Dial C for Cyber Attack

In 1964, the science fiction author Arthur C. Clarke wrote the short story "Dial F for Frankenstein". In the story, reports of chaos in banking, transportation, military, and industrial systems follow an unexplained event where every phone on earth rang at the same time. Clarke's protagonist discovers the truth: as satellites linked the world's communications systems, those connections reached a critical threshold similar to that of the billions of synapses in the human brain. The previously independent systems had achieved what we would today call artificial intelligence.

While the World Wide Web has not, to our knowledge, developed into a malevolent artificial intelligence, Clarke was spot on in his understanding of the implications of a globally linked system of communications and computers. While we celebrate every clever new app or web-based innovation, we are only now beginning to understand that the darker side of these systems goes beyond e-mail spam, momentary losses of connectivity, or the loss of private information to hackers. Cyber attacks have and will continue to damage private sector and government systems. In the past few weeks alone, there have been widely reported attacks on U.S. power plants, and on the New York Times, Wall Street Journal, and the Washington Post.

Historically, our nation has approached critical infrastructure protection through a focus on physical and human security systems. We must now include cyber security into that process. Cyber security has some unique challenges, including its technical nature and the fact that attacks can originate from thousands of miles away.

Perhaps most importantly, threat vectors and vulnerabilities change with every new device, software update, and innovative hacker. We must therefore recognize that cyber security is a *process*, and incorporate it into an overall culture of security alongside our physical and human factor security processes.

American ports, terminals, ships, refineries, and support systems are vital components of our nation's critical infrastructure, national security, and economy. Cyber attacks on industrial control systems could kill or injure workers, damage equipment, expose the public and the environment to harmful pollutants, and lead to extensive economic damage. The loss of ship and cargo scheduling systems could substantially slow cargo operations in ports, leading to backups across the transportation system. A less overt cyber attack could facilitate the smuggling of people, weapons of mass destruction, or other contraband into the country.

In short, there are as many potential avenues for cyber damage in the maritime sector as there are cyber systems. While only some cyber attack scenarios in the maritime sector could credibly lead to a Transportation Security Incident[1], we must identify and prioritize those risks, take this threat seriously, and work together to improve our defenses.

Fortunately, the process for doing so is parallel in structure to that of other security and safety efforts: assess risk, adopt measures to reduce that risk, assess progress, revise, and continue. These processes, taken together, can significantly improve an organization's risk reduction efforts and increase resilience through continuity of business planning.

---

[1] As defined in 33 Code of Federal Regulations Part 101.105

Looking specifically at cyber security, consider the following steps:

- Conduct a Risk Assessment – begin by assessing what parts of your enterprise are controlled or supported by computer systems. What are the consequences should those systems become inoperable, controlled by outside parties, or misused by internal parties?
- Identify and Adopt Best Practices – what information technology security standards are most applicable to your systems? Are your systems meeting those standards, are your employees familiar with them? When were they last updated? What backup systems, redundancies, or replacements are available?
- Secure Your Supply Chain – As with just-in-time inventory and production systems, consider the cyber vulnerabilities and practices of your suppliers, customers, and other organizations critical to your company's profitability. Discuss cyber security with those organizations and consider incorporating good cyber practices into marketing and contracting.
- Measure Your Progress – Test your cyber practices through drills and exercises. Identify any gaps or lessons learned, and set specific goals with timelines for making needed improvements.
- Revise and improve security – Review your latest risk assessment, evaluate any new cyber systems you may have added since that time, incorporate lessons learned and revise your cyber security policies and procedures accordingly.

One way to start this process is to take advantage of the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). ICS-CERT provides a wide range of information, tools, and services that can help companies assess their security, identify recommended practices, and improve their cyber security. http://ics-cert.us-cert.gov/

The men and women of the United States Coast Guard take our responsibility to protect the nation from threats seriously. As in other areas, we will work with the private sector, and with other federal, tribal, state, and local agencies to address this new threat. The President's recently signed cyber security Executive Order sets requirements for executive branch agencies to address cyber risks. We have started that work already, and will keep the private sector informed of our progress. We will also be asking for advice and cooperation.

In Clarke's story, humanity faced a threat from its own creation. Today, it is not a singular super intelligence that threatens us, but simply other human beings, seeking to exploit existing systems to their own evil ends. If we address this threat with the resolve, innovation, and determination we have employed for other threats in the past we will continue to preserve our economy, our lives, and our freedom.

- Captain Andrew Tucci, U.S. Coast Guard[i]

---

[i] For more information on port security and other Coast Guard activities, see http://www.uscg.mil/hq/cg5/cg544/ or go to Homeport at https://homeport.uscg.mil