Cybersecurity Framework for Maritime Port Management

By

Maryyum Masood and Rizwana Abbasi

Maritime ports act as mediums for international trade and transportation. They facilitate the legitime flow of trade and the transfer of goods between ships and shore. Ports have the requisite infrastructure to run routine operations, such as handling the docking of ships and cranes and management of storage facilities and warehouses. Ports not only link the sea lines of communication (SLOC) but also connect to land transportation, such as highways, railroads, and airports, enabling the smooth movement of goods to and from the ports.

Maritime ports authorize customs clearance and are involved in regulatory checks, ensuring compliance with national and international law. Ports perform most of these functions digitally. Maritime ports are now under serious threat of malicious cyberattacks that can disrupt and compromise port operations worldwide.

Industry is deeply interconnected, and a cyberattack on one major port can send shockwaves through global trade networks. Consider a scenario where a major port, responsible for handling millions of cargo containers, suddenly halts operations due to a cyberattack. Cranes freeze, logistics systems collapse, and cargo ships are left stranded at sea. This is not a hypothetical scenario; it is a real and escalating threat to global trade.

The maritime industry, long seen as the backbone of international commerce, now faces an urgent cybersecurity crisis. Ports are no longer just about cranes and cargo; they have evolved into digital ecosystems reliant on interconnected networks, automation, and artificial intelligence. As ports become smarter, they are also becoming more vulnerable. Cybercriminals are increasingly exploiting these vulnerabilities, causing financial losses, operational disruptions, and even national security risks.

Maritime cyberattacks are no longer rare occurrences, they are becoming alarmingly frequent. In 2023, a ransomware attack crippled more than 1,000 vessels by targeting a software provider used across the shipping industry. The attack forced the shipping industry to shut down its ShipManager system, affecting global supply chains. A year earlier, the Port of Lisbon suffered a cyberattack that took its website offline for days, with the ransomware group LockBit claiming responsibility and alleging that it had stolen financial reports, contracts, and ship logs.

In Germany, a 2022 cyberattack on two oil companies disrupted fuel shipments, forcing Shell to reroute supplies and exposing the vulnerabilities of critical maritime infrastructure. The 2017 NotPetya ransomware attack, which paralyzed Maersk and caused an estimated $300 million in damage, remains one of the most devastating cyberattacks in shipping history.

Ports are among the most attractive targets for cybercriminals. The motives behind these attacks vary as some hackers seek financial gain, while others aim to steal sensitive trade-related data, and some may even use cyberattacks as part of hybrid warfare.

The economic consequences are staggering, from ransom payments and insurance hikes to delays that can ripple across global supply chains. Beyond financial losses, cyber threats to ports pose serious security risks. For example, a well-coordinated cyberattack on a major port could disrupt military logistics, cripple trade networks, or even manipulate cargo data to facilitate smuggling and illicit trade.

Hackers carry the potential for unauthorized intrusion into ports' digital networks and interrupt ports' routine operation through malicious software attacks. The workforce involved in port management may be trapped into revealing sensitive data by clicking on malicious links. The hackers can also disrupt digital networks that regulate critical port infrastructure, such as cranes, pumps, and valves. Supervisory control and data acquisition (SCADA) systems can come under cyber threats disrupting routine functions. Nonstandard computing hardware like sensors, actuators, or appliances that transmit data from the network wirelessly are vulnerable to data theft.

Hackers can steal data such as cargo manifests, crew information, and financial records. They can also manipulate data, such as altering cargo manifests, or manipulate navigation systems. Hackers can also steal intellectual property, such as trade secrets or proprietary software.

Another pressing issue is supply-chain security. Ports rely on a complex web of third-party vendors for logistics, software, and cargo management. If one vendor is compromised, the entire port system could be at risk.

Hackers can also use unmanned aerial vehicles (UAVs) for surveillance means or to attack port infrastructure, such as damaging equipment or disrupting power supplies. Ports may be exposed to cyberattacks through third-party suppliers, such as logistics providers or maintenance contractors. Ports may be exposed to cyberattacks through cargo and containers, which may contain malicious devices or software.

Cybersecurity in the maritime sector is often treated as an afterthought. Many ports still operate with outdated software and weak security protocols, making them easy targets. Given the critical role of ports in the global economy, the widening cybersecurity gap is a growing challenge. Strengthening port security necessitates urgent regulatory mechanisms, some of which are proposed below.

Regulatory Mechanisms

To mitigate the growing cyber threat, ports should adopt internationally recognized cybersecurity frameworks. First, ports should adhere to the rules and protocols of the International Maritime Organization's (IMO) Maritime Cyber Risk Management Guidelines, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and ISO 27001 standards. Implementing these frameworks will help establish clear security protocols and ensure that ports are prepared to defend against cyberattacks.

Second, network security should be reinforced by segmenting information technology (IT) and operational technology (OT) systems, preventing malware from spreading across critical infrastructure. Regular penetration testing and vulnerability assessments can further identify weak points before attackers do.

Third, investing in cybersecurity training for port workers is equally crucial. Many cyberattacks exploit human error—phishing e-mails, weak passwords, and social engineering attacks remain among the most common entry points for hackers. A well-trained workforce can serve as the first line of defense against these threats.

Fourth, leveraging artificial intelligence and machine learning for threat detection can enhance ports' ability to identify cyber risks before they escalate into full-scale attacks. Artificial intelligence (AI)–led systems can monitor network activity in real time, flagging suspicious behavior and predicting potential breaches before they happen. In this regard, the strict security assessments of third-party vendors and blockchain-based cargo tracking can enhance transparency and reduce the risk of supply-chain cyberattacks.

Fifth, beyond prevention, ports should also be prepared to respond effectively to cyber incidents. For this, establishing cyber incident response teams (CIRT) can ensure that ports have trained professionals ready to mitigate and recover from cyberattacks swiftly.

Sixth, regular cyber drills and crisis simulations should be conducted to test response plans. This ensures that when an attack occurs, the damage is minimized, and recovery is swift.

Seventh, international collaboration to deal with these threats is essential. Governments, port authorities, and private stakeholders should work together to share intelligence, standardize security protocols, and invest in collective defense mechanisms.

Public-private partnerships can play a key role in funding advanced cybersecurity infrastructure, while international regulatory bodies like the IMO must enforce stricter cybersecurity mandates across the industry. Finally, as ports transition into smart ports, powered by the internet of things (IoT), AI, and automation, cybersecurity should be at the forefront of maritime security strategies. Emerging technologies like quantum computing and zero trust architecture will play a crucial role in strengthening digital defenses, but ports should remain vigilant. The very technologies designed to enhance security could also introduce new vulnerabilities if not properly managed.

Cybersecurity is no longer just a technical issue; it is a fundamental pillar of modern port management. If cybersecurity continues to be treated as an afterthought, the next major cyberattack could bring global trade to a standstill. Ports are the lifelines of the world economy, and securing them is not just about protecting data, it is about safeguarding the stability of international commerce and national security.

Maryyum Masood is working as a Research Officer & Associate Editor at the Center for International Strategic Studies (CISS) Islamabad. She is an MPhil scholar in the Department of Strategic Studies at the National Defense University (NDU) Islamabad.

Rizwana Abbasi is an Associate Professor of Security Studies at the National University of Modern Languages, Islamabad, a non-resident Fellow of the Center for International Strategic Studies (CISS), Islamabad, and a Visiting Fellow at the Central European University of Austria.