CYBER RISK MANAGEMENT

PREPARING FOR NEW OPERATIONAL RISKS

Captain Andrew E. Tucci, U.S. Coast Guard, Commander, Sector Long Island Sound, Captain of the Port Long Island Sound (COTP), Federal Maritime Security Coordinator (FMSC)

Shipping is an industry as old as history itself. The ancient city of Troy, located at the mouth of the Dardanelles, shows that regular maritime trade occurred at least 5,000 years ago. If seafarers have been managing operational and business risks since the Phoenicians traded their purple dye, the increasing use of cyber technology promises vast unchartered waters.

Cyber technology is the use of computer or digital systems to store, manipulate, or transmit data, or potentially to control or monitor physical processes or conditions. A key aspect of cyber technology is that cyber systems can be connected to other systems, providing an opportunity for unauthorized persons to intercept, access, or change data and the underlying software. Cyber security is concerned with maintaining the confidentiality, integrity, and availability of this data.

In addition to numerous attacks on business systems, the Coast Guard is aware of cyber incidents impacting operating systems in the maritime industry, including cargo systems, navigation (ECDIS) systems, and the deliberate exploitation of cyber enabled security cameras.

However it is defined, cyber technology is ubiquitous in society and is slowly but surely making its way into the traditional world of shipping. From digitized bills of lading and letters of credit to the navigation, propulsion, and cargo systems onboard ships, cyber technology is now a mandatory part of port and ship operations. Many companies are rapidly adopting the next generation of cyber technology in the form of big data, AI, predictive analytics, and improved real time cargo tracking via the "internet of things". Autonomous ships will soon move from the drawing board to the shipyard. Driverless electric trucks already move containers across terminals in many ports.

Vessel and facility operators recognize that while cyber technology brings many benefits, it also represents significant security challenges. The International Maritime Organization, via the Maritime Safety Committee, recently adopted interim guidelines on maritime cyber risk management [1]. In the United States the U.S. Coast Guard, under the authority of the Maritime Transportation Security Act (MTSA), establishes security standards and requires port facilities to develop security plans for port facilities. These plans enable the US to comply with the International Ship and Port Facility Security (ISPS) Code.

While these plans have traditionally focused on physical security risks, the need to address cyber vulnerabilities has been apparent for some time. Computer-enabled systems control gates, verify the legitimacy of people and cargo entering a terminal, monitor for unauthorized persons and hazardous substances, and play a key role in routine and emergency communications. The growth of the Internet of Things, and anticipated 5G networks will compound the integration of cyber and physical security.

The US Coast Guard has required that MTSA regulated vessels and facilities to report cyber breaches that impact physical security systems since 2013. For example, if a facility uses cyber technologies to control access to the facility, operate security cameras, control cargo movement,

or communicate emergency or security information, then an attack or unexplained failure on these systems must be reported. These reporting requirements are no different than if non-cyber versions of these systems were compromised.

MTSA regulated facilities may report cyber incidents directly to the National Response Center at 1-800-424-8802, or, alternatively, to the National Cybersecurity Communications Integration Center (NCCIC). Reporting alerts authorities to possible threats and is part of the information sharing that is crucial for any effective cyber security regime.

The Coast Guard has also been working with the industry, including the American Association of Port Authorities, to identify and promote cyber best practices. Among these is the Cyber Security Framework developed by the US Department of Commerce's National Institute of Standards and Technology (NIST). A detailed explanation of the Framework is beyond the scope of this paper, but it is built around the following core functions:

- Identify – Identify the software, hardware, users, and governance structure that make up an organization's cyber systems
- Protect – develop and implement appropriate safeguards to ensure the integrity of cyber systems
- Detect – Develop and implement activities to identify the occurrence of a cyber security event
- Respond – Develop and implement activities to take action once a cyber security event is detected
- Recover – Develop and implement activities to promote resilience and to restore any capabilities or services that were impaired due to a cybersecurity event

The United States Computer Emergency Readiness Team U.S.-CERT and other organizations provide information, standards, and best practices to promote cyber security. In 2015, the US Coast Guard held a public meeting in Washington, DC to seek input on more formally integrating cyber risks into MTSA security plans for facilities. The Coast Guard is developing guidelines to help facilities accomplish this.

MANAGING CYBER RISK

Securing computer technology is not and should not be seen as a stand-alone problem, but simply as another of the many risks the marine industry manages daily. As with other types of risk, cyber risks can be managed well or badly, but can't be eliminated. Understanding the unique aspects of cyber risk, and how cyber and physical risks can interact, is the key to a successful program.

Risk is commonly thought of as a product of threat, vulnerability, and consequences. Cyber technology changes each of these factors.

- For physical threats, the number of threat vectors to a ship or a port terminal is limited, since a certain degree of sophistication is needed to present a credible threat. Furthermore, those threat actors must be close to their target before launching an attack. In contrast, cyber threat actors are legion and can operate from anywhere in the world
- Physical vulnerability is limited to the fence line of a facility, or the gunnel of a ship. In the cyber domain, every new system constitutes an increase in the surface area vulnerable to attack or misuse. A newly installed wireless printer doesn't add to a facility's perimeter fencing, but it is vulnerable to cyber attack. If that isn't enough, it is surely connected to multiple systems, which have connections of their own. Cyber vulnerabilities increase exponentially with the number of connections
- Cyber technology poses an equally alarming increase in possible consequences. All those systems that the new device is connected to are not just access points – they do something important. When they fail, it matters

Another important aspect of cyber risk is that it is effectively invisible. A gap in a fence or an unguarded brow is obvious to even untrained observers, but a software flaw or missing security update can't be seen – except by hackers and by well trained, vigilant, cyber security experts. Even after a breach occurs it is hard to detect; it is often 6 months or more before an organization becomes aware that they have been hacked.

CYBER AND PHYSICAL RISKS

Cyber risks are not independent, isolated vectors – in many cases they can have a synergistic impact with physical security risks. For example, a cyber-enabled security camera, if hacked, could significantly increase the vulnerability of a marine terminal to a physical attack or criminal intrusion. Undetected physical intrusion could, in turn, allow for the installation of keyloggers or similar devices that would allow for increased cyber access. If a computer controlled alarm system failed, employees would not be alerted to a fire, physical attack, or other emergency. In these ways, cyber vulnerabilities can magnify the vulnerability or consequences of a non-cyber event.

Cyber technology associated with the Internet of Things (IoT) is one area where seemingly minor cyber risks can combine with physical systems to create substantial risk. The use of IoT devices is growing, including devices such as cameras, gate controls, traffic lights, scales, alarms, and environmental monitors routinely found in ports. IoT falls into a middle ground between business systems and industrial

control systems, and as such may be overlooked by an organization's cyber management structure.

It is important for organizations to recognize this relationship between cyber and non-cyber risks, and to ensure their cyber and physical security cultures reflect the same degree of integration as their cyber and physical security systems. If, as in many organizations, cyber security is managed at the corporate headquarters level while physical security is managed at the operational level, then the organization needs to take positive steps to integrate those structures, close oversight gaps, and bring all skills and perspectives into identifying and reducing security risks.

The Coast Guard encourages prudent mariners and waterfront facility operators to consider assembling a diverse team of safety and security professionals, including port operators as well as IT specialists, to fully understand the risks, and to find the best and most cost effective solutions. While there are many technical standards that may be appropriate, a holistic approach will likely find effective training, operational and administrative solutions and will promote an integrated approach to cyber risk management.

Port communities as a whole should also collaborate on cyber and other security risks. US Coast Guard Captains of the Port chair Area Maritime Security Committees in port areas across the country. These committees include the private sector as well as federal, state, and local agencies. Addressing cyber as well as physical threats, they share best practices, plan for security events, and conduct exercises. While cyber security is a significant challenge for the maritime industry, it can be managed through collaboration among the many professionals who work on ships and in ports every day.

REFERENCES

[1] MSC 96, Interim Guidelines on Maritime Cyber Risk Management, MSC1/Circ 1526, 1 June 2016

ABOUT THE AUTHOR

Captain Tucci is a 27 year Coast Guard veteran and currently serves as the Sector Commander and Captain of the Port in New Haven, Connecticut where he is responsible for all Coast Guard operations in Connecticut, Long Island, and the surrounding waters. In his previous tour at Coast Guard Headquarters in Washington DC he developed national policy related to port and facility safety and security, and was one of several key authors of the Coast Guard Cyber Strategy.

ABOUT THE ORGANISATION

The United States Coast Guard is a branch of the U.S. Armed Forces and is responsible for maritime safety, security, and environmental stewardship in U.S. ports and waterways. The Coast Guard is also a first responder and humanitarian service that provides aid to people in distress or impacted by natural and man-made disasters at sea or ashore. The Coast Guard is a member of the Intelligence Community, and is a law enforcement and regulatory agency with broad legal authorities associated with maritime transportation, hazardous materials shipping, bridge administration, oil spill response, pilotage, and vessel construction and operation.

ENQUIRIES

Andrew.E.Tucci@uscg.mil