Maritime Cybersecurity

Jim Merten, MA, CEM

Port Security Specialist (Recovery/ Salvage)

Sector Columbia River Overview

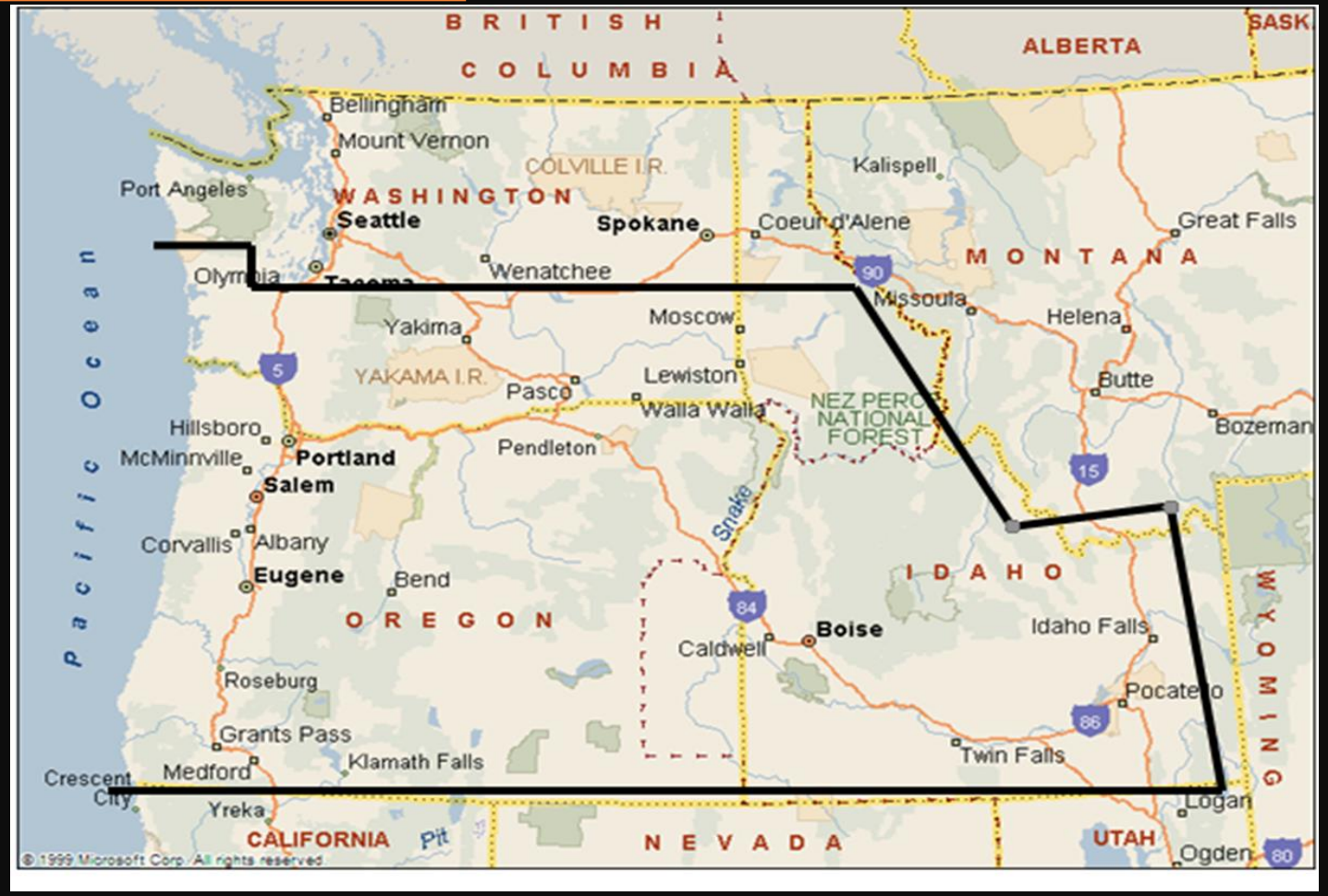
- USCG Sector Columbia River (SCR) is located in Warrenton, Oregon. Marine Safety Unit Portland, a subordinate command of the Sector (and the Sector's Prevention Department) is located in Portland, Oregon. Sector will be relocating to Portland in 2023.

- The Columbia-Willamette-Snake MTS, formed by the navigable portions of the Columbia, Willamette, and Snake Rivers, is a vital element of the economic engine of the American Northwest, and more broadly, to the Nation as a whole.

- It is one of the few port systems in the Nation to export more goods than it imports.

- It is also the top gateway for American wheat and barley exports, as well as a major exporter of corn, bulk minerals, timber, and paper products.

Sector Columbia River Overview



CG Cyber Strategy

- **Maritime Critical Infrastructure:**
  - Vessels
  - Facilities
  - Port complexes
  - Intermodal connections
  - Bridges
  - Other components needed to operate the MTS
  - People who operate these systems & live/recreate in our maritime domain.

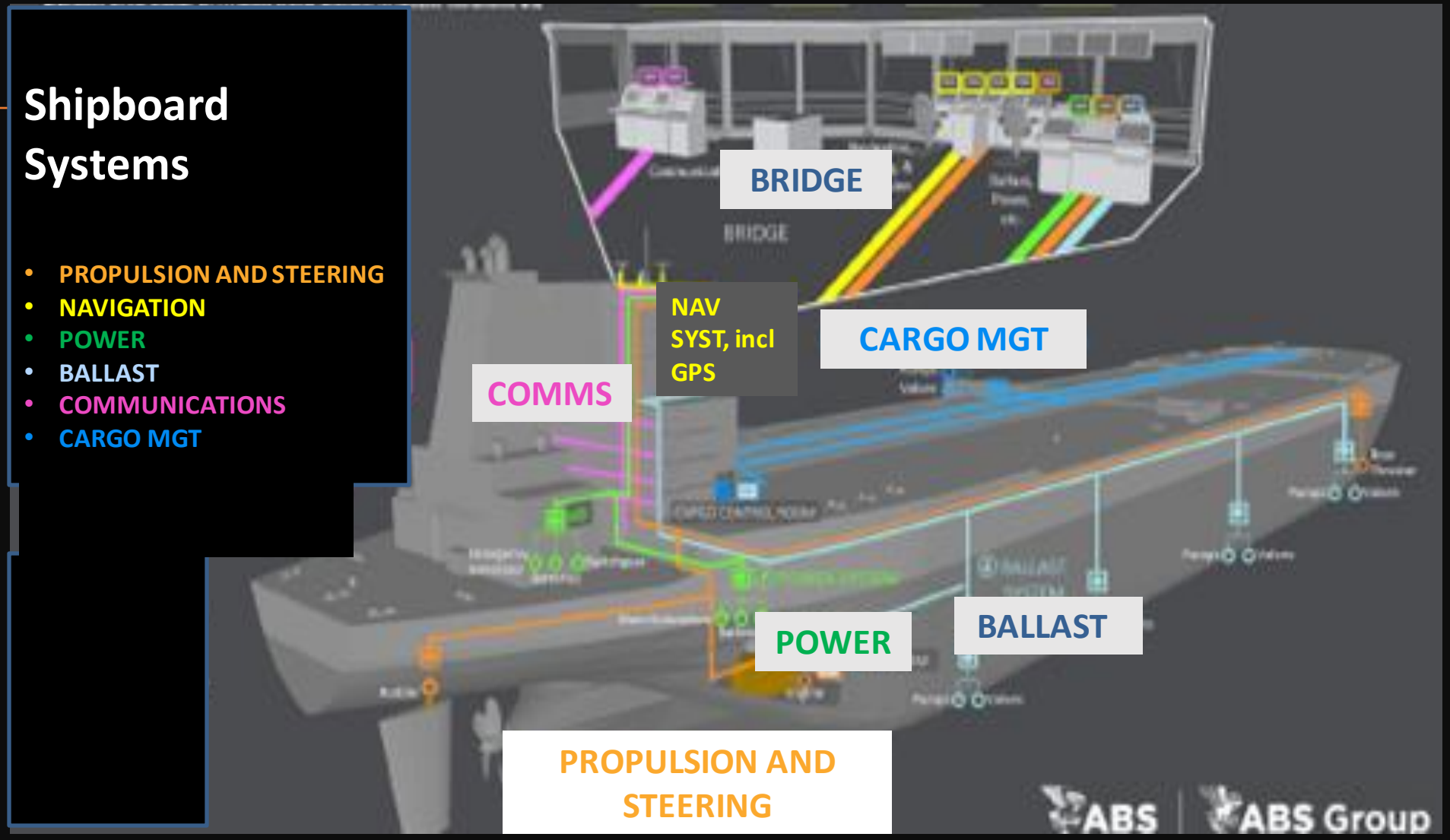
Marine Transportation System Supply Chain

Systems in the MTS at Risk

What Kinds of Systems are at Risk in the MTS?

Shipboard Systems

- PROPULSION AND STEERING
- NAVIGATION
- POWER
- BALLAST
- COMMUNICATIONS
- CARGO MGT



What Kinds of Systems within the MTS are at Risk?

Cybersecurity Incidents and Case Study

Maritime Cybersecurity Incidents

USCG Sector Columbia River

AUG 2020

Industry Partner Email Spoof

Industry Partner email spoof, phishing attempt within the COTP Zone.

JAN 2021

Bluewater Shipping Phishing Attempt

Bluewater shipping notified the CG that one of our own email addresses was spoofed. The awareness and actions from the agent receiving the emails were key to avoid compromise of their system.

OCT 2020

IMO Hack

The International Maritime Organization was hit with a ransomware attack.

Foss Maritime Phishing Attempt

Foss Maritime discovered a phishing attempt and alerted employees and the CG, thwarting further attack.

NOV 2020

Port of Kennewick

The Port of Kennewick was hit with a ransomware attack. This Port is not an MTSA facility, but we still track incidents.

FEB 2021

Columbia River Bar Pilots

The Bar Pilot's off-site contracted server was hit with a DDoS attack. The server was switched to backups and brought back on-line after a short delay.

DEC 2020

SolarWinds

SolarWinds malware discovered to be in systems since 2019. Advanced Persistent Treat (APT), acknowledged. DHS/ CISA issued a rare Emergency Directive. Government agencies most vulnerable

MAR 2021

Port in the COTP Zone

System compromised due to the Microsoft Exchange Vulnerability. CG CYBER Protection Team deployed to assist.

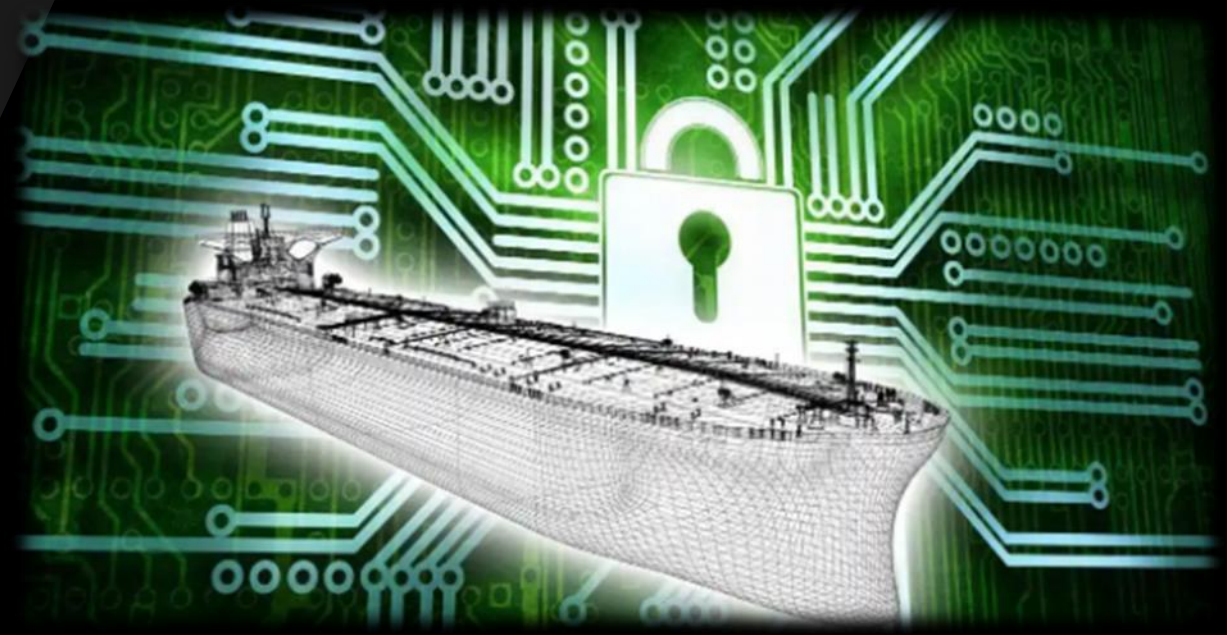
Case Study – “The Shipyard”

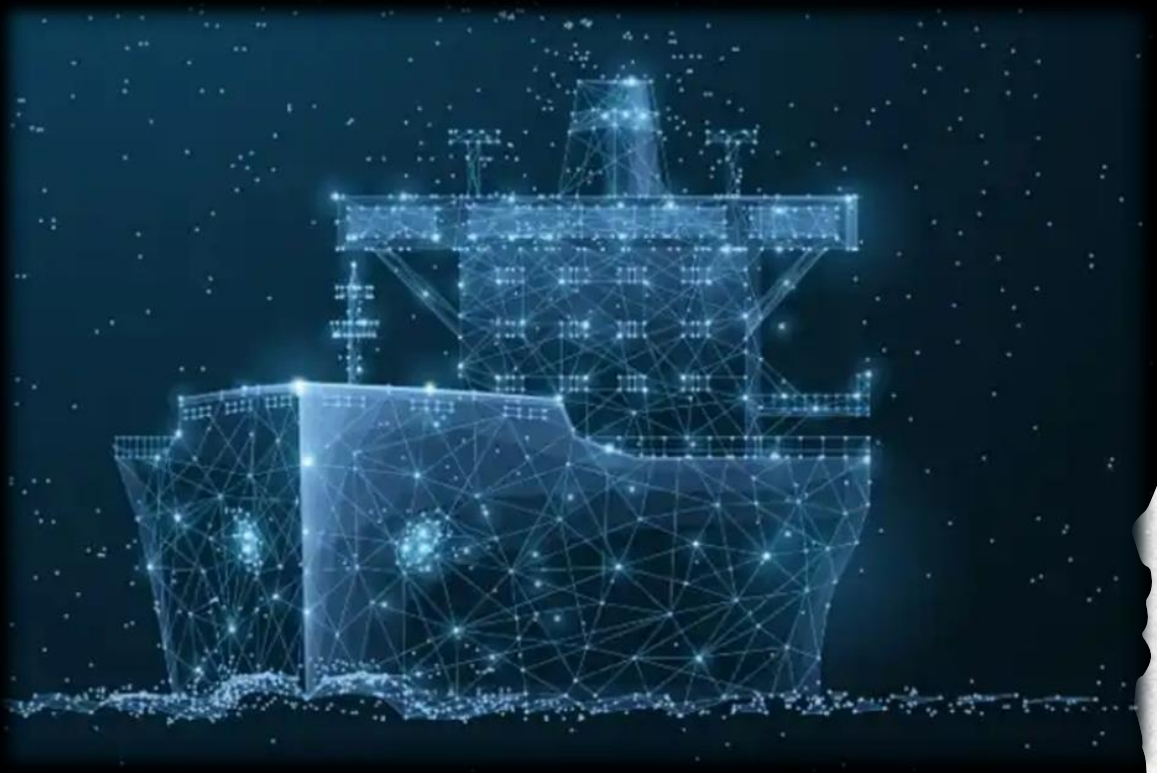
- On Monday, June 6, 2022, “The Shipyard” became concerned about suspicious, unauthorized activity that was occurring in relation to their network environment. Specifically, they learned of a connection between a device on their network and a known malicious IP address.
- They immediately engaged external cybersecurity forensic experts at Stroz Friedberg through counsel. Stroz Friedberg is continuing to conduct a comprehensive digital and forensic investigation through forensic acquisition of systems, malware analysis, firewall and other log collection and analysis, and dark web scanning. Given certain developments and new information they have identified via the work Stroz Friedberg is conducting, they notified the CG.
- This Shipyard is not MTSA regulated so this does not come through our regular cyber incident reporting structure. (CG)

Findings

As of June 29, core systems are back up and running, and the shipyard does not currently anticipate any material negative impact to operations or timetables for customer deliverables. Shipyard has taken deliberate steps to review and fortify systems and to implement tactical measures under the guidance of their system recovery and restoration expert, MoxFive, before bringing them back online.

To date, the shipyard has identified evidence that the threat actor accessed their network environment on or about April 20, 2022. A domain controller and several accounts were compromised. The threat actor also deleted certain event logs and other forensic artifacts from systems and re-named malware and processes to approximate shipyards internal naming conventions





Findings Cont.

The forensic team identified the presence of data exfiltration malware in use during the May 18 - June 6, 2022 time frame, and evidence that internal files and customer-related files and information were accessed and ex-filtrated. Extensive work is underway on a prioritized basis to identify forensic evidence of the specific customer information and files that may have been accessed or removed from the network.

TIMELINE

Shipyard Cyber Attack
SCR COTP Zone

20APR22

Threat actor gained access to the network environment.

18MAY22

Internal and Customer files were accessed and exfiltrated.

06JUN22

Shipyard discovered the intrusion and was concerned about suspicious unauthorized access. Yard immediately employed forensic experts Stroz Friedberg through legal counsel

08JUN22

Took system off-line.

09JUN22

Made external notifications to DoD, FBI, DCSA, and DHS CISA.

29JUN22

Core systems back up and running. Over 5TB of data stolen.

USCG Cyber Protection Team

USCG Cyber Protection Team

- Based in Alexandria, Virginia, CPT is the Coast Guard's deployable unit responsible for offering cybersecurity services to the Marine Transportation System (MTS).
- CPT consists of three teams of active duty Coast Guard cybersecurity professionals who are trained and certified in delivering the four core CPT services: **Assess, Hunt, Clear and Harden.**

USCG Cyber Protection Team

- The CPT ’s mission is to enhance the resiliency of MTS Critical Infrastructure against cyber disruption through consistent proactive engagements with public and private industry organizations.

- The CPT stands ready for worldwide deployment to conduct operations.

USCG Cyber Protection Team

MaritimeCyber@uscg.mil.

USCG Cyber Protection Team Missions

Assess

- *Penetration Testing:*
- Determine susceptibility to a real world incident by identifying weaknesses in security through internal or remote emulation of the tactics, techniques and procedures of Cyber threat actors.
- *Configuration Review:*
- Analyze operating system and database settings and configurations compared to industry standards, guidelines, and best practices.

Hunt

- *Threat Hunting:*
- Intel-driven operations to illuminate known or unknown adversaries on a network and determine the scope and purpose of a potential compromise.

USCG Cyber Protection Team Missions

Clear

- *Incident Response:*
- Assist stakeholders to target, contain and clear malicious activity from cyber systems. Identify indicators of compromise to enhance security posture.

Harden

- *Remediation of Vulnerabilities:*
- Recommend best practices for securing systems against specific findings of **Assess** or **Clear** engagements.

What if I have a Cyber Incident in the MTS?

MTSA Regulated Facilities:

National Response Center

Phone: 1-800-424-8802

NRC Watch Email: NRC@uscg.mil

Non- MTSA Regulated Facilities:

USCG Sector Columbia River Command Center

(503) 861-6300

Jim Merten,
Port Security Specialist (Recovery/Salvage)

James.t.merten2@uscg.mil