INTELLIGENCE SHARING

IN MARINE PORT SECURITY OPERATIONS

Presidia Security Consulting | www.presidiasecurity.com | 613.883.7805

Introduction

Since 9/11 marine port security has been the subject of increased scrutiny as it is clear that, through these access and egress points into both Canada and the United States, flows much undetected and uninterrupted contraband. Numerous reviews initiated by the United States Government Accountability Office (GAO) and the Canadian Standing Senate Committee on National Security and Defence have clearly articulated that ports are a haven for criminal activity and organized crime, as well as targets for potential terrorist activity. Both these reviews demand an increase in the level of intelligence sharing amongst partner agencies focused on policing and security of marine port operations.

Discussion

Marine ports are complex working environments. They include many commercial entities complemented by multiple regulatory and law enforcement agencies, each with a key role in the maintenance of legislative compliance and the overall provision of security services. It is most evident that our, marine ports are a vital component of both Canadian and United States economies. To understand the economic impact of our ports one must recognize that shipping today represents more than 90 percent of world trade. One average size container ship represents approximately $30-$50 million of cargo.[1] Currently, it is estimated that Canada's Port Authorities handle more than 460 million tonnes of cargo annually amounting to approximately $162 billion worth of goods.[2] Not surprisingly with the United States this impact is exponentially larger. For example in 2006 it was estimated that the American marine cargo activity generated a total of $1, 975.4 billion of total economic activity.[3] These figures clearly demonstrate that North American marine ports are an attractive transportation and supply nodes that, if not properly controlled ,provides a fertile ground for criminal and terrorist related activity and threatens our overall national security

For many years' Canadian law enforcement has been aware of the threat posed by organized crime at marine ports. With the poignant disbanding of the Ports Canada Police in 1997 port enforcement responsibilities shifted entirely to local police agencies and private security

[1] *http://www.acpa-ports.net/industry/industry.html*

[2] *http://www.acpa-ports.net/industry/industry.html*

[3] *The Local and Regional Economic Impacts of the US Deepwater Port System, 2006, page 6*

companies. In 1998, Criminal Intelligence Service Canada (CISC) began reporting on the organized criminal threat at Canada's marine ports and, in March 2000, established a National Working Group to coordinate information and intelligence sharing pertaining to organized crime in marine ports[4]. This reporting continued until approximately 2005 when CISC changed its focus and commenced reporting on the various "criminal markets". However, it is clear that Canada's marine ports continue to provide an environment well suited to illicit activity. Though the events of 2001 heightened our security awareness including additional concerns regarding our marine ports, they remain a major conduit into North America for illegal individuals and continue to be our Achilles heel from an enforcement and security perspective.

Within Canada, there have been numerous reviews and studies pertaining to the security of marine ports, in particular the Senate Standing Committee on National Security and Defence which has been very active and focused on this area of vital interest. In 2007 it released a follow-up report to its 2003study. This latest report was entitled "Canadian Security Guide Book - An Update of Security Problems in Search of Solutions – Seaports"[5]. The report provided an update on the recommendations made in 2003, along with new recommendations. One of the main issues, made most clear in this report, is the multitude of agencies that are involved in the venue of marine port security. They include Public Safety Canada, Royal Canadian Mounted Police, Canada Border Services Agency, Transport Canada, Canadian Coast Guard, Department of Fisheries and Oceans, provincial and municipal police services as well as the Department of National Defence, not to mention the many private security agencies engaged to protect the assets of numerous commercial companies within the marine port environment. Although several actions have been taken to address marine port security, such as the development of Integrated Port Enforcement Teams (IPET) and Marine Security Operations Centres (MSOC), the timely collection and passage of security and police related information and intelligence continues to be a challenge. This is not expected to change anytime soon until leadership, coordination and accountability matters are more clearly defined. Today, for the most part, for proprietary concerns, agencies continue their stove pipe in orientation and one can appreciate this situation is further exacerbated and magnified for intelligence operations in support of marine port security in the United States.

A plethora of studies, inquiries, reviews and articles have highlighted the problems associated with the sharing of security and law enforcement intelligence. Even with tragic events such 9/11, and the subsequent report by the National Commission on Terrorist Attacks Upon the United

[4] *http://www.cisc.gc.ca/annual_reports/annual_report_2003/ports_2003_e.html*

[5] *Canadian Security Guide Book - An Update of Security Problems in Search of Solutions – Seaports, Senate Standing Committee on National Security and Defence, March 2007*

States (the "9/11 Commission Report") police and intelligence agencies still struggle with the processes for the robust and timely sharing of information and intelligence. These issues of sharing are often tied to "inter-agency turf wars", stove piping of information, lack of common standards and practices and regulatory barriers (such as Access to Information and Privacy Acts and Freedom of Information Acts). The biggest challenges in developing technologies that support the sharing of information in a seamless manner, are the quagmire of bureaucracy and the lack of focussed leadership when advancing various intelligence related initiatives through the government procurement processes.

However, it is important to note that although there are many challenges and struggles there have been some clear successes; such as the IPETs and MSOCs mentioned earlier. Within several jurisdictions in the United States, efforts have been made to find innovative solutions in the development and sharing of intelligence related to marine ports. In the area of stakeholder coordination and collaboration_initiatives, there have been activities under the Area Maritime Security Committees (AMSC). AMSCs serve as forums for local seaport stakeholders from federal agencies, state and local government, law enforcement, and private industries to gain a comprehensive perspective of security issues at the nation's seaports. In addition to the Area Maritime Security Committees, several ports have created other methods by which they can share information and intelligence through protocols for detecting and monitoring port-related security risks and systems for increasing intelligence-sharing.

Some of these efforts are undertaken daily, such as daily security briefings held at the Port of Boston involving local, state, and federal law enforcement, as well as representatives of private industry, to discuss information that might be relevant to security at either the port or Logan airport. Another good example is the San Diego Harbour Police Homeland Security Unit which coordinates community outreach and public awareness campaigns to make port tenants, marina residents, hospitality workers and others more aware of terrorist activities and how to report them.[6] One other progressive initiative is the Maritime Security Initiative (MSI) developed by the New Jersey State Police Marine Services Bureau (MSB). It addresses the changing trends in terrorism and other criminal activities, within maritime communities. The Maritime Security Initiative recognizes the current trends while increasing port security and developing maritime intelligence. The MSI program encourages the development and sharing of intelligence and relies on the development of a combined Intelligence Base(?), and Community Outreach program, through the building of cooperative community and corporate partnerships. The

[6] *Protecting America's Ports: Promising Practices, Police Executive Research Forum, January 2008*

various partners can now report suspicious activities directly to the New Jersey State Police using the internet.[7]

There has been some advancement in Canada and the United States in particular as it pertains to the sharing of intelligence in support of marine port security operations, however, still much more must be addressed. As demonstrated by various initiatives in the United States, it is important for any marine port intelligence program to be "holistic" in nature and to include both government and private entities. Additionally, initiatives and objectives must be clearly defined and dedicated leadership accountable for achieving these goals and objectives as the situation dictates. This is essential for ensuring the protection and regulatory functioning of each of our Ports. Such direction and focus will erode and at some point eradicate illicit activity of organized crime, petty criminals and terrorists that continue to use our ports as a transportation backbone for their activities. In the absence of this coordination, ports will continue to be an environment rich in potential for many illicit activities. Though oft articulated, through numerous reviews and studies, it is time for our security and law enforcement agencies to overcome the often "self imposed" barriers and to begin sharing intelligence in a well planned strategic manner. Part of the answer will be to develop a "public-private partnership" to build a secure web-based information sharing platform that will allow the various entities involved in marine port security to contribute unclassified information in a timely manner. Only by actively engaging all partners in the collection and sharing of intelligence can proper security of our marine ports be realized. Marine Port security is vital to the economic viability of Canada and North America and, as such, it is crucial that proper intelligence sharing support this important function. It is time for Canada to develop a central organization, complete with legislative authority to establish its responsibility, to report to government annually on the security and law enforcement status of this country.

Conclusion

It is extremely important for all organizations to ensure that they have the proper strategies in place to minimize the risk to their core business functions and their employees. Ensuring that administrative investigations are conducted in a professional and focused manner is one of those strategies.

[7] *njsp.org/maritime*

About the Author

W.H. (Bud) Garrick

W.H. (Bud) Garrick has more than 30 years of experience in the realm of police and security operations both domestically and internationally. He served with the Canadian Forces Military Police for 27 years, retiring as a Lieutenant Colonel and Commanding Officer of the Canadian Forces National Investigation Service, upon retirement he assumed the position of Deputy Director General for Criminal Intelligence Service Canada. He is currently the Vice President of Presidia Security Consulting.

Additional Articles from Presidia Security[8]

Ask the Question – What is Your Security Strategy?

Security is often thought of as a tactical issue that should remain at the "gates and guards" level. While these tactical security pieces may be important they are most effective as part of a security strategy that is designed to mitigate the threats and risks to your company and its operations. True security strategy is integrated into a company's "C Suite" and is seen as an enabler. The questions and discussion that follow outline the framework for a company security strategy.

Assessing and Tracking Threats - Protecting Your Employees and Your Company

Recent incidents of violence in the workplace in Canada tragically illustrate what happens when threats materialize into actions; they serve as a stark reminder to businesses across the country of their responsibility to protect their employees in the spirit of "due diligence" and "due care and attention." Rarely, if ever, do these violent situations manifest themselves without some sort of prior indicators. This underscores the importance of having proper procedures in place to track and assess threats to your employees. Take the time to review the following recommendations to determine whether your company is prepared to address threats to employees.

Executive Protection Considerations

In today's fiscally challenged business environment it may be difficult to justify providing an Executive Protection Program for an organization's key executives. However, in making this important decision one also has to consider what the cost would be to the organization's bottom line and, perhaps more importantly, to its reputation should a key member of the senior leadership team be the target of an act aimed at harming or embarrassing the individual and the organization.

Due Diligence Investigations

If asked, many companies would say that they have "due diligence investigation" processes in place; however, these processes are often designed to review the financial and operational affairs of a particular company and fail to closely inspect the background of the main principals or executives of the company. In addition, many companies do nothing more than cursory checks on individuals they are about to hire. The lack of a robust background investigation can result in wasted time and can cause legal and financial problems. There is an abundance of legal findings across Canada, as well as internationally, that clearly articulate the liability facing companies who do not carry out appropriate due diligence investigations. In order to inspect this issue closer one must first begin with a definition and understanding of what "due diligence" consists of.

Take a Moment to Celebrate Success

Take a moment today to think about the successes you have had and the team that got you there. It is well worth it.

---

[8] *Available online at our website: www.presidiasecurity.com/library.html*

A Solid Foundation for Administrative Investigations

"Is it time for the implementation of standards, including proper training and oversight, as it pertains to the conduct of "administrative investigations"? It could be argued that administrative investigations are purely "administrative" in nature and as such there is no requirement for an enhanced capability. However, it can also just as easily be argued that these types of investigations can have a very negative impact on the lives of those being investigated, including the potential loss of their livelihood. They also bring with them a large degree of "personal and institutional liability" on the part of those individuals conducting the investigations and the" "organizations for which they are employed."

Setting up an Intelligence Hub - Published in FrontLine Magazine

Intelligence in some form is in use today across a broad spectrum. No longer just the purview of Government entities, business intelligence is a common term and practice among corporations. Today, in the internet age, there is an abundance of readily accessible information about any given topic, organization or person. The immense growth of social networking in recent years has added to a rich information bank that is readily accessible to anyone with an internet connection. The challenge today is to sift through vast quantities of information to uncover and piece together the information you require into an intelligence picture that supports your operations. The value of your own information can increase exponentially when combined with open source research and information from other entities with whom you are willing to share.

Security Policy

"Policy writing: next to cleaning the coffee break area, doing personnel assessments or wrestling a hungry grizzly bear, it is probably one of the least desirable tasks in any organization. Its mere mention can send employees scrambling over desks and seeking cover in the hopes of being spared the mind---numbing drudgery of documenting the company's rules, procedures and practices. There is a good reason for this: writing is hard work – and writing clearly, concisely and meaningfully is even harder still. When it comes to communicating an effective security policy, capturing that policy on paper (or, in today's digital environment, electronically) is only the first – albeit most critical – step. Disseminating the policy and ensuring compliance are close second and third priorities, followed by periodic reviews to ensure the aforementioned policy continues to meet your organization's requirements. "

Travel Security

"Media reports continue to include stories about company executives, oil field workers and regular travellers who have been the victims of kidnappings, armed robberies and murder while visiting foreign countries. Recent events have seen a Canadian woman kidnapped in northern Nigeria and her captors demanding $136,000 for her release. This woman was a financial advisor who was in Nigeria with other Canadians as part of an exchange program and she was kidnapped as she was entering a house after attending a social event. There are also ongoing reports of oil workers being kidnapped by rebels in South America and Africa; it would appear that these types of incidents are increasing rather becoming a thing of the past. "

Duty of Care

"The dynamic threat environment that persists in today's business climate demand constant vigilance and discipline. Under the Canadian Criminal Code, companies owe a duty of care to their employees. This means businesses must take "reasonable steps" to protect workers, whether they are in Canada or working internationally. If companies do not meet this duty of care, they can be found criminally and financially liable under the Criminal Code. In the most

extreme cases, the company can face hefty fines and the executives can be prosecuted and potentially jailed. In addition to the criminal prosecution, individuals can also face personal civil litigation. "