Northwestern University Transportation Center

Business Advisory Council - Industry Technical Workshop

Cybersecurity Practices in Transportation and Logistics

Sheeba Varughese
Chief Information Officer

May 15, 2024

Port of Los Angeles

- America's Port®
- Founded Dec. 9, 1907
- A department of the City of LA
- Governed by the Los Angeles Board of Harbor Commissioners
- Ranked as No. 1 container port in Western Hemisphere for 24 consecutive years (2000-2023)
- 7,500 acres (4,300 land/3,200 water)
- 43 miles of waterfront
- 25 cargo terminals including seven container terminals
- 122 miles of rail
- 15 marinas
- Connection to one in nine jobs in Southern California and nearly 3 million jobs nationwide

Cyber Security

Cyber Security Operations Center (CSOC) Focus:
Port Cybersecurity Operations

Cyber Resilience Center (CRC) Focus:
Port Ecosystem Resilience

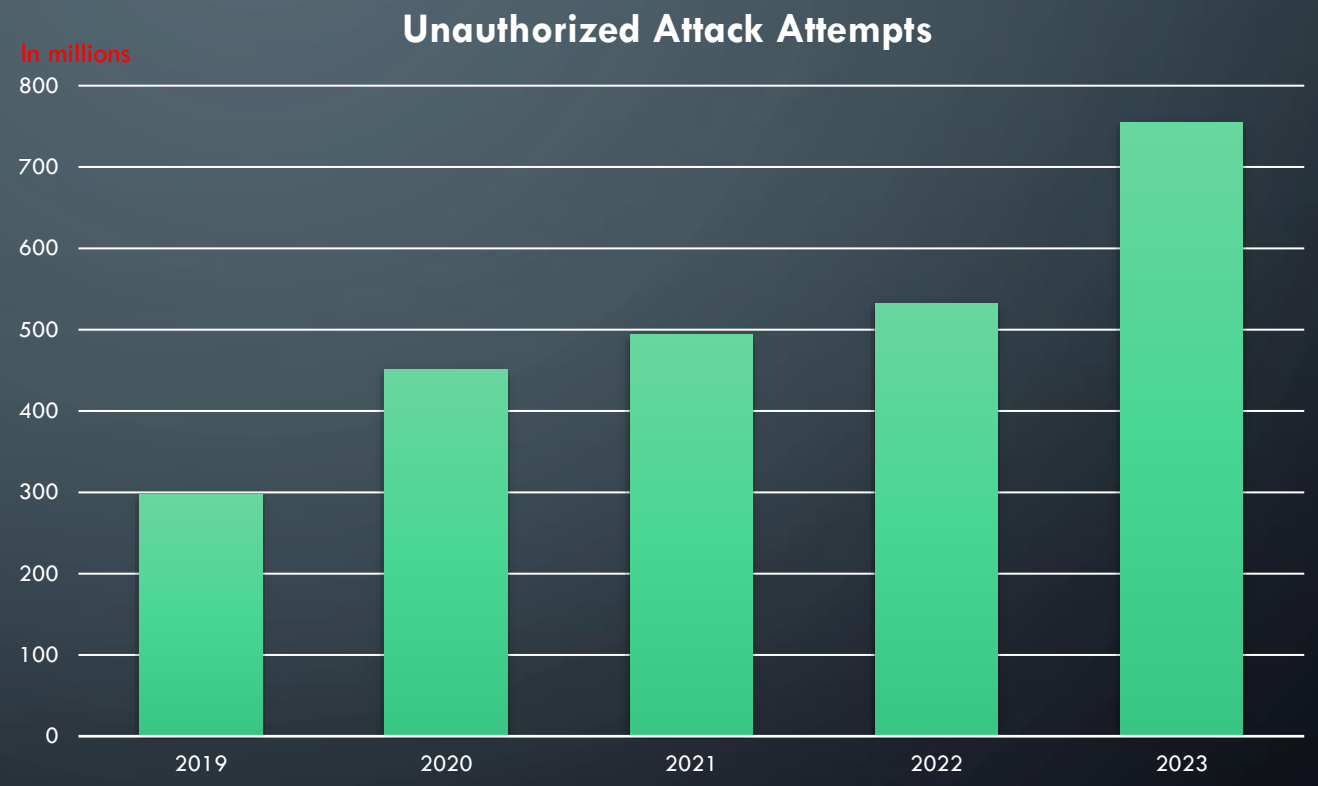
Port of Los Angeles Cyber Security

- Technologies: Cyber Security Operations Center – Best of breed solutions
- Processes: ISO 27001 certified Information Security Management System, NIST, FedRAMP
- People:
  - CSOC Team: Full-time employees with industry credentials
  - Computer Users: Mandatory cyber security awareness training

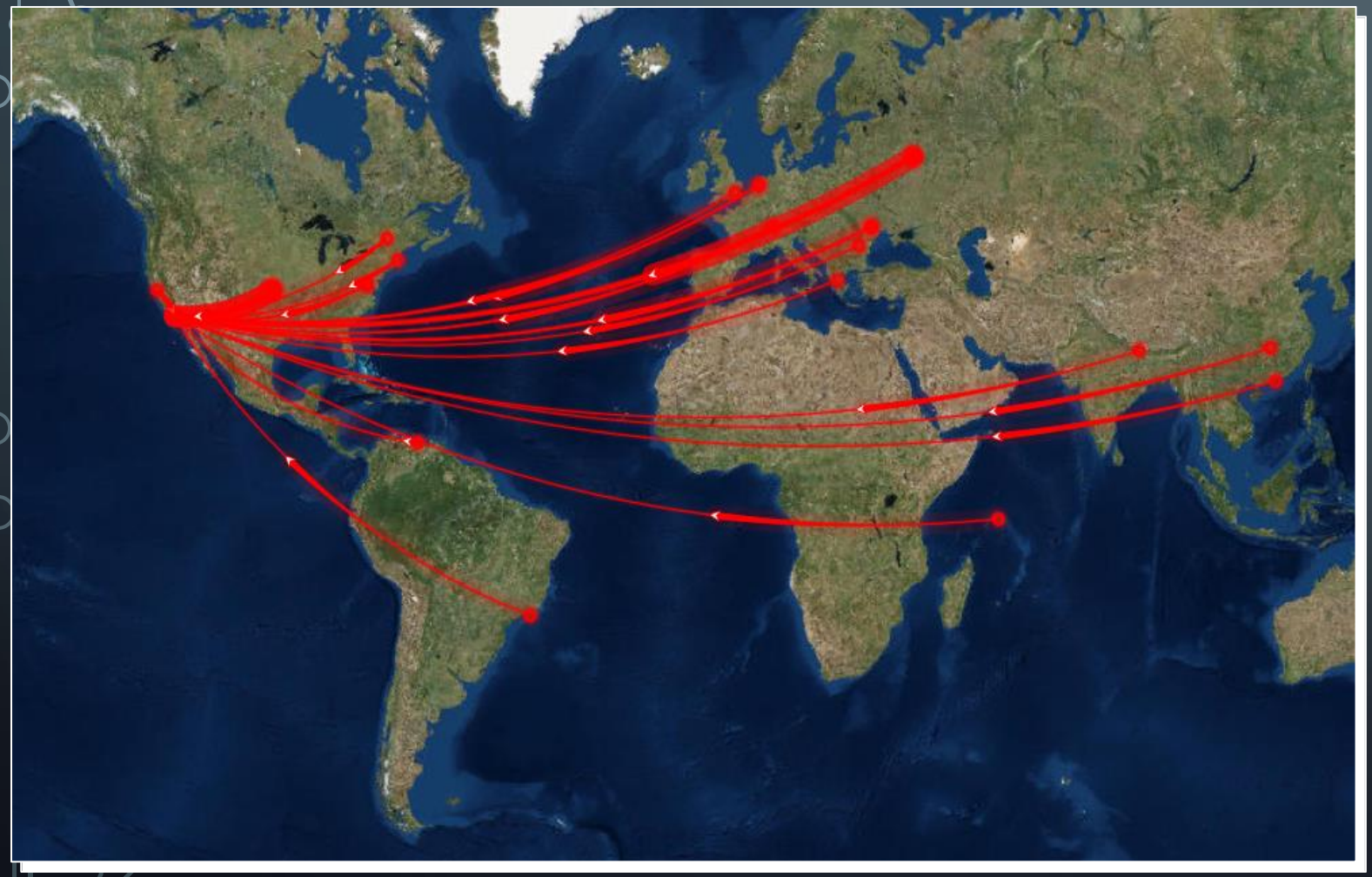
Cyber Operations Center / Use Cases

THE PORT OF LOS ANGELES

- Security Posture Overview
- Situational Awareness
- Infrastructure Monitoring
- Denial of Service/Distributed Denial of Service (DoS/DDoS)
- Malware Outbreak
- Trusted 3rd Party and External Vendor Provider Services



Cyber Resilience Center



- Cyber attacks continued against our computer systems with more frequent intrusion attempts
- Cyber risks increased
  - Digitalization
  - Maritime Incidents
  - Coordinated Attacks
- Port of Los Angeles established contract agreement with IBM

Cyber Resilience Center Concept

- Reduce cyber risks that could disrupt the flow of cargo
- Early warning system for the ecosystem with improved quality, quantity and speed of cyber information sharing
- Greater collective knowledge of relevant cyber threats in the supply chain community
- Collaboration forum for stakeholder cyber personnel
- Information/advisory resource for recovery
- CRC is non-invasive, non-disruptive to existing cyber security operations

Cyber Resilience Center Facility

State-of-the-Art facility completed October 2022

- 24x7, Onsite 8-5 and On-call After Hours
- Secured
- Located at the Harbor Administration Building

ISO 27001 CERTIFIED by schellman

Cyber Resilience Center Operations

Operated by IBM

- Operational since January 2022
- Qualified Cybersecurity Analysts
- Weekly threat intelligence reports
- Correlate ecosystem security events
- Share, distribute and notify stakeholders of potential risks to the ecosystem
- Annual Cyber Security Awareness Training
- ISO 27001 certified

Cyber Resilience Center Use Cases

THE PORT OF LOS ANGELES

- Threat Intelligence and Threat Landscape for Maritime Sector
- CRC Ecosystem Security Posture
- Malware/Hacker Group Focused
- Ecosystem Cyber Incident Focused

Cyber Resilience Center

THE PORT OF LOS ANGELES

What CRC will not do

- Not a replacement of stakeholders' cybersecurity efforts or security efforts overall
- Not intended to take responsibility for whether stakeholders take action on what risks are shared with them
- Not designed to intrude on stakeholders' current system
- Will not share information shared beyond the designated list of Port of LA stakeholders
- No sensitive information (i.e. no personally identifiable or business sensitive data)
- Not intended to expose stakeholders' cyber vulnerabilities
- Not additional information noise
- Not an elimination of stakeholders' cyber risks

Cyber Resilience Center

THE PORT OF LOS ANGELES

Questions?