BREAKBULK
AMERICAS

Responding to Inevitable Port Cyber Attacks: Case Study Comparison of Rotterdam and Seattle

Student Names: Arian Estrada, Sahith Gedela, Jason Lazo, Abdul Turay, Nathan Victoriano

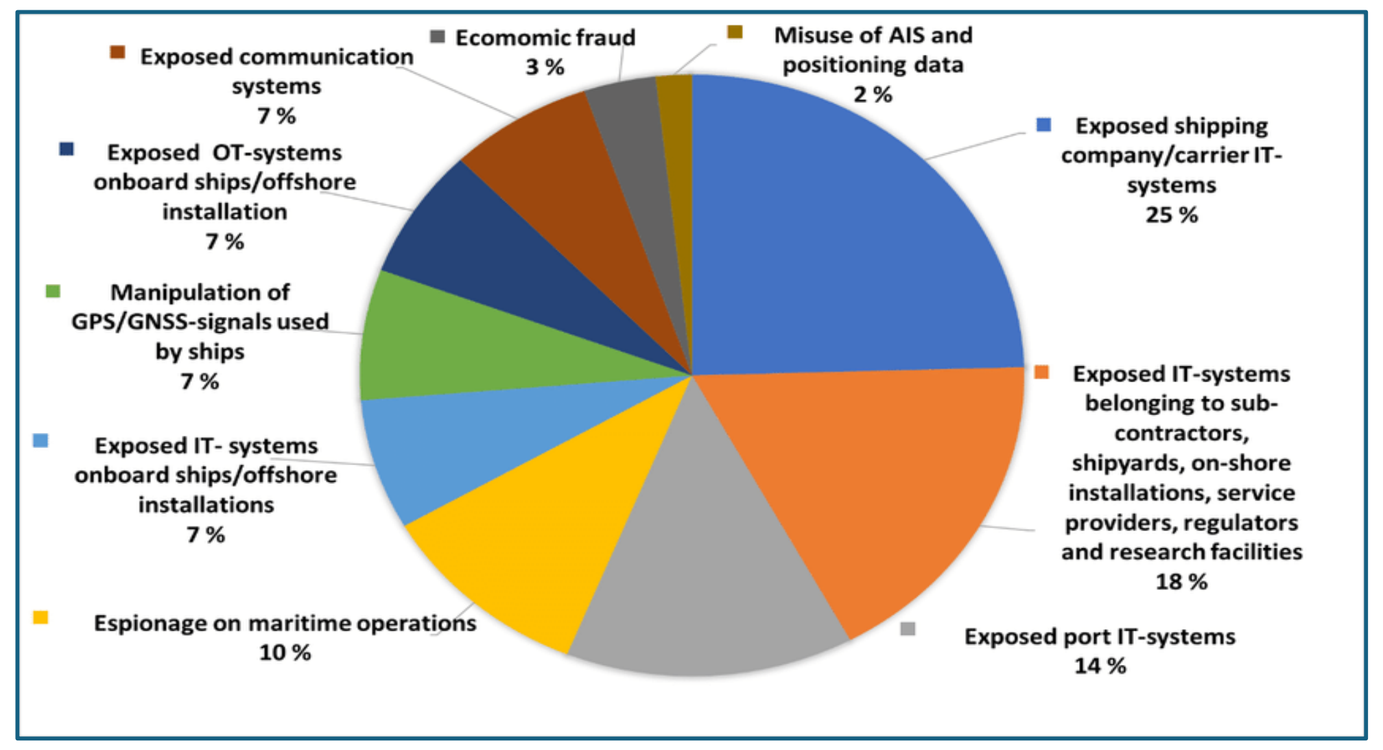
Faculty Advisor:
Professor Daniel Cassler

University of Houston

Abstract

According to the Naval Dome firm, cyberattacks on maritime transport have increased by 400% in 2020. The current port infrastructure needs to adopt newer, safer technologies to increase efficiency and security for port infrastructures. With various ports supporting markets worldwide, these ports are the lifeline of the maritime industry. Therefore, its security and efficiency should be of utmost priority. However, the digital programs currently being used by ports have proven to be vulnerable to cyberattacks. Our research highlights two port infrastructure examples, one being The Port Seattle and The Port of Rotterdam. These studies highlighted their three best prevention practices and incident plan recommendations to ensure the long-term safety of port cybersecurity.

Maritime Cybersecurity



Graph 1: Top cyber-attacks on the maritime adapted from ResearchGate

25% Cyberattacks caused by Exposed IT Systems

$ The Maritime Supply Chain represents $5.4 Billion

Port of Seattle

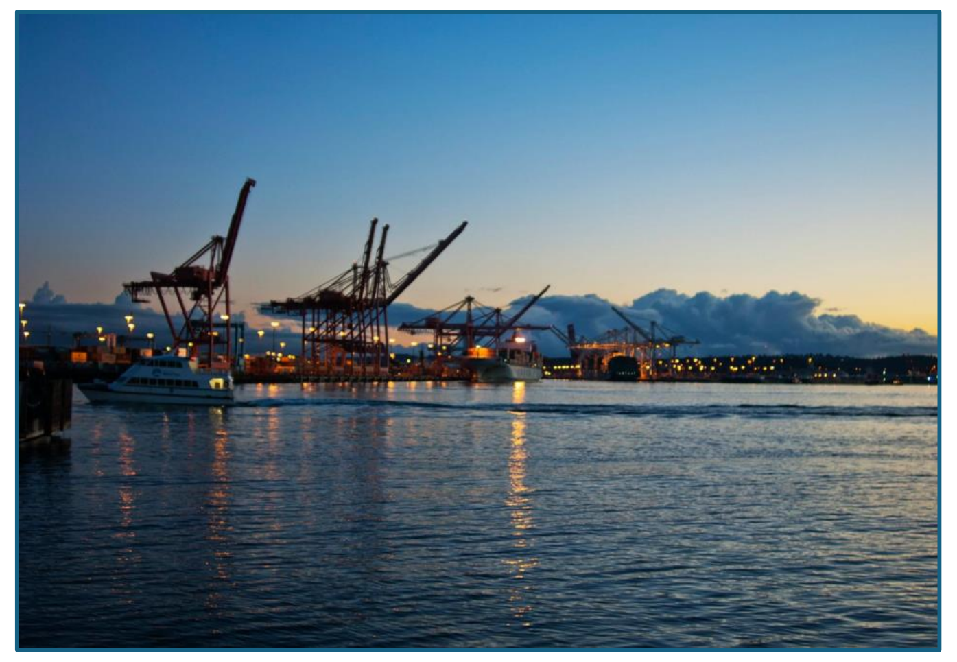


Photo 1: Port of Seattle
(Taken by The Authority of Washington Business).

On August 24, 2024, the Port of Seattle was hacked by Rhysidia, an illegal cyber-attack organization, and had critical systems compromised causing system wide delays. Even after the Ransomware attack, the Port of Seattle has refused to pay the $6 million in ransom to Rhysidia. As of September 2024, the port is still partially immobilized to the concern of retailers and suppliers around the globe. Since being founded in 1911, the port of Seattle has risen to becoming one of the most significant economic forces within Washington. Their total exports in 2023 were worth $13.2 billion and their total imports were worth $57.4 billion.

7-day recovery time

$ 6 million in estimated losses and counting

Ransomware caused by exposed IT Systems

Port of Rotterdam

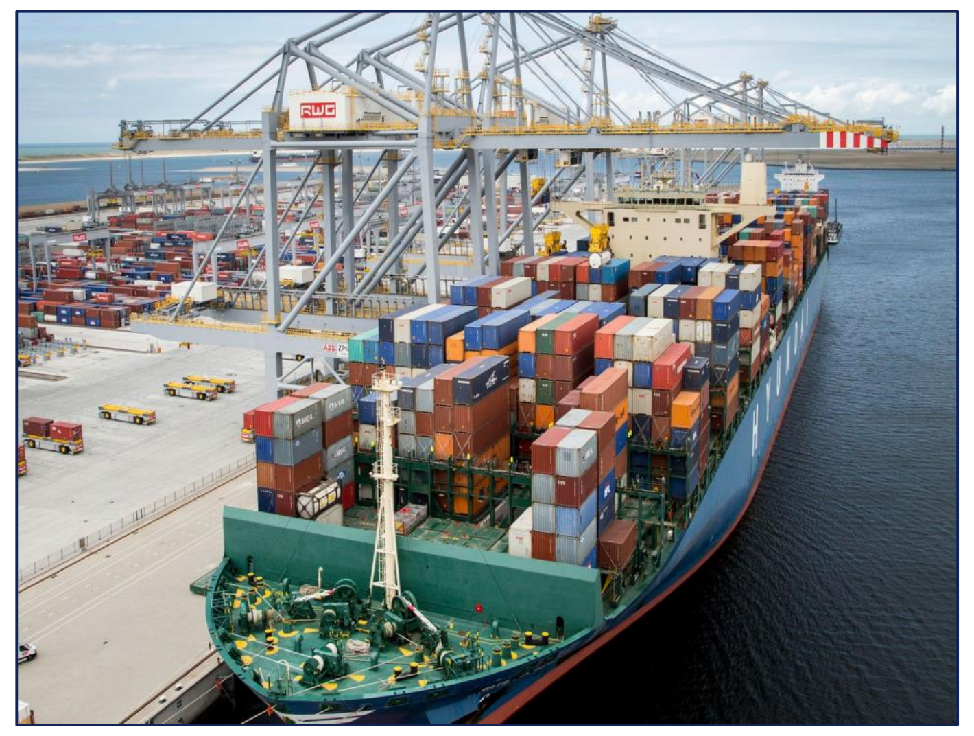


Photo 2: Vessel at Port Rotterdam
Shutterstock. (2019).

In the past, there have been a series of ransomware attacks that have negatively impacted 17 ports and oil terminals across Europe as of January 2022. Also, in June 2023 Port Rotterdam was attacked with a DDOS malicious cyberattack to disrupt software systems moreover, Port Rotterdam is in the Netherlands. Port Rotterdam is the biggest seaport in Europe. Port Rotterdam is important for oil and gas transportation across many cities in Europe and the world. According to Maritime Gateway News 2023, "report from Dutch news outlet RTL shed light on the motive behind the cyberattacks. A hacker group self-identified as NoName 057(16) claimed responsibility.

5-day recovery time

$ 300 million in estimated loses

DDoS caused by exposed IT Systems

Prevention Strategies

Cybersecurity practices

Automatic identification systems (AIS), Voyage data recorder (VDR), Electronic chart display and information systems (ECDIS), specialized IT or OT systems, and firewalls.

DDoS Protection

Has the ability to monitor cybersecurity threats live. Blocks out communications with outdated or unauthorized ports and or applications. Implements a load balancer along with restricting network traffic to designated areas.

Block Chain Technology

Can be utilized for peer-to-peer transactions, security of data and communications. Cuts costs by cutting out middle-men and 3rd party web services/ programs.

Incident Response Plan

Notify the CISA and cut off infected systems

Rotterdam mitigated financial losses by emphasizing labor and technology consulting toward remaining 50% of working ports

Anticipate 5-7 Day recovery time. Seattle and Rotterdam emphasized to not pay ransom

Conclusion

Based upon the case studies of the cyber-attacks done on Port Rotterdam and Seattle, a prevention plan and incident response plan can be synthesized. There have significant gaps in Port Maritime Security; as outdated and exposed IT systems continued to be exposed despite recommendations made by the International Association of Harbor and Ports. Thus, mitigating losses through past practices is best.

Scan to see our Sources

Cullen College of Engineering
UNIVERSITY OF HOUSTON

DRIVING THE BLUE ECONOMY
TEXAS A&M UNIVERSITY AT GALVESTON

UTC Overseas

4D SUPPLY CHAIN CONSULTING

BECHTEL