Cyber Risks in the Marine Transportation System

The U.S. Coast Guard Approach

Vice Admiral Charles D. Michel, U.S. Coast Guard
Rear Admiral Paul F. Thomas, U.S. Coast Guard
Captain Andrew E. Tucci, U.S. Coast Guard

Historic Background and Coast Guard Mission

The U.S. Coast Guard has a long history of protecting our nation from all manner of threats and hazards. When Alexander Hamilton founded what was then called the Revenue Marine, he charged those early sailors with patrolling our coasts and protecting our ports with vigilance.

Piracy and smuggling were the main threats of the day, but soon enough other risks appeared. Boiler explosions, navigation hazards, and fires on merchant vessels all threatened the safety of the nation's marine transportation system. The Coast Guard, including our various predecessor agencies, developed the capabilities needed to protect the nation from those and other risks, including oil spills, the dominance of foreign flag ships for our overseas trade, and terrorism. Stemming from the sabotage at Black Tom's Island in New York in 1916, the Coast Guard established Captains of the Port[*] whose duties center on port wide risks and maritime critical infrastructure protection.

Today, cyber related risks are unquestionably a large and rapidly growing portion of all the risks our ports, facilities, and vessels face. The Coast Guard must address this threat if we are going to continue to achieve our mission of protecting the safety, security, and stewardship of America's waters.

Cyber Risks and the Marine Transportation System

The U.S. Coast Guard is proud of our service to the country. We are also grateful for the professionalism and cooperation of the marine industry in helping to build and operate the safest, most secure Marine Transportation System (MTS) in the world. The ports, terminals, vessels, related infrastructure and, most importantly the people that operate it drive the American economy and are vital to the nation's strength and prosperity.

Vessel and facility operators use computers and cyber dependent technologies for navigation, communications, engineering, cargo, ballast, safety, environmental control, and many other purposes. Emergency systems such as security monitoring, fire detection, and alarms increasingly rely on cyber technology. Collectively these technologies enable the MTS to operate with an impressive record of efficiency and reliability.

The Coast Guard's mission is to reduce the risk of deaths, injuries, property damage, environmental impacts, and disruptions to the MTS itself. Accordingly, our focus is on industrial control and other systems that could lead to these types of events. The integrity of IT systems that handle, for example, financial transactions is not, *per se*, a Coast Guard concern. Sound cyber risk programs will look at all types of risk, and operators need to be alert for the possibility that low risk or administrative IT systems may provide a network connection or backdoor to higher risk systems.

[*] See http://www.uscg.mil/hq/cg5/cg544/docs/Captain%20of%20the%20Port.pdf for details.

While these cyber systems create benefits, they also introduce risk. Exploitation, misuse, or simple failure of cyber systems can cause injury or death, harm the marine environment, or disrupt vital trade activity. For example, vessels rely almost exclusively on networked GPS-based systems for navigation, while facilities often use the same technologies for cargo tracking and control. Each provides multiple sources of failure, either through a disruption to the GPS signal, or malware that impacts the way the signal is interpreted, displayed, and used on the vessel or facility.

Cyber vulnerabilities are in no way limited to GPS. Engineering and other systems are equally vulnerable. The Coast Guard and other authorities have documented cyber related impacts on technologies ranging from container terminal operations ashore to offshore platform stability and dynamic positioning systems for offshore supply vessels. While in some cases modern day pirates and smugglers 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, could disable vital systems if done at the wrong time or under the wrong conditions.

The engine control room on a modern cruise ship. Photo credit: LCDR Eric Allen, USCG

Commercial pressure and the ever increasing demand for speed, efficiency, centralized control, and convenience creates incentives to make greater and more integrated use of these systems. This in turn increases vulnerability and the “attack surface” available to hackers and criminals, as well as to simple misuse.

Vessel and facility operators must be able to recognize cyber risks alongside more conventional threats and vulnerabilities. Once recognized, operators should address them via established safety and security regimens, such as security plans, safety management systems, and company policies.

The U.S. Coast Guard Strategic Approach

The Coast Guard's operating model for all types of risk is to prevent incidents, accidents, and attacks whenever possible, and to be prepared to respond to those events when they do occur. Both have a role in the Coast Guard's Cyber Strategy. Appendix 1, the cyber risk "bowtie model," illustrates some of the prevention and response related aspects of this approach.

The Prevention side of this equation is to identify and establish broadly accepted industry standards that reduce the likelihood of an incident occurring. In developing Prevention standards and programs for cyber and other vulnerabilities, the following principles apply:

Principles of the Coast Guard's Prevention Program

The Coast Guard's prevention standards are ***risk based***. That is, they correlate the degree of protection with the potential consequences. For example, vessels and facilities that handle liquefied natural gas are subject to greater requirements than those that handle most other products. For any individual vessel or facility, vital systems such as firefighting, lifesaving, and communications are generally given more scrutiny than those with only a secondary influence on safety or security.

Coast Guard personnel observing the security and safety control systems at a marine terminal. USCG photo

The Coast Guard's

Prevention Program:

Risk Based,

Performance Oriented,

Customized to the unique

marine environment

In addressing potential cyber vulnerabilities, the Coast Guard will follow a similar risk based approach. While a vessel or facility may have any number of cyber dependent systems, our concern is with those few where failure or exploitation of the system might result in significant safety, security, or environmental consequences.

A second principle is that the Coast Guard uses ***performance standards*** wherever possible. That is, the purpose of our standards is to achieve a high degree of safety and security performance – to protect the mariners, facility workers and vessel passengers from harm, to protect the marine environment, and to avoid damage to property and equipment. There are many ways to accomplish that goal, and the Coast Guard strives to allow industry the greatest flexibility. In some cases, such as with our Maritime Transportation Security Act requirements, our regulations are almost entirely performance based. Even in cases where more prescriptive requirements are appropriate, such as engineering standards, the Coast Guard allows and encourages industry to propose alternative methods that achieve an equivalent level of safety or security.

Despite the technical nature of cyber systems, the Coast Guard believes that the principle of performance standards can and should be part of any vessel or facility’s approach to reducing cyber risks. In some cases, an operator may choose to mitigate a cyber vulnerability through an established technical protocol. In other cases, training programs, physical access controls, or a simple manual backup may be a better option. The business needs of the organization should serve to identify the best method of reducing the risk.

Cyber risks are an international threat. The Coast Guard is working with the International Maritime Organization to improve cyber risk management for vessels and ports subject to SOLAS and the ISPS Code.

A third aspect of the Coast Guard’s Prevention model is that our standards reflect the ***unique risks of the marine environment***. Heat, vibration, salt water, weather, and other factors require standards suitable for this environment. Coast Guard approval of items such as fire extinguishers and marine wiring reflect this reality.

The marine environment includes unique risks that any cyber risk management effort must address. These include serious consequences to people, the environment, property, and the marine transportation system as a whole. The Coast Guard’s cyber risk management program is concerned with these special maritime risks. Businesses certainly face other cyber risks, such as the loss of proprietary or financial data. These risks, while very real, are not unique to the maritime environment and are outside the Coast Guard’s mission. The technical aspects of cyber security are also not uniquely maritime. Computers onboard a vessel or on a marine facility are no different from those in other environments, and the threats they face come in one and zeros wherever the computer is located and without regard to its ultimate function. Technical protocols need to be appropriate for the system and threat in question. They need no modification for vessel or marine facility use.

Response, Investigation and Recovery

Because we can’t expect to prevent all incidents (cyber related or otherwise), preparedness is equally important to reducing the overall risk to the public and MTS. In many cases, addressing the consequences of a cyber event – such as an oil spill caused by computer controlled pump – is no different than if the incident had no cyber aspect. In such an incident, the responsible party would activate their spill response plan under the direction of the Coast Guard and other agency officials.

Appendix 2 describes cyber notification requirements. Notification triggers any needed immediate response actions and alerts the COTP to a possible port-wide threat. The Coast Guard will also support the Federal Bureau of Investigation and others in the investigation of cyber related crimes.

The Coast Guard investigates pollution incidents, marine casualties and certain other incidents to determine the factors that led to the incident and prevent reoccurrences. If the investigation reveals a cyber nexus, the Coast Guard will work with law enforcement and other appropriate agencies to gather evidence and support criminal prosecution. In all cases, the Coast Guard will typically require the operator to conduct tests or inspections to ensure a system is safe before resuming normal operations. For cyber incidents, that process might include measures to ensure a system is free of malware or known vulnerabilities.

How Can Vessel and Facility Operators Manage Cyber Risks?

The NIST Framework identifies the following core functions:

Identify
Protect
Detect
Respond
Recover

The marine industry has a long history of success in risk management. Mariners and port workers identify and evaluate risks on every watch and shift. Vessel and facility operators should view cyber along with the physical, human factor, and other risks they already face. The NIST Framework provides guidance on how to accomplish this. The first step is to identify and evaluate the sources of risk.

While physical and personnel risks are relatively easy to identify, cyber risks pose a unique challenge. Cyber vulnerabilities are invisible to the casual observer and cyber attacks can originate from anywhere in the world. Information technology specialists can help, but their focus is often with routine business applications. IT specialists may not fully recognize the various operational systems on a vessel or waterfront, the potential consequences should they fail, or have an operator's perspective on potential non-technical (and lower cost) solutions.

Risk Assessment:

To assess cyber risk, designate a responsible individual and assemble a team that includes operators, emergency managers, safety, security, and information technology specialists.[†] Very briefly, their risk assessment process would proceed as follows:

- Inventory cyber dependent systems that perform or support vital operational, safety, security, or environmental protection functions.
- Map any connections between these systems and other networks. Note which systems are accessible via routine internet connection and for portable media such as USB and CD drives. This step in the process helps to identify potential **vulnerabilities**. Note that even systems with no connection to the internet whatsoever are still subject to insider threats and simple technical failures.
- For each system, discuss the potential **consequences** if the system was exploited, malfunctioned, was unavailable, or simply failed under "worst case scenario" situations. Remember, Murphy's Law always applies, and adversaries may combine a cyber attack with a physical attack.

[†] This is the most important step – the team must include individuals with all of these skills.

- Considering both the vulnerability and the potential consequences, evaluate the relative risk for each system. Systems with multiple vulnerabilities and high potential consequences have higher risk than those with few vulnerabilities and low potential consequences.

Risk Mitigation:

Once the team recognizes their cyber risks, the organization can select mitigation strategies to reduce that risk. Prevention/protection strategies reduce vulnerabilities and the frequency of successful attacks or adverse events. While high-risk systems should naturally have more robust protection strategies, this does not necessarily equate to sophisticated technical solutions. For example, physical access control and training may be sufficient for systems where the primary vulnerability is an insider threat. Where risk managers choose technical solutions, they must also recognize their limitations.

The term *Defense in Depth* refers to a multi-faceted and multi-layered approach to cyber defense. Defense in depth considers the various people, technology, and operating policies an organization might adopt. It includes protection, detection, response, and recovery activities. Defense in depth recognizes that no single strategy can ensure security.

There are many private and public resources available to help companies address cyber risks, including ICS-CERT. Identifying these resources in advance and designating specific personnel with the responsibility to contact them will improve preparedness.

Many systems are only capable of recognizing and blocking known threats. Unfortunately, the pace of innovation in the malware world is increasing, zero day exploits are common, and a strategy that relies exclusively on a perimeter defense designed to filter out known threats will not be successful.

Operators can also reduce risk at the consequence end. For example, manual backups may be appropriate for situations where the cyber failure is disruptive, but does not include immediate life, safety, or environmental impacts. Manual backups can be an excellent way of building cyber resilience – provided the manual system is reliable and personnel still know how to use it!

Exercises can help identify the procedures an organization may need to take to isolate a suspect system, purge it of malware, and safely resume operations. Including a cyber aspect into an existing security, natural disaster, or environmental response plan can help an organization prepare for a cyber incident with an "all hazards" approach.

The teamwork approach among operators, IT specialists, and other risk managers is vital. Only a multi-talented team can develop multi-talented solutions. Regardless of the strategy chosen, operators need to see risk assessment and risk mitigation as continuous processes, not one-time- events. While this is true for any risk an organization may face, the rapid change in technology and its ever increasing use in society make this especially important.

Risk Management:

Once an organization has identified, evaluated, and mitigated cyber related risks to an acceptable level, it must still do two things to maintain that condition. First, organizations need to incorporate their cyber procedures into appropriate internal policy and operating requirements. These will vary from organization to organization, but may include the following:

- Safety Management System/ISO procedures
- MTSA required security plans
- Operations manuals
- Continuity of Operations/Continuity of Business plans
- Company training programs and policies

Second, because no risk is static, organizations must view cyber security as a process, and establish a regular schedule to review cyber risks, re-evaluate the need for mitigation measures, and ensure personnel understand and can follow good cyber practices. Rapid changes in technology and ubiquitous cyber threats make this concept especially important. Ultimately, an organization should strive to incorporate cyber into an existing culture of safety, security, and risk management.

Ultimately, cyber risk management is a leadership responsibility. Organizations should identify a senior individual as the person responsible for cyber risk management. That individual, and other leaders, must recognize that creating a strong cyber culture as an "all hands" responsibility. With the visible backing of senior leadership, an organization can develop the strong cyber culture needed to keep the operations safe, secure, and efficient.

Conclusion:

Despite the apparent complexity and scale of cyber threats, we can and are adding cyber to a long list of risks the maritime industry and the Coast Guard have overcome. More senior members of the Coast Guard, and of industry can look back on their careers and see great advances in environmental stewardship, safety, and conventional security. Those accomplishments reflect a cooperative approach that establishes meaningful standards to address real risks, devises flexible strategies to meet those standards, and shares responsibilities to maintain those systems over time. We have strengthened our nation and ensured that our ports and waterways are a safe place to live, conduct business, and link our economy to the world.

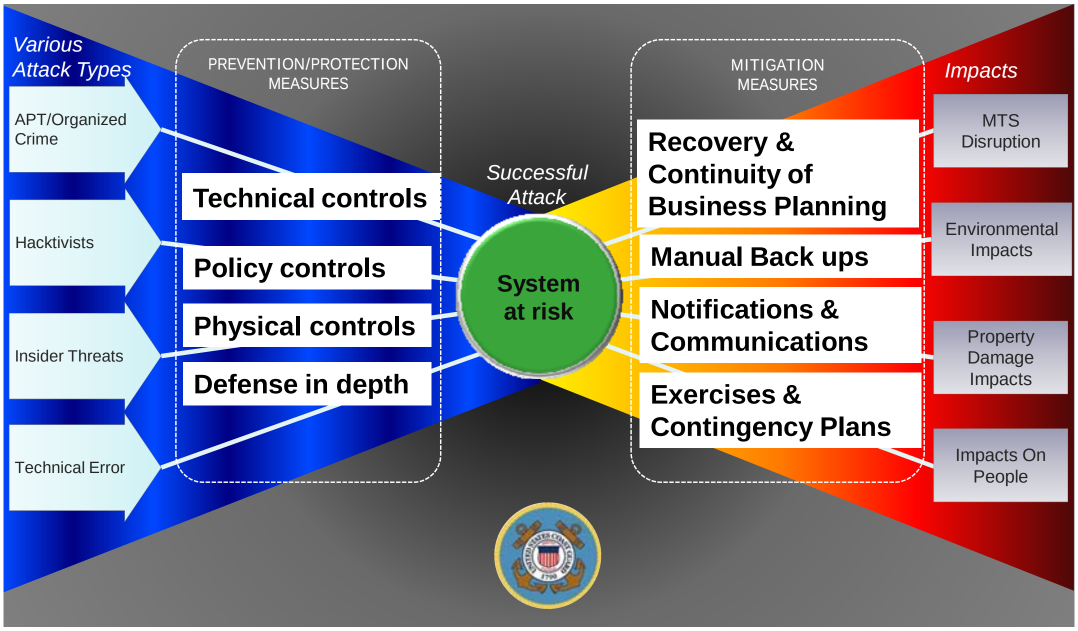
While cyber risk management certainly requires some technical skills from the current and next generation of leaders, it will succeed on the foundation of those of us (these authors included) that still think an A-60 bulkhead is the best firewall for any situation.

Appendix 1 – Cyber Risk Bowtie Model

The model below depicts cyber risk management activities. On the left, the model notes several types of attack or threat vectors. These range from sophisticated, targeted attacks from “Advanced Persistent Threats” (including, but not limited to nation-states), down to a simple technical error, such as improper software update. The term “insider threats” also represents a broad range of actors – from those with special access and a desire to inflict deliberate harm on an organization to those who unknowingly introduce malware by clicking on the wrong link or plugging a personal smart phone or other device into a USB drive or other port.

Cyber Risk Bowtie Model

All activities must take place against a backdrop of the training, education, and policies needed to promote a culture of cyber security.



Prevention/Protection measures reduce the likelihood of an incident by creating barriers to the malware or other measures that can compromise a system. These include technical measures, policy and training, and physical access controls. Once an incident has occurred, communications, response, and contingency plans reduce the impact of the event and promote rapid recovery. An organization with strong cyber resilience will consider all types of threats, institute both protection and response procedures to reduce risk, and promote a strong culture of cyber security through training, education, and leadership.

Appendix 2, Cyber Incident Notifications and Investigations

Coast Guard regulations[‡] require MTSA regulated vessel and facility operators to report suspicious activity, breaches of security, and Transportation Security Incidents to the U.S. Coast Guard. This includes incidents and activities with a cyber nexus. In cases of a TSI or other emergent incident, notification enables the Coast Guard and other security partners to take immediate action to protect the port and respond to the threat. Suspicious activity reports provide the Captain of the Port with information that, in combination with other sources, may indicate a port-wide threat.

In practice, cyber incident reporting has some unique challenges. In many cases computer security monitoring, such as intrusion detection, is done remotely rather than at the vessel or facility operator level. Detecting a cyber incident, recognizing the potential for it to impact systems related to Coast Guard requirements, and relaying that information to the Coast Guard as well as the vessel or facility operator in a timely manner is not as straightforward as it might be for a physical security incident.

The definition of "suspicious activity" in a cyber context is also problematic. Larger organizations may experience near-constant attacks on their firewalls or routinely find malware on various networked systems. Reporting every such incident is neither practical nor desired.

The Coast Guard and industry have a shared goal of keeping our nation safe, secure and protecting our marine transportation system. Organizations must report cyber incidents that threaten that goal, affect vital systems, or impair functions described in Coast Guard security plans. Our purpose is to promote mutual security, never to punish those who make a judgment call in good faith.

The Coast Guard also recognizes that cyber incident reporting requires diligent attention to confidentiality. As of this writing, several federal government organizations accept or require cyber incident reports. Agencies are working to streamline these systems in a way that minimizes the impact on industry, maximizes security, and ensures that agencies have access to the information they need to carry out their responsibilities. While the nuances of that effort are beyond the scope of this paper, suffice to say that this is a complex task, and that the Coast Guard and other agencies ask for patience, cooperation, and suggestions on accomplishing this goal.

The National Response Center (NRC) is the designated reporting point for Coast Guard regulated vessels and facilities. The NRC is staffed by trained professionals who treat all security reports as Protected Critical Infrastructure Information. Distribution of these reports is limited to law enforcement agencies on a need to know basis. In cases where extreme discretion is appropriate, vessel and facility operators have the option of reporting an incident directly to the local Captain of the Port, with a follow up call to the NRC providing only generic information for documentation purposes. Regardless of how a report is made, the Coast Guard will share the information with the FBI, and with other agencies with cyber security responsibilities. With the help of those agencies, we will facilitate efforts to help the impacted vessel or facility operator recover from the incident, resume operations, and support prosecution efforts.

[‡] 33 CFR 101.305

Appendix 3 – Cybersecurity Roles and Responsibilities

A full discussion of the various cyber security related authorities and responsibilities within the federal government is beyond the scope of this paper. Broadly speaking, the Department of Homeland Security is primarily responsible for critical infrastructure protection, the Department of Justice is primarily responsible for criminal investigations, while the Department of Defense is responsible for national defense.

	DHS	DOJ	DOD
Lead role	**Protection, Information Sharing**	**Investigation and Prosecution**	**National Defense**
Responsibilities	Coordinate national response to significant cyber incidents Disseminate domestic cyber threat and vulnerability analysis Protect critical infrastructure Secure federal civilian systems Investigate cyber crimes under DHS jurisdiction Coordinate cyber threat investigations	Prosecute cyber crimes Investigate cyber crimes Lead domestic national security operations Conduct domestic collection and analysis of cyber threat intelligence Coordinate cyber threat investigations	Defend the nation from attack Gather foreign cyber threat intelligence Secure national security and military systems Support the national protection, prevention, mitigation of, and recovery from cyber incidents Investigate cyber crimes under military jurisdiction

These descriptions are best understood as generalizations. Individual agencies often have their own, unique authorities. For example, within DHS, the U.S. Secret Service has authority to investigate and prosecute certain types of computer fraud and other cyber crimes.

The U.S. Coast Guard, as a member of the Department of Homeland Security, has responsibility to help protect the nation’s maritime critical infrastructure, and to promote safety and security in the Marine Transportation System. As a member of the U.S. Armed Forces, the Coast Guard works closely with the Department of Defense, including U.S. Cyber Command, in defending the nation. As a law enforcement agency, the Coast Guard has authority to investigate violations of all federal crimes with a maritime nexus (14 U.S.C.). Finally, the Coast Guard is a member of the intelligence community, providing us access to many sources of information that can help us with our mission to protect the American people.