- Vessel risk profile
- Physical security

4.18. **Assessment tools**
- Use of checklists in conducting security assessment
- Ship layout
- Areas that should have restricted access
- Location and function of ship access points
- Open deck arrangement and height of deck above water
- Emergency and stand-by equipment
- Numerical strength, reliability, and security duties of crew
- Existing security and safety equipment for passengers and crew
- Existing arrangements with private security companies for ship and waterside security services
- Existing protective measures and procedures, including: inspection, control and monitoring equipment, personnel identification documents, communications, alarms, lighting, and access control

4.19. **On-scene security surveys**
- Preparations required prior to survey
- Lists procedures, measures, and operations to be evaluated
- Discusses the security aspects of a ship’s layout
- SSA should address the following elements onboard or within a ship:
  1. Physical security
  2. Structural integrity
  3. Personnel protection systems
  4. Procedural policies
  5. Radio and telecommunication systems, including computer systems and networks
  6. Other areas that may, if damaged or used for illicit observation, pose a risk to people, property, or operations onboard the ship or within a port facility
- Discusses importance and elements of physical security aboard the ship
- Describes significance of structural integrity for ships
- Discusses components and operations of systems to protect shipboard personnel
- States the role of proper procedures in preventing and mitigating security incidents
- Describes the use of information technology and communications in ship operations and in maintaining security
- Identifies other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations aboard the ship or within a port facility
- Discusses the identification of vulnerabilities in above areas and preparation of countermeasures
- States the importance of having in place emergency plans to deal with contingencies
- Explains and demonstrates how to carry out a security assessment with new plans in place and checks if further mitigating measures are required
- Those involved in a SSA should be able to draw upon expert assistance in relation to:
  1. Knowledge of current security threats and patterns
  2. Recognition and detection of weapons, dangerous substances and devices
  3. Recognition, on a non-discriminatory basis, of characteristics and behavioral patterns of persons who are likely to threaten security
  4. Techniques used to circumvent security measures
  5. Methods used to cause a security incident
  6. Effects of explosives on ship’s structures and equipment
  7. Ship security
  8. Ship/port interface business practices
  9. Contingency planning, emergency preparedness and response
  10. Physical security
  11. Radio and telecommunications systems, including computer systems and networks
  12. Marine engineering
  13. Ship and port operations
- Survey should:
  - Identify existing security measures, procedures, and operations
  - Identify and evaluate key shipboard operations that are important to protect
  - Identify threats and their likelihood to occur (prioritize security measures)
- Survey should evaluate measures for:
  - Ensuring performance of all ship security duties
  - Monitoring restricted areas
  - Controlling ship access and identification systems
  - Monitoring deck areas and areas surrounding ship
  - Controlling embarkation of persons and their effects
  - Supervising handling of cargo and ship store deliveries
o Ensuring security communications, information, and equipment are readily available

- The SSA should examine each identified point of access, including open weather decks, and evaluate its potential for use by individuals who might seek to breach security. This includes points of access available to individuals having legitimate access as well as those who seek to obtain unauthorized entry.

- The SSA should consider the continuing relevance of the existing security measures and guidance, procedures and operations, under both routine and emergency conditions and should determine security guidance including:
  1. The restricted areas
  2. The response procedures to fire or other emergency conditions
  3. The level of supervision of the ship's personnel, passengers, visitors, vendors, repair technicians, dock workers, etc.
  4. The frequency and effectiveness of security patrol
  5. The access control systems, including identification systems
  6. The security communications systems and procedure
  7. The security doors, barriers and lighting
  8. The security and surveillance equipment and systems, if any

- The SSA should consider all possible threats, which may include the following types of security incidents:
  1. Damage to, or destruction of, the ship or of a port facility, e.g. by explosive devices, arson, sabotage or vandalism
  2. Hijacking or seizure of the ship or of persons on board
  3. Tampering with cargo, essential ship equipment or systems or ship's stores
  4. Unauthorized access or use, including presence of stowaways
  5. Smuggling weapons or equipment, including weapons of mass destruction
  6. Use of the ship to carry those intending to cause a security incident and/or their equipment
  7. Use of the ship itself as a weapon or as a means to cause damage or destruction
  8. Attacks from seaward whilst at berth or at anchor, and attacks whilst at sea

- The SSA should take into account all possible vulnerabilities, which may include:
  1. Conflicts between safety and security measures
  2. Conflicts between shipboard duties and security assignments
  3. Watch-keeping duties, number of ship's personnel, particularly with implications on crew fatigue, alertness and performance
  4. Any identified security training deficiencies
  5. Any security equipment and systems, including communication systems
4.20. **Security assessment documentation**
- Upon completion of the SSA, a report shall be prepared, consisting of a summary of how the assessment was conducted, a description of each vulnerability found during the assessment and a description of counter measures that could be used to address each vulnerability. The report shall be protected from unauthorized access or disclosure.

**Ship Security Plan (SSP)**

4.21. **Purpose**
- Each ship carries a SSP approved by the Administration
- The SSP addresses measures that should be taken at each security level
- Detailed knowledge required for SSO and CSO, but trainees should have general knowledge, with respect to their assignments
- Monitored and reviewed by the Company and Ship Security Officers

4.22. **Contents**
- Shall establish procedures for the performance of ship security duties
- All SSPs should:
  - detail the organizational structure of security for the ship
  - detail the ship's relationships with the Company, port facilities, other ships and relevant authorities with security responsibility
  - detail the communication systems to allow effective continuous communication within the ship and between the ship and others, including port facilities
  - detail the basic security measures for security level 1, both operational and physical, that will always be in place
  - detail the additional security measures that will allow the ship to progress without delay to security level 2 and, when necessary, to security level 3
  - provide for regular review, or audit, of the SSP and for its amendment in response to experience or changing circumstances
  - reporting procedures to the appropriate Contracting Governments contact points
- All SSPs should be approved by, or on behalf of, the Administration. If an Administration uses a Recognized Security Organization (RSO) to review or approve the SSP, the RSO should not be associated with any other RSO that prepared, or assisted in the preparation of, the plan.

4.23. **Confidentiality issues**
- The SSP is a confidential document that must be protected from unauthorized access or disclosure
- Not generally subject to inspection by Port State Control
  - When and to what extent SSP may be inspected by Port State Control Officers

4.24. **Implementation**
- Shared responsibility by CSO and SSO, with SSO at frontline
- Need to clearly define who is responsible for what
- The importance of giving due regards to the effect that security measures may have on personnel who remain on board the ship for long periods
- Maintaining security of ship/port interface
- Usage of Declaration of Security
- Implementation of security procedures

4.25. **Maintenance and modification**
- Needs to be a dynamic document
- Route for suggesting modifications and approval necessary before a modification becomes new policy; amendments shall not be implemented unless approved by the Administration and flag state

4.26. **Declaration of Security**
- Explains what it is and what it addresses
- States who determines when it should be completed
- Lists the situations in which the ship can be required to have the DOS be completed
- States who is required to complete it
- ISPS details when it should be completed, who may initiate it, and who is required to sign it

5. **The Role of Onboard Security Guards**

The Role of Onboard Security Guards ties together requirements from ISPS with Carnival Corporation & plc security practices. These roles define the job objectives onboard, while this course defines the learning objectives that lead to effective understanding of and action in onboard duties. The different functions of security guards may vary in port, at sea, and in territorial waters, and this section also fosters the understanding that onboard security guards have physical duties, such as patrols, and less visibly obvious duties, such as behavioral screening, to continuously detect and minimize all types of threats. Where applicable, practical training will complement explanations of guards' duties.

5.1. **Screening**

  **Physical Screening and Search Methods**
• **Evolution of passenger screening**

• **Passenger and client relations**
  o Addresses issues of customer service and appropriate behavior and disposition for security personnel conducting screening procedures

• **Check point overview**

• **Special screening situations**
  o Religious/cultural clothing; persons with disabilities; children; and elderly

• **Screener awareness**

• **Equipment and systems overview**
  o Security latches and locks
  o Lighting
  o Time-sensitive key devices
  o Peep holes
  o Radio communications and hand held radios
  o Overboard detection equipment
  o Acoustic hailing device/long range acoustic device
  o Global Maritime Distress & Safety System (GMDSS)
  o Voyage Data Recorders (VDRs)
  o Automatic Identification System (AIS)
  o Ship Security Alert System
  o Automatic Intrusion Detection Device (burglar alarm)
  o General alarm
  o Closed Circuit Television Video (CCTV) Surveillance
  o Explosive and narcotics detection equipment
  o X-ray machines for baggage and containers
  o Metal detectors
  o RADAR
  o Hand held search wands

• **Operational limitations**
  o Limitations of individual items
  o Issues such as effective range, reliability, environmental sensitivities, and human error

• **Testing, calibration, maintenance, and storage**

• **Screening risks and protection**
  o Radiation Protection
- Principles, risks, and effects
- Protection when dealing with security equipment
- Protection when dealing with weapons and bombs
- Differences/similarities among atomic, biological, and chemical weapons
  - Weapons of Mass Destruction (WMD)
  - Dangerous goods and hazardous materials
    - Materials that are: radioactive, flammable, explosive, corrosive, oxidizing, asphyxiating, toxic, pathogenic, allergenic, or biologically/chemically hazardous

**PRACTICAL EXERCISE #1:** Screening checkpoint lab: hands-on application of operating technology with correct operational and precautionary measures

- **Access to recorded CCTV and images**
  - Understanding of who is authorized to obtain video surveillance records
  - Methods for sharing information with law enforcement officials
  - Retention of records
    - Ship policies should comply with need to provide law enforcement officials with a copy of all records of video surveillance that the official believes may provide evidence of a crime that has been reported

- **Methods of physical searches and non-intrusive inspections**
  - Unless there are clear security grounds to do so, members of the ship’s crew should not be required to search their colleagues or their personal effects
  - Searches of people, personal effects, baggage, stores, and onboard sweeps
  - Body check
  - Requirement and availability of female security personnel to conduct pat downs/searches on female passengers

- **Techniques used to circumvent security measures**
  - Smuggling, concealments, and covers; concealed weapons, knives, and swords; concealed firearms; body packing
  - Methods to evade security systems and controls

- **Preventing unauthorized access to ships and restricted areas onboard**
  - Stowaways

- **Implementing and coordinating searches**
o Searches should be planned in advance with detailed routes and places on the route where weapons, devices, etc. may be hidden; ensure plans have no overlap or omission; practice carrying out searches as a drill

o Check cards: color coordinated cards issued to each searcher for their area of responsibility; when all cards are returned, the search is complete

o Basic equipment for searches
  ▪ Flashlights and batteries
  ▪ Screwdrivers, wrenches, and crowbars
  ▪ Mirrors and probes
  ▪ Gloves, hard hats, overalls, and non-slip footwear
  ▪ Plastic bags and envelopes for collection of evidence
  ▪ Documentation and reporting forms

o Procedures to ensure effective search:
  ▪ Crewmembers should not be allowed to search their own areas
  ▪ Search should be conducted according to a plan and be carefully controlled
  ▪ Special consideration for search parties in pairs; one working “high” and one working "low;" one remains on guard while one reports finding
  ▪ Searchers should be able to recognize suspicious items
  ▪ Should have a system for marking “clean” areas
  ▪ Maintain contact with UHF/VHF radios, while understanding the dangers of using radios if near an Improvised Explosive Device (IED)
  ▪ Searchers should know responses upon finding a suspicious package, device, or situation
  ▪ Searchers should be aware a weapon or device may be intentionally disguised to match its location or context

o Familiarity with places that weapons or devices can be hidden
  ▪ Cabins
  ▪ Companionways
  ▪ Toilet and shower
  ▪ Deck
  ▪ Engine room
  ▪ Galleys and stewards stores

PRACTICAL EXERCISE #2: hands-on practice of conducting physical searches of people and their effects

Behavioral Screening
• Non-technological identification techniques
Not all threats may fall into visible categories of weapons, drugs, and explosives, and it is important to be able to identify suspicious activity and non-conformities.

Counter-surveillance and situational awareness
  - Watching for people, behaviors, objects, or operations that are out of the ordinary

Recognition of persons posing a potential threat to security

- Importance of observation in recognizing these persons
- Important to avoid gender, age, and ethnic stereotyping and profiling
- Patterns are useful, but each situation is different and should be treated as such
- Possible criminal behavior:
  - Persons using unwarranted excessive language that is obscene, derogatory, foul, etc
  - Persons groping themselves in the vicinity of children’s play areas
  - Persons who may be drinking excessively
  - Passengers attempting to establish relationships with crewmembers
  - Crewmembers attempting to establish relationships with passengers
  - Individuals offering sexual favors
  - Violent crewmembers and passengers
  - Mentally disturbed or suicidal crewmembers and passengers

Examples of behavior for other threats, beyond criminal activities:

- Behaving unusually, such as staring or quickly looking away from personnel or displaying anxious behaviors such as retracing steps
- Unknown persons attempting to gain access to vessels or facilities
- Unknown persons loitering in the vicinity of ships or port facilities for extended periods of time
- Unknown persons telephoning facilities to ascertain security, personnel, or standard operating procedures
- Unknown persons attempting to gain information about vessels or facilities by walking up to personnel or their families and engaging in conversation
- E-mails attempting to obtain information regarding the facility, personnel, or standard operating procedures
- Out of the ordinary phone calls
- Sudden and marked changes in behavior
- Questions about operations of the ship
- Requests for access to restricted areas
- A passenger whose ticket information is NOT identical with that in their passport
- A passenger who does NOT speak the language of the country of origin listed in their passport
- A passenger who has purchased a ticket, which seems incompatible with their means
- A passenger who arrives for embarkation either with no luggage or with so little luggage that it seems inadequate for the voyage time
- A person who arrives at the very last minute before sailing time and asks to purchase a ticket
- A passenger found wandering around in parts of the ship, which passengers do NOT normally frequent
- A passenger wandering around the ship’s decks at unusual hours or in unusual circumstances
- A passenger who remains in their cabin and does not come out for meals/recreation, but always orders meals brought to the cabin
- A passenger who shows signs of nervousness or fear
- A passenger who does not disembark on the shore excursions during the voyage
- A passenger who enters the dining room or other public rooms with items NOT USUALLY taken to such places, such as large valises, wrapped packages, or is strangely dressed
- A group of passengers who supposedly do not know one another, but who maintain contact through signals or gestures, who meet in quiet places on the ship, or who have identical items purchased in the same place, such as valises of the same sort, hats of the same sort, etc

5.2. Watch Standing
- Control, monitoring, and patrol of the ship’s interior and exterior areas
- Restricted areas
- Security personnel bearing/disposition (posture, tone of voice, etc)
- Prudent night round duties and reporting

5.3. Crime Scene Preservation
- Understanding crime
  - Physical and sexual assaults
  - Homicide/murder
  - Drug trafficking
  - Prostitution
  - Arson
  - Piracy
  - Terrorism
- Excessive use of alcohol and its effect on crime
- Missing persons
- Theft over $10,000
- Firing at or tampering with vessel
- Those who are likely to commit crimes

- **Representative incidents in the international maritime environment**
  - Incident statistics and underlying motivations and results

- **Prevention**
  - How criminals identify their victims
  - Where crime is likely to occur
  - Vigilance is important in preventing crime

- **Detection**

- **Investigation and response: initial actions and subsequent responses from guards**
  - Causes for investigation:
    - Observation by crewmember of a reportable incident
    - Anonymous hot line tip
    - Passenger complaint to security
    - Personnel complaint
    - Shore side contacts
    - Government agencies
    - The company
    - Port merchants
  - Definition of an investigation
    - Observations (what did you see, hear, smell, feel, etc)
    - Interviews (informants, victims, suspects, and witnesses)
    - Statement taking (what a person saw, what they were told, what they did, and what they know)
    - Report writing (investigator summary of the investigation)
    - Logs (crime scene log, evidence log, detention log, and photo log)
    - Evidence collection (clothing, bedding, injuries, and sexual assault kit)
    - Photography
  - Techniques used by law enforcement
  - Restriction of access to passenger staterooms and crime scenes
    - Crime scene may require enhanced control measures
  - Investigative methods
    - Law enforcement may prefer employees not enter a crime scene; should be done only if necessary
• First priority: your safety and the safety of others, including providing assistance to the injured
• Assist injured people in a manner that is minimally destructive to potential evidence at the scene
  • For example, when cutting clothing try not to cut through bullet holes or stab wounds
• Obtain all information possible regarding the original condition of the crime scene. If possible, preserve the initial scene response with photographs
• Use photo log to index photos
• Photograph, at eye level, the original scene as soon as possible
  • Points of entry and exit
  • Surrounding area
• Secure photographs
• Overall, medium, and close range photos
• If using digital photography:
  • Maintain photo log
  • Keep original digital media card secure
  • Do not delete any photos
  • If possible, start with a clean card
• Helpful to have photographs and blueprints of the ship
  o If you must enter the scene, record your entry into the scene and all subsequent findings
    • Unauthorized persons should be prevented from entering
    • Anyone who enters may have to testify at any future criminal proceeding
    • Log: names, employee numbers, date, and time of arrival and departure
  o When responding to a crime scene, take steps to accurately record and document the important aspects of the scene
    • Where, who, what, when, why, how
  o Take extensive notes – do not rely on your memory or the memory of others present at the scene; include a rough sketch of the scene with a notation that the sketch is not to scale
  o Do not allow anyone to move or alter the scene
    • Secure scene until law enforcement has processed and released the scene
    • Tape off the parameter
  o Document any persons, ships, boats or vehicles near the scene
  o Victims, witnesses and suspects must be removed from the scene and separated to prevent them from purposely or inadvertently altering or destroying the evidence
  o If suspects or witnesses attempt to leave or depart the ship, obtain complete identification and any additional information that can assist in locating these individuals at a later date
Steps should be taken to maintain all ship or dock surveillance videos of the scene for the time period directly before and after the time the incident is believed to have occurred.

Maintain and preserve door lock logs and video camera footage.

A minimum two-person entry team per scene is recommended. Should a significant evidentiary find be noted or seen, both persons should observe and document the evidence in place. Document all personnel that come into contact with evidence.

Consider contamination issues prior to entry:
- Clean, protective clothing
- Clean socks or clean plastic bags over shoes
- Plastic or rubber gloves
  - Should be changed for each item of evidence if fluids, fibers, or other substances that could easily be transferred are collected
- Hair net or hat

Follow a cleared route for personnel going into and out of the crime scene.

Use marking tape to designate cleared areas.

Avoid wandering over the scene or tracking small particles referred to as trace evidence from place to place, for example: hairs, fibers, or other small items of evidentiary value.

Take your time and do not rush.

Be alert for all forms of physical evidence.

Be cautious to not lose or destroy evidence.

Look everywhere.

**Evidence collection, handling, and storage**

- Especially important for: sexual assault; homicide; suicide; poisoning; property crime; drink spiking; drug trafficking; acts of terrorism.
- Seal and label evidence correctly.
- Should only be attempted if the evidence would be destroyed because the scene cannot be secured or the evidence would be lost for another reason.

Paper bags:
- Provide excellent breathability, which prevents moisture buildup that can destroy DNA evidence.
- Package all clothing and biological items in paper.
- Good for fiber evidence as paper does not generate static electricity.

Plastic:
- Good for dry items, powders, tablets, paper items, fingerprint evidence.
- Wet or damp items should not be placed in plastic packaging.
- Should be used for drug evidence.
- Nylon bags
  - For items to be checked for explosive residue
- Cardboard boxes
  - Good for heavy items
  - Not recommended for trace material such as hairs and fibers
  - Excellent for guns and knives
- Glass jars and vials
  - Blood samples, liquids, flammables, liquids for date-rape drugs
  - Paint cans
  - Explosive samples
  - Items with accelerants
- Labeling evidence should include:
  - Ship identifier
  - Date of collection
  - Item number
  - Description of evidence
  - Location where item was found
  - Name of evidence finder, with initials (on label, not evidence)
  - Name of second person that witnessed collection, with initials (on label, not evidence)
- Procedures for collecting different electronic evidence
  - Computer; networked or business computer; other electronic storage device
  - Wireless telephone
  - Cordless telephone
  - Answering machine
  - Caller ID device
  - Electronic paging device
  - Facsimile machine
  - Smart cards and magnetic strip cards
  - ID card printers
  - Printers
  - Copiers
  - Compact Disc duplicators and labelers
  - Digital cameras/video/audio
  - Electronic game devices
  - Home electronic devices
  - Global Positioning System
  - Personal Data Assistants/hand held computers
  - Vehicle computer devices
  - Tracking an internet email

- Chain of custody and (potential) response of government agencies or law enforcement
  - U.S. has investigative jurisdiction for crimes if:
- The ship, regardless of flag, is a U.S.-owned vessel, either whole or in part, regardless of nationality of victim or suspect
- Crime occurs in U.S. territorial waters (within 12 miles of the coast), regardless of nationality of victim or suspect
- Victim or suspect is a U.S. national on any vessel that departed from or will arrive in a U.S. port

- **Reporting**
  - Notification of authorities, operating lines, the Corporation; who and how to contact them
  - Database reporting, evidence log, and sign-in log
    - Maintain and preserve door lock logs
    - Evidence log
      - Detailed description of the evidence
      - Date and time the evidence was collected
      - Specific location where the evidence was collected
      - Who collected the evidence
      - Where the evidence is stored
  - Crimes that need to be reported according to CVSSA
    - Homicide
    - Death
    - Missing U.S. national
    - Kidnapping
    - Assault with serious bodily injury
    - Firing or tampering with vessels
    - Theft greater than $10,000
    - Sexual assault
    - Rape

- **Interviews and statements**
  - Statement written by witness or dictated directly to the investigator; signed by witness and witnessed by a company representative
  - Interview of informants, victims, suspects, and witnesses
    - Consideration of: tone of the conversation; environment (location and feel); establishment of rapport; non-judgmental; do not interrupt answers; avoid giving perception of consequences
    - Report: factual summary of the whole investigation; summary of incident; summary of statements; observations; actions, and disposition
    - When (date and time), who (their relationships and contact details), where, what happened, why (if known), and how (if known)
  - Clarification of what criminal activity needs to be reported vs. that which can be voluntarily reported
Summary of: what you were told, what you saw, what you did, statements taken, and findings/conclusions

- **Variance in procedures**
  - Arson
  - Homicides/serious physical assault
    - Secure all involved (state)rooms and areas
    - Photograph victim prior to movement or removal
    - Secure body of deceased in refrigeration
    - Secure all weapons and potential weapons
    - Separate and relocate all involved parties
    - Ensure that investigators oversee and document removal of any and all items from rooms
    - Attempt to obtain consensual blood, urine, and DNA samples from suspect and victim; refrigerate blood and urine samples
      - Can be useful for alcohol, drugs, and date rape drug analysis
  - Sexual assaults
    - Rape kit performed by ship’s doctor
    - Secure victim and suspect rooms
    - Preserve trash, bed linens, and under garments in victim and suspect rooms
    - May be observed by a security guard of the same sex
    - If possible, have the subject and/or victim disrobe over butcher paper to collect any loose or falling trace evidence. Package this paper in the same container used for the subject or victim’s clothing
    - Separate all involved parties
    - Attempt to obtain consensual blood, urine, and DNA samples from suspect and victim; refrigerate blood and urine samples
      - Can be useful for alcohol, drugs, and date rape drug analysis
  - Suicide and poisoning/drink spiking
    - Suicide prevention and awareness training
    - Secure any weapons, poisons, drinks, drink containers, pills, etc
    - Photograph victim prior to removal
    - Hangings, if victim is obviously dead and life-saving measures have been deemed futile by medical personnel:
      - Do not untie any knots
      - Cut victim down away from all knots
      - Maintain body in refrigeration
• Keep all notes, writings, etc of the victim and their associates
  o Battery, property crimes, and drug trafficking
    ▪ Keep all notes, writings, etc of the victim and their associates
    ▪ Secure all involved (state) rooms where incident occurred
    ▪ Secure all potential evidence and contraband
    ▪ Separate and relocate all parties
    ▪ Photograph victims and evidence
    ▪ Take close up photo of injuries
    ▪ Be aware of multiple co-conspirators
    ▪ Be aware that drugs may not be in clearly recognizable forms

• Victim and witness sensitivity and awareness

PRACTICAL EXERCISE #3: scenario with staged crime scene that practices detection, investigation, response, scene entry/processing, and evidence collection; scenario followed with hands-on practice of reporting and documentation of a crime, as well as role-playing to practice victim and witness awareness and sensitivity

5.4. Dispute Resolution
• Crowd Management and Control
  o Understand responses to various ship alarms
  o Importance of crew response as a unit
  o Requires knowledge and understanding of ship layout
  o Description of basic psychology of a crowd onboard a cruise vessel
  o Motivations and mindset of passengers and other personnel
    ▪ Disbelief; fear of starting panic; want to confirm accuracy of warning; panicked response with irrational behavior; instinctive reaction to look for members of their group; attempt to seek safety in seemingly safe places
    ▪ Stress and its effects
  o Methods, purpose, and importance of education and awareness of passengers and crew
  o Measures to publicize crime/incident prevention
  o Effective communication with passengers during an emergency
    ▪ Speak with confidence and authority
    ▪ Be assertive
    ▪ Speak slowly and concisely
    ▪ Only speak what you know, do not guess
    ▪ Consideration of language barriers
    ▪ Bi/multi lingual crew and passengers
    ▪ High visibility clothing
- Making the general public aware of security and safety tips
- Mustering procedures
- Assist passengers en route to assembly and embarkation stations

- **Self Defense**
  - Self defense techniques
  - Handcuff and restraint training
  - Introduction with primary and intermediate control skills

**PRACTICAL EXERCISE #4**: staged scenario mimicking shipboard crisis with panicked passengers and security guard that needs to effectively control the situation and communicate with passengers; hands-on practice of self defense mechanisms

5.5. **Surveillance**
- Maintaining security of the ship/port interface

5.6. **Threat identification, mitigation, and response**
- Identification of weapons
  - Firearms, knives, and swords
  - Describes the damage they can cause and their appearance
- Identification of drugs and narcotics
  - Overview
    - Methods of introduction of illicit drugs onboard
    - Methods to detect and deter drug offenders
    - Equipment to detect and identify drugs on board
    - Basic understanding of origin, composition, and appearance of drugs capable of identification onboard
  - Commonly abused
  - New
  - Describes the damage and/or behavioral changes they can cause
- Identification of explosives/devices
  - Atomic, biological, or chemical weapons
  - Weapons of Mass Destruction (WMD)
  - Package bomb: no return address; strange odor; wrong title or name; lopsided packaging; oil stains on wrapper; protruding wires
  - Differences among military, commercial, high explosive, and Improvised Explosive Devices (IEDs)
  - Describes the damage they can cause and their appearance
  - Procedures for phone calls, written notes, emails, and person-to-person/direct threats
  - Use of bomb suppression blanket
- Response when weapons, drugs, dangerous substances, and explosives/devices are identified
- Responses for weapons
- Responses for drugs
- Responses for explosive devices

**PRACTICAL EXERCISE #5**: hands-on exercises using technology and search techniques to detect and identify weapons, drugs, and/or explosives; discussion of appropriate responses if items are detected

### 6. Shoreside Security

Shoreside Security expands on Maritime Security Policy by noting how policies may not be applied equally in all countries or ports. Although operating line specific training can address specific ports of major concern that are most applicable to that line, this section uses a few notable examples to emphasize the importance of shipboard crew security training, as security measures at ports can differ widely in the world.

#### 6.1. Countries, flag states, and ports visited by Carnival Corporation & plc

- Description and comparison of maritime security and implementation of policies in locations most applicable to all of the operating lines

#### 6.2. Countries and/or ports with high security standards

- Acknowledgement of locations with high security standards that complement Carnival's goals and practices

#### 6.3. Countries and/or ports with low security standards

- Acknowledgement of locations with low security standards that limit Carnival's goals and practices

#### 6.4. Importance of ship security independent of port security

- Description of how thoroughly trained employees can counter security limitations at ports

### 7. Protecting the Ship

Protecting the Ship focuses on how different elements are incorporated into security procedures onboard a ship, especially as the ship is entering a port. As the 3 subtopics (security levels, flag state role, and contracting government role) have already been introduced in the course, this section further addresses how ship security personnel interpret and apply different policies and regulations from ISPS, from a flag state, and from other governments. The focus is no longer on the definition or general role of these elements, but how they are actively applied to maintain a secure ship, particularly at a ship/port interface.
7.1. ISPS and MARSEC security levels
- Implementation of actions at Level 1
- Implementation of actions and changes at Level 2
- Implementation of actions and changes at Level 3

7.2. Flag states
- Application of flag state requirements

7.3. Contracting governments
- Interpretation of government threat warnings

8. Drills and Exercises

Drills and Exercises addresses how the knowledge, skills, and responses learned in this course will continue to enhance security even when no visible threats or incidents arise. Continued comprehension and practice of security measures through drills and exercises, and assessment of those practices, reinforces the learning objectives and aims of this course.

8.1. Emergency procedures and contingency planning
- Discusses action to take in case of a breach of security
- Discusses contingency plans for:
  - Hijacking
  - Bomb threats
  - Unidentified objects/explosives
  - Damage to/destruction of port
  - Piracy attack
  - Terrorism attack
  - Stowaways

8.2. Security drills and exercises
- Drills should be conducted at least once every 3 months
  - Where more than 25% of the ship’s personnel have been changed at any one time with personnel that have not previously participated in any drill on that ship within the last 3 months, a drill should be conducted within 1 week of the crew change
- Exercises should be carried out at least once each calendar year with no more than 18 months between the exercises
- Reflective of probability of specific threats, but also have a balance of scenario diversity to enhance responder awareness and preparedness
- On ship and with port facilities
- Actual security event may substitute for an equivalent drill or exercise
8.3. Assessment of drills and exercises
- Audits, reviews, inspections, and verifications

9. Information Collection and Reporting

Information Collection and Reporting is an imperative element of threat identification and security preparedness. This section is divided into basic gathering, assessment, and exchange of information, as addressed in ISPS, to encourage a sense of situational awareness based on available information and communications. The advanced section expands beyond what is referenced in ISPS and aims to educate ship security guards in a similar fashion to security guards from other industries to further assist in understanding, and thus being able to successfully counter, terrorism and piracy threats. As Information Collection and Reporting will reveal and communicate sensitive security topics, it is imperative that those involved in such communication appreciate and protect the sensitive and confidential nature of security plans, records, reports, and communications. This section details specific information that should be protected, including information that is part of an Information Technology (IT) system. This section is complemented by practical training that stages a scenario that requires proper information collection and reporting to occur prior to entering a port.

9.1. Basic (ISPS)
- Gathering, assessing, and exchanging information
  - More specifically, collection and appropriate dissemination of information about port conditions before entering the port
  - Transferring knowledge of security risks and threats into security actions prior to entering a port
- Maintenance of communication
- Situational awareness

9.2. Advanced
- Foreign intelligence
- Counterintelligence and counter surveillance
- Mindset, motivations, and methods of terrorists and pirates

9.3. Information and communication security
- What information is protected
- Personal and medical sensitive information and importance of keeping it confidential
- Additional confidential records
- The collection, use, and disclosure of confidential information should be limited to authorized personnel with a need to know

9.4. Information Technology (IT) security
• Records may be kept in an electronic format; shall be protected by procedures aimed at preventing the unauthorized access, destruction, or release of confidential information

PRACTICAL EXERCISE #6: scenario that recreates the process of ship personnel entering a port with certain security risk and threat assessments, and the group must facilitate discussion of how to interpret information, and they will ultimately be required to decide what prudent actions should be taken to reflect the port’s condition and carry out these actions; discussion/list-making of what is considered secure information and what is not

10. Security Administration

While the subtopics of Security Administration may have been addressed briefly in other course topics, this section expands on administrative factors that, when fulfilled, will lead to successful implementation and application of the academy’s curriculum. Some of the basic skills to ensure proper Security Administration include written and verbal communication abilities, as well as accurate documentation and record keeping, which include the reporting of non-conformities. This section is complemented by practical training with practice of basic ship communication skills and practice of reporting different types of security incidents.

10.1. Written and verbal communication skills
• Interpersonal skills that foster positive communications among crewmembers and between crewmembers and passengers
• Knowledge and understanding of nautical terminology that is relevant to maritime operations
• Ability to report and document a security incident
• Knowledge of proper methods and routes of security-related communications

10.2. Documentation and record keeping
• States documents that shall be available on board at all times
• Describes the International Ship Security Certificate, its validity and verification requirements
• States the requirements of the Continuous Synopsis Record and what it shall contain
• States the activities for which records shall be kept on board and the duration for which they should be retained
• What records are to be kept and for how long
• Verification and certification of ships
• Reporting security incidents
- Verification of identification and travel documents for passengers; genuine vs. forged notes

10.3. Monitoring and control
- Role of SSO to review the SSP and the implicit responsibility of the Master in this regard

10.4. Security audits and inspections
- States the requirements for carrying out internal audits and inspections

10.5. Reporting non-conformities
- States the requirement for reporting non-conformities and deficiencies identified during internal audits, periodic reviews, and security inspections

PRACTICAL EXERCISE #7: practice written and verbal communication skills based on example documentation, logs, and communications; discussion with instructor giving an example of different security incidents and trainees respond with how the given incident should be reported and documented, if necessary

11. Transformation of Policies into Procedures

This section combines lecture-based discussion of notable case studies with practical training of staged security threats and incidents. Case study analysis provides a way for students to understand the events and possibly mistakes that have led to successful security attacks or incidents, with a goal of students able to provide insight, based on knowledge acquired in this course, as to how those events could have prevented or mitigated. The practical training part of this section applies policies, equipment, and skills to real world events that may occur in cruise ship operations. After assessments, plans, and procedures have taken place, the shipboard security guard must now enact those into real prevention and response measures on the ship. A discussion-based lecture will circulate these ideas and plans, while practical training requires students to actively demonstrate they have achieved comprehension of course learning objectives.

11.1. Crime
- Case study

11.2. Terrorism
- Case study

11.3. Piracy
- Case study
11.4. Civil unrest

- Case study

PRACTICAL EXERCISE #8: Series of staged scenarios that may occur during a typical cruise operation, from the boarding and screening of passengers to the arriving at a port and the disembarkation of passengers for a shore excursion; at least one scenario comes from the topics outlined in 11.1 – 11.4, for a minimum of four scenarios that practice prevention and mitigation measures; examples: report of a murder onboard while in international waters; detection of a possible IED during screening; suspicious small boats approach a cruise ship off the coast of Yemen; reports of shootings in tourist areas while entering a port

12. Course Review

13. Evaluation