U. S. Department of Homeland Security

United States Coast Guard

Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: CG-0921
Phone: (202) 372-3500
FAX: (202) 372-2311

TESTIMONY OF
REAR ADMIRAL PAUL F. THOMAS
ASSISTANT COMMANDANT FOR PREVENTION POLICY

ON
CYBERSECURITY IN U. S. PORTS

BEFORE THE
HOUSE COMMITTEE ON HOMELAND SECURITY
BORDER & MARITIME SECURITY SUBCOMMITTEE

8 OCTOBER 2015

Introduction

Good morning Madam Chairman and distinguished Members of the committee. I am honored to be here to discuss cybersecurity in U.S. ports. I will focus my comments in three areas. The first is to recognize the importance of cybersecurity and then explain cyber safety concerns, which emphasize the need to view this issue as a "cyber risk management" challenge. The second is to explain the need for an approach that emphasizes the essential role and responsibilities of maritime industry partners. The third is to outline what we have achieved and propose a way forward.

The Coast Guard has a long history of working with port partners to mitigate safety, security, and environmental risks to U.S. ports and maritime critical infrastructure. Since our founding in 1790, we have patrolled in the nation's ports and waterways to prevent and respond to major threats and hazards. Since Congress established the Steamboat Inspection Service in 1852, Coast Guard prevention authorities have evolved alongside emerging threats and changing port infrastructure. The Coast Guard established Captains of the Port to execute these authorities and work with our partners to prepare our ports for natural disasters, accidents, and deliberate acts.

Over time, the Coast Guard and the maritime industry have cooperated to address the risks associated with new threats and technologies. Security threats have evolved from coastal piracy to complex smuggling operations, transnational organized crime, and terrorism. Safety risks have likewise evolved as merchant shipping progressed from sailing ships to ships driven by coal fired steam boilers, to diesel engines and most recently to liquefied natural gas. Waterfront operations evolved from break bulk cargos to containerization, with sophisticated systems now controlling the movement and tracking of containerized and liquid cargos.

The Coast Guard's recently developed Cyber Strategy proposes three strategic priorities for the service – defending our own cyberspace, enabling Coast Guard operations, and protecting maritime critical infrastructure. Cybersecurity in U.S. ports is a key goal of this strategy.

Cyber Risks and the Marine Transportation System

Similar to other sectors, emerging cyber threats in the port environment are diverse and complex. Cyber risks manifest themselves as both safety and security concerns. As such, the Coast Guard is emphasizing the term "cyber risk management," which also addresses how much the maritime transportation system (MTS) relies on information technology systems to connect to the global supply chain. Vessel and facility operators use computers and cyber dependent systems for navigation, communications, engineering, cargo, ballast, safety, environmental control, and emergency systems such as security monitoring, fire detection and alarm systems. Collectively these systems enable the MTS to operate with an impressive record of efficiency and reliability.

While these information technology systems create benefits, they also introduce potential risks. Exploitation, misuse, or simple failure of information technology systems can cause injury or death, harm the marine environment, or disrupt vital trade activity.

Outside the U.S., cyber-related incidents among technology systems have been reported ranging from container terminal operations ashore to offshore platform stability and dynamic positioning for offshore supply vessels. While in some cases criminals may have been the source of these events, others have been the result of non-targeted malware or relatively unsophisticated insider threats. Even legitimate functions, such as remotely driven software updates, can disable vital systems if done at the wrong time or under the wrong conditions.

In one well-publicized event, organized crime exploited a European container terminal's cargo tracking system to facilitate drug smuggling. Cargo control is also one of the requirements of the Coast Guard's Maritime Transportation Security Act (MTSA) regulations, and we are well aware that such an incident, or one even more serious, might occur in the United States.

"Cyber risk management" also has safety implications. We are aware of incidents in which software problems led to the failure of dynamic positioning or navigation systems. These were not due to targeted attacks, but malware that migrated to vital systems through poor information technology practices.

As port facilities and vessels continue to incorporate information technology systems into their operations, the Coast Guard must adapt its regulatory regime accordingly. Regardless of whether an incident is a cyber-attack, or a cyber accident, we must recognize the potential consequences to mariners, port workers, the public, and the marine environment. With approximately 360 sea and river ports that handle more than $1.3 trillion in annual cargo, our nation is critically dependent on a safe, secure, and efficient MTS.

Unity of Effort - Partnerships, Learning, and Coordination

The Coast Guard is working closely with the Department of Homeland Security (DHS) and other government agencies to help the maritime industry identify their cyber risks.

This past March, the Coast Guard sponsored a seminar at the DHS Center of Excellence at Rutgers University on maritime cyber risks. We held a similar event at the Coast Guard Academy, and a follow-up at the California Maritime Academy to address specific cyber research questions. Each of these events included a broad range of cyber practitioners from industry, government, and academia.

In another effort, the Coast Guard Research and Development Center (supported by DHS S&T/Cyber Security Division) recently evaluated cyber vulnerabilities associated with wireless access to maritime critical infrastructure at certain U.S. ports. The preliminary results indicate significant vulnerabilities. While this study is relatively narrow in scope, the Coast Guard is continuing to evaluate the broad range of cyber risks in the maritime domain.

The Coast Guard has also partnered with various groups to evaluate and address cyber risks more systematically. Working with the American Association of Port Authorities and the National Institute of Standards and Technology (NIST), we are developing a cyber risk profile for bulk liquid terminals – such as those that transfer oil, gasoline, and liquid hazardous materials.

Another area with potentially significant consequences is the offshore oil and natural gas industry. This industry relies on information technology systems for a wide variety of functions – from the dynamic positioning systems that allow for precise navigation control, even in heavy wind and sea conditions, to real-time monitoring of drilling and production activity. Along with senior representatives from industry, the Department of Energy, and DHS, I recently attended a meeting of the Energy Sector Coordinating Committee in Houston. The exclusive purpose of this meeting was to discuss cyber risks. While the potential threats to this industry could be serious, I was very pleased with the cooperation and realistic approach that the participants expressed. As part of a related effort, the Coast Guard is working with the National Offshore Safety Advisory Committee to address cyber risks in the offshore industry.

Our work with other agencies, advisory bodies, and institutions has helped us identify the standards and best practices that can reduce risk. The Coast Guard is a strong advocate for using effective cybersecurity tools, guidelines, and sources of information. These include the Cybersecurity Framework developed by the NIST, the Cyber Capability Maturity Model developed by the Department of Energy, and the services provided by DHS' Computer Emergency Response Team (CERT), among others.

International Considerations

Cyber risks are an inherently global issue, and cooperation with international partners is an important part of our strategy. Covert electronic surveillance by foreign ships visiting our ports is a long standing security concern, and cyber technology certainly provides new avenues for such activity. Sound cyber practices by marine terminals can help minimize the likelihood that they might become victims of such activity, or of less nefarious activity that might still impact their business or operations.

Failure to follow sound cyber practices may create as much risk as not conducting proper equipment maintenance or adequate crew training for conventional shipboard emergencies. Accordingly, the Coast Guard is working within the International Maritime Organization to incorporate cyber risks into Safety Management System requirements, as well as the International Ship and Port Facility Security (ISPS) Code. While this is a deliberate and lengthy process, we have strong support from several nations, including Canada, South Korea, and Japan.

Coast Guard Activities to Address Cyber Risks in the Marine Transportation System

The Coast Guard is and has been working to address cyber risks in the Marine Transportation System. In 2012, we directed all of our Area Maritime Security Committees (AMSC) to consider cyber issues alongside more conventional risks as they evaluated potential security risks to their ports. Required by the MTSA, AMSCs are public-private partnerships that are chaired by the local Captain of the Port. All port stakeholders are represented at their local AMSC, including representatives from the federal, state, and local government, as well as private industry and labor.

Across the country, AMSCs have established cyber sub-committees, evaluated cybersecurity risks, held cyber-related exercises, and assisted in the evaluation of port security grant funding, including grants directed specifically at cybersecurity vulnerabilities. AMSCs also serve as a forum to share best practices across government and industry, such as the FBI's InfraGard program.

Because no amount of effort can guarantee that a cyber incident will not occur, the management of cyber risk demands a significant resilience and recovery aspect. AMSCs include a recovery annex to their Area Maritime Security Plans and these annexes are well suited to include cyber events as an element in port contingency planning. If or when there is a cyber incident in any given port area, our collective goal must be to continue safe and secure operations with minimal disruptions.

Current Challenges and Future Plans

The Coast Guard has made considerable progress in improving our own understanding of cyber risks, as well as improving cyber preparedness in ports and across the maritime industry. Despite these accomplishments, we know that significant work remains.

Our ultimate goal is to incorporate cyber risk management into the existing safety and security regimes that have served the industry, the Coast Guard, and the public so well, for so long. This past January, we held a public meeting to solicit suggestions on how to best accomplish this goal. We will continue to engage with industry and the public as we proceed.

The complexity of cyber technology, and the fast pace of change, suggest that any requirements will need to be risk and performance based. That is, rather than mandate a specific technical solution, the Coast Guard believes that facility and vessel operators should identify and evaluate the vulnerabilities and consequences associated with their cyber systems, and put in place an appropriate suite of mitigating measures sufficient to achieve an acceptable level of security. This approach has served the industry and public well in conventional safety and security risks. Our challenge is to devise a methodology suited to the nuances of cyber risk. Of course it must produce meaningful results in a way that the vessel or facility operators can demonstrate an acceptable level of security to the Coast Guard and other interested parties.

In addition to policy development, we recognize the need to develop our own workforce and take other measures to ensure we have the capacity and skills necessary to carry out those policies. The Coast Guard Cyber Strategy identifies several factors to this end, including training, education, organizational structure, and partnerships.

In addressing cyber risks to ports and other aspects of the maritime industry, our commitment is to address those risks with the same level of professionalism, efficiency, and effectiveness that the public has come to expect. The Coast Guard will continue to adapt, as it has done over the last two centuries, to the challenges and opportunities that accompany technological advancements in our operating environment.

Thank you for the opportunity to testify today, and thank you for your continued support of the United States Coast Guard. I am pleased to answer your questions.