Quick Steps to Strengthen Cybersecurity at Ports

The increasing digital interconnectedness of systems enabling Marine Transportation System operations, to include ship navigation, cargo movement, engineering, safety, and security monitoring have introduced cyber vectors of attack and vulnerabilities that, if exploited by a bad actor, could devastate U.S. trade and commerce. This is a much bigger issue - one of the downsides of a connected society where millions of new vectors of cyber attack are added each time we decide to control an action from our phones or remotely. Any smart system (also known as cyber/physical systems), using microchips to converge data with operational technologies (OT) and machinery will have similar vulnerabilities. As for cranes, other port equipment, and even the building systems on site, the cyber risk remains regardless of the manufacturer or software.

Authored by:

NAWE
THE NATIONAL ASSOCIATION OF WATERFRONT EMPLOYERS

BUILDING Cyber Security

NAWE
THE NATIONAL ASSOCIATION OF WATERFRONT EMPLOYERS

BUILDING Cyber Security

- [ ] **Bring the Port Team Together Today**
Terminal operators must bring their IT, facility, and OT teams together immediately to confirm connectivity and assess their current risk. Shared visibility of the operating environment is crucial to unite teams and work together. The most effective means of low-cost, immediate remediations is to check passwords, secure remote/wireless access points, install multi-factor authentication, and update software protections. Next, perform tabletop exercises to practice cyberattack response protocols. Then, update mandated Facility Security Plans to ensure that all network connected technologies, including cranes and other cargo handling equipment, meet or exceed guidance released in the Maritime Security Directive, 2024-002-Worldwide-Foreign Adversarial Technological, Physical, and Cyber Influence.

- [ ] **Captains of the Port (COTP)**
When designated by the MDZ Maritime Defense Commander (MARDEFCOM), the COTP, serving as the Harbor Defense Commander (HDC), can request the Coast Guard's cyber protection teams to assist with threat intelligence and the discovery of vulnerable or unguarded attack vectors with specialized network analysis kits. These kits can map assets and the Human Machine Interfaces (HMI's) that control them to provide port authorities a comprehensive view of software status and the next steps for mitigation. Ports should also ask for scanning technologies to identify and confirm all data transmitting sources, including modems and other wireless access devices. When appropriate, the HDC also can access sensitive security information from US Transportation Command (TRANSCOM) to address and close certain vulnerabilities. When ready, the Port team should bring in this range of federal expertise.

- [ ] **Consider how a specialized vendor can mitigate the OT risk**
Once vulnerabilities are identified, a risk assessment to port safety, operations, and security must result in a plan for a suite of private sector capabilities. This will provide continuous visibility of the industrial environment, implement network segmentation and controls to mitigate cyber risk across the entire fleet of connected equipment. The capabilities should address access management and other Zero Trust architectures, monitoring sensors, and other protections, to respond, recover and develop digital twins to provide a virtual representation of equipment performance.

- [ ] **Apply for federal grant funding**
The federal government has a range of grants available that will help improve cyber safety, security, and reliability. This includes the Department of Transportation's Port Infrastructure Development Program (PIDP), which should be consistent with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) recommendations to improve port security when awarded. The Department of Homeland Security also offers funding through its Port Security Grants Program which aims to improve port-wide security management.

- [ ] **Install a cyber check point between the manufacturer and the crane**
Port operators can use grant funds to establish or expand smart port network operations centers to monitor performance and manage the data, programming, and software in the cranes and other equipment. A qualified cyber specialist is essential to clear all actions and cut the external data connections with no impact to the crane or port operations.

NAWE
THE NATIONAL ASSOCIATION OF WATERFRONT EMPLOYERS

BUILDING Cyber Security

- [ ] **Treat Cyber threats to OT as a Port Safety Priority**
When data or software is compromised through a ransomware attack, it's a bad day for the Port's IT team. If a cyber attack to the cranes or other cargo handling equipment hurts someone or causes property damage, it's a really bad day for the CEO and the insurance companies. Not only can cranes be stopped – exploitation of the automated controls can result in an accident impacting lives and property.

- [ ] **Check Insurance Coverage for Crane Operations**
Lloyd's of London implemented changes last year to exclude coverage for cyber attacks during a war, retaliation by one state against another, and attacks on critical infrastructure. Port managers should check both cyber and property/casualty insurance policies for the fine print and request that investments in port risk mitigations be valued during policy renewals.

- [ ] **Do Not Chase or Rely on Compliance**
While the Coast Guard will establish minimum cybersecurity requirements that meet international and industry-recognized frameworks, each port operator should determine their own unique risk and identify the suite of technologies from companies who track, know, and can quickly respond to the threat better than the government.

- [ ] **Consider Changes in Purchase Orders**
For the marine terminal operators in the process of purchasing new cranes or other connected equipment, add terms and performance specifications that mitigate surveillance and cyber risk. Also, plan to invest and install after-market software protections and other applications to mitigate risk.

- [ ] **Specify Cyber Protections in Future Orders**
The port team must review and update performance and acquisition documents prior to purchase to stipulate terms and conditions for the software, controllers, and connectivity that meets the Facility Security Plan. Once deployed, continuous visibility of equipment remains critical to monitoring which devices are communicating to each other or even of communications reaching industrial devices from outside the port.

- [ ] **Send your Team to National Cyber Security Exercises**
National organizations have organized events like the Maritime and Control Systems Cybersecurity Con specifically for the port industry to raise awareness, share ideas, and offer solutions to mitigate cyber risk.

- [ ] **Have Expertise on Call**
Starting with your local COTP, CISA and FBI representative, but extending to companies with the experience to safeguard your entire inventory of cyber-physical systems, identify the sources of protections and recovery now while your cranes are operating, as opposed to when they go down and each hour is lost revenue.

If you have questions or need more information on these items, please email ckennedy@nawe.us