Cybersecurity and Infrastructure Security Agency

December 2020

PORT FACILITY CYBERSECURITY RISKS

Maritime facilities are critical for the shipment and reception of raw and finished goods for trade within the United States and with other countries. More than 90 percent of the volume of overseas trade enters or leaves the United States by ship. In order to operate efficiently, maritime facilities use information technology (IT) and operational technology (OT) systems for various functions, including communication, equipment operation, cargo tracking, and business operations. Compromise of these systems could lead to disruptions of port operations and related supply chains, resulting in financial losses.

The Department of Homeland Security (DHS)/Cybersecurity and Infrastructure Security Agency (CISA) developed this infographic to show examples of how cyber attacks could impact different aspects of port operations. The risks identified here do not encompass all risks to maritime facilities, and are only meant to demonstrate some of the potential activities of malicious cyber actors. Compromise of these systems could lead to an incident resulting in public health and safety concerns, environmental damage, transportation system disruptions, or economic disruption in a particular area.

Port Components at Risk

1 Facility Access

The degradation or disruption of systems used to identify and direct cargo, truck drivers, and facility personnel can cause significant congestion or the closure of the terminal until systems restoration is complete.

2 Terminal Headquarters – Data

Malicious actors may access information systems within the terminal in order to access sensitive client and cargo information. Malicious actors may also attempt to use this information to steal cargo or smuggle illicit cargo through the terminal.

3 Terminal Headquarters – Ransomware

The manipulation or destruction of data, most commonly seen in ransomware attacks, can disrupt operations within a facility until systems and data can be restored from reliable, isolated backups. Previous attacks have resulted in facilities being partially or completely offline for days, resulting in significant business losses.

4 Operational Technology (OT) Systems

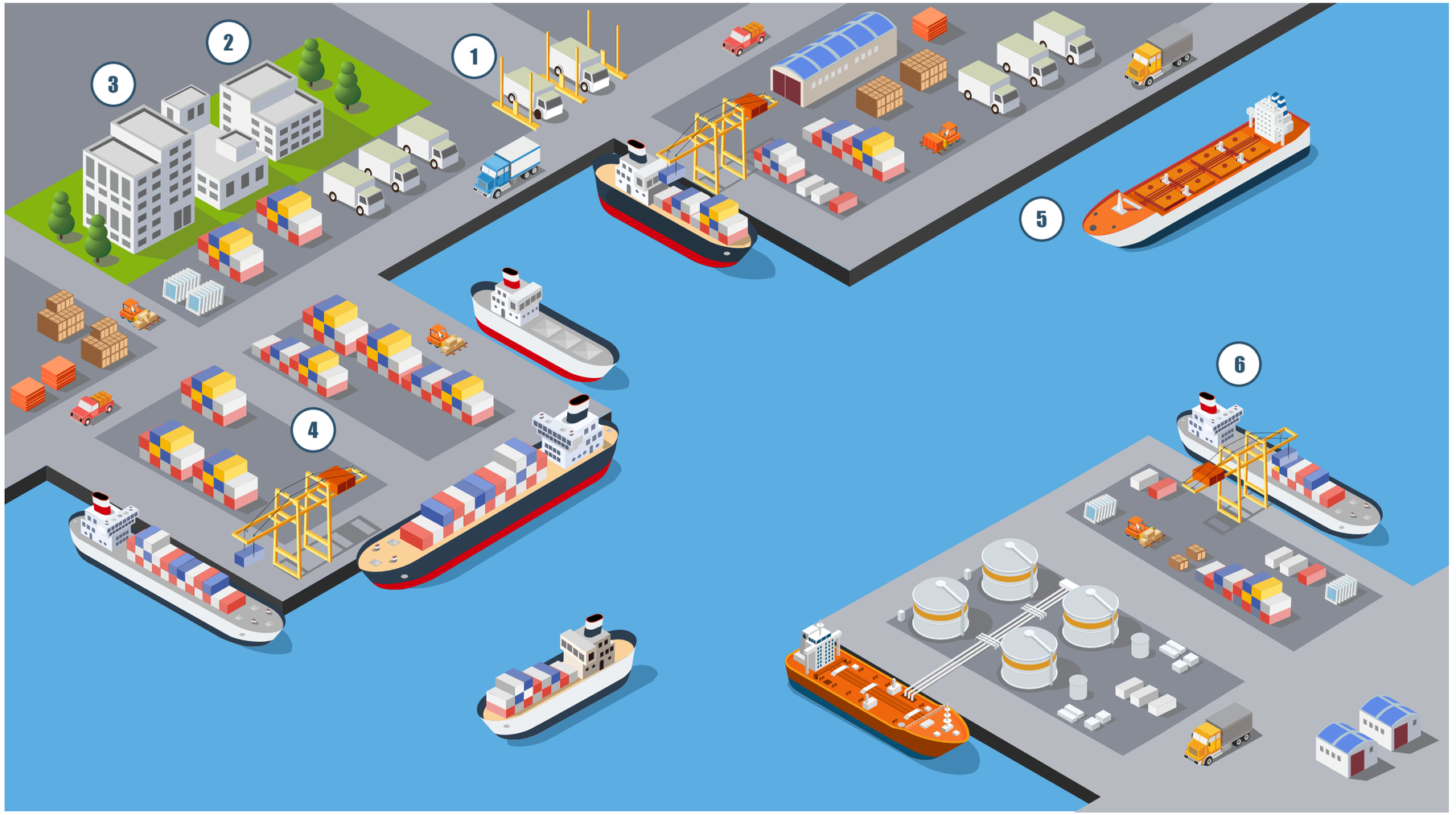
OT Systems – systems, devices, and communications links used to control physical processes at ports, including cargo handling equipment and pumps – are being increasingly incorporated into maritime facilities. The compromise of OT systems could cause changes to cargo movements, interrupt port operations, and cause physical damage to equipment and safety risks for personnel.

5 Positioning, Navigation, and Timing (PNT)

Position, Navigation, and Timing is pervasive throughout the Maritime subsector, and plays an essential role in many maritime functions such as vessel navigation and port logistics. Loss of PNT services would disrupt vessel movements in the port and complex logistics systems at port facilities. Loss of PNT could also lead to collisions and allisions, resulting in potential damage to fixed infrastructure, pollution, release of hazardous material, fires, loss of life, vessel sinking, and blocking of a navigable channel.

6 Vessel

Compromised systems aboard a vessel or inside a port facility could lead to the compromise of additional waterside or landside systems. Interconnectivity between berthed vessels and maritime facilities through the sharing of Wi-Fi, network connections, USB storage devices, etc. can lead to system compromises that otherwise may not have occurred.



Maritime industry partners can take several steps to lower the risk to their facilities from malicious cyber activity. The infographic titled “Cybersecurity for Maritime Facilities” (**https://homeport.uscg.mil/Lists/Content/Attachments/54645/NRMC%20-%20Cybersecurity%20for%20Maritime%20Facilities.pdf**) introduces the use of the NIST Framework and provides an overview of how and what to report to federal entities in the event of a significant cyber incident. CISA’s Cyber Essentials (www.cisa.gov/cyber-essentials) is a guide for smaller organizations to develop an actionable understanding of where and how to start implementing organizational cybersecurity practices. Suspected PNT degradation, disruptions, and other issues or anomalies should be reported to the U.S. Coast Guard Navigation Center (**www.navcen.uscg.gov**).