PORT SECURITY: AN EXERCISE IN PARTNERSHIPS

COORDINATION IS CRITICAL TO COMBAT THE DYNAMIC PERILS OF CYBER AND PHYSICAL SECURITY

By Barry Parker

Security continues to be an important concern throughout the maritime world, with the challenges steadily broadening throughout all touchpoints for industrial supply chains or passenger movements through ports. The security scope is broadening as well, as it is not just physical security that is top of mind; it is cyber security as well.

It is not a small task to keep ports safe, and it is not a task that is limited to just security personnel. Coordination among port police and technology personnel is critical for physical and cyber security, and partnerships between ports, terminal operators and others are necessary for success.

Exponential Electronic Growth

With electronic digital controls replacing analog mechanical controls on all manner of industrial equipment, the exponential growth in the number of interfaces has been a hot-button item for security industry professionals. As people, devices and systems become more interconnected, port professionals must look not only at traditional security to keep individual facilities safe and secure, but they must consider impacts of cyber security that come with all this connectivity. Physical security is paramount, but throughout the maritime and supply chain worlds, the cyber component – which is also dynamic (meaning that threats can change on a daily basis) – is now receiving equal amounts of attention.

April Danos, director of information technology for the Greater Lafourche Port Commission and chair of the AAPA Cybersecurity Subcommittee, part of the AAPA's Information Technology Committee (see sidebar), explained, "Operational technology, or OT, is all about industrial controls, things like automated cranes, or a card reader that controls a gate. Information technology, or IT, is needed to secure those systems. In the example of the card reader, a cyber breach – where someone tampers with the data – could enable unauthorized people to enter a secure area." Other examples of what might happen, cited by Danos, include a situation where firmware controlling a port's security camera is not updated, creating a vulnerability where a hacker, or worse, someone planning a physical attack, could gain control of the camera. She said, "Our job is to think it through….to envision the worst case scenarios and come up with the worst nightmare. Then we can begin to plan properly."

Port Fourchon, like many AAPA members, is a "landlord port," which influences the way that security is organized. Danos explains, "As a landlord port, it is our tenants who do the physical doing when it comes to running and operating their facilities and systems. When it comes to security matters, they take their guidance from the U.S. Coast Guard, which requires Facility Security Plans."

The port, however, maintains a backbone of collaborative command and control software and hardware assets that make coordinated incident response and security possible. Additionally, the port maintains a dialogue with its tenants, agency response partners, and the local Coast Guard in order to provide a layered, more resilient approach to security as a whole. Resiliency is very much on the mind of Danos and her colleagues: "If something like a GPS hack happened and it led to a vessel collision, it would be a port problem. How do we respond? We are constantly thinking about how to get back up and running, as quickly as possible," she said.

> "Our job is to think it through….to envision the worst case scenarios and come up with the worst nightmare. Then we can begin to plan properly."
>
> *—April Danos, Director of Information Technology, Greater Lafourche Port Commission*

At the level of individual terminals, the Coast Guard has also been ratcheting up security requirements – notably with the Transportation Worker Individual Credential (TWIC). Jim Strey, president/CEO of idSoftware, explained that new rules initiated, which will enter into full force in August 2018 (following a two-year phase-in period), require "All Class-A facilities to comply with rules requiring all TWIC cards to be read electronically – with biometrics validated each time a card holder enters the facility." Strey explained, "At these facilities, anybody – even delivery truck drivers – needs to have a valid TWIC card with the biometric indicator." idSoftware, which has offices in Jacksonville, Fla., and Greenville, S.C., creates and sells products such as SecureGate Ports and VisCheck Ports that "let terminals comply with these new rules." However, in the interests of keeping this electronic data intact and safe from cyber security threats, "no data is actually stored in our system," said Strey, and any transmission of data (for example, from a hand-held device) is encrypted. "Our primary focus is about who is on the facility at any point in time."

For terminals where certain dangerous cargo (CDC) is handled, the new regulations are being felt, as well. However, less than a year past the startup date of the tighter regulations, a pilot project is already underway with a group of facilities around the United States, including Port Everglades, Fla.; Panama City, Fla.; Mobile, Ala.; and Freeport, Texas. On the West Coast, projects are underway in San Diego and at Everett, Wash.

The importance of the cyber realm is also evident in the positioning taken by KBRwyle. Serving mainly governmental entities, KBRwyle is a subsidiary of KBR, a Texas-based provider of differentiated services and technologies that acquired Honeywell Technology Solutions Inc. (HTSI) in late 2016. KBRwyle has two tools, Portable Cyber Assessment Tool (PCAT) and CSTAR (a reporting tool), that are used to document a company's risk posture

AAPA Resources

Two AAPA technical committees and one subcommittee tackle issues related to topics discussed in this article. The Security Committee, chaired by Joseph Lawless, of the Massachusetts Port Authority, is tasked with: "…collecting and disseminating information pertaining to protection of cargo and facilities from theft, pilferage and vandalism, including prudent business and operating practices, appropriate facility design security and personnel training and procedures and port security technologies and techniques." The Information Technology Committee, chaired by Lance Kaneshiro, from the Port of Los Angeles, has the mission of "monitoring, collecting and disseminating knowledge regarding the development of information technology, including but not limited to the areas of electronic data interchange, management information systems and other automation initiatives in the area of information technology undertaken by federal agencies and ports in AAPA member counties, as well as monitoring such initiatives throughout the world…" The Cybersecurity Subcommittee, chaired by April Danos, from the Port of Fourchon, is part of the IT Committee and has the mission of monitoring, collecting and disseminating knowledge regarding cybersecurity. The Department of Homeland Security (which includes U.S. Customs and Border Protection and the U.S. Coast Guard) plays a key role in security matters. A March 2017 AAPA brief on Government Relations Priorities: Maritime Security outlines recommendations for federal lawmakers. It can be found at: http://bit.ly/AAPAbrief

against the National Institute of Standards and Technology (NIST), Risk Management Framework (RMF). Stephanie Gonzales, a director of security solutions sales & capture at KBRwyle, said that true security is not found in a piece of hardware or software alone. "We provide a holistic security solution that addresses cyber and physical security threats. We provide vulnerability assessments and penetration testing for SCADA (a control system architecture) and IT systems."

Beyond the actual regulations requiring facilities (and also vessels) to maintain security plans, the Coast Guard continues to provide recommendations on matters related to security. In November 2016, the agency issued a voluntary "Cybersecurity Profile" for facilities engaged in maritime transfers of bulk liquids, including oil and natural gas. As explained by the Coast Guard on its Maritime Commons blog, "The Profile pulls into one document the recommended cybersecurity safeguards and provides a starting point to review and adapt risk management processes. It outlines a desired minimum state of cybersecurity and provides the opportunity to plan for future business decisions." In December 2016, the agency issued a Policy Letter advising both U.S. terminal and vessel operators (who have filed Facility or Vessel Security Plans, FSPs and VSPs, respectively) to report suspicious cyber activity and actual breaches of cyber security directed specifically at maritime systems to the National Response Center – a hotline used since the early 1990s for notifying the government about oil and chemical spills. The letter can be accessed at: http://bit.ly/USCGhomeport

> "At these facilities, anybody – even delivery truck drivers – needs to have a valid TWIC card with the biometric indicator."
>
> *—Jim Strey, President/CEO, idSoftware*

Going forward, the Coast Guard is on a path toward issuing guidance, in the form a Navigation and Vessel Inspection Circular (NAVIC), on cyber security. The NAVIC, which will not create new laws, will provide terminals and other sites that file FSPs with guidelines on the best ways to include cyber risk management when these plans are revised. One challenge here is that the cyber aspect may not have been considered at the time of their installation for systems put in place to comply with earlier guidelines and actual rules. So, in essence, the new NAVIC will create a path for FSP holders to catch up. Danos said that the plans for the NAVIC are in progress, though she was uncertain of exactly when they'd be released.

On an organizational basis, a useful viewpoint comes from a high-level cyber security session, which took place at the recent Seatrade Cruise Global conference, held at Port Everglades, Fla., in mid-March 2017. One panel member, a DHS veteran, talked about making thinking about cyber matters in the age of inter-connectedness as a "horizontal" (organization-wide, and then externally to vendors and partners) activity, rather than as a "vertical" activity (architected around separate silos for "operations," "finance" and "IT"). Though this presentation was aimed at operators of vessels, the same advice, adjusted for each organizational schematic, would certainly apply to ports.