Shipping Sector

This document contains information about this sector in relation to cyber security and incident response. The information can be used for scoping an Incident response gameplay. This information is for guidance purposes only. Not all information will match every industry.

Examples of some shipping sector industries:

- Shipbuilding/wharfs
- Ports
- Freight land/sea

Known Cyberattacks against the shipping sector:

- https://marine-digital.com/cybersecurity_in_shipping_and_ports
- https://www.maritimeprofessional.com/news/cyber-security-threats-challenge-international-369770
- https://www.mitags.org/guide-ship-cybersecurity/
- https://portswigger.net/daily-swig/when-the-screens-went-black-how-notpetya-taught-maersk-to-rely-on-resilience-not-luck-to-mitigate-future-cyber-attacks

More information:

The most known attack on the shipping industry was the NotPetya attack on Maersk. It brought down their entire network leveraging the EternalBlue vulnerability to take control over their network. They were saved by a power outage in Nigeria, saving one of their domain controllers.

The shipping industry is constantly under cyber attacks. They have many attack surfaces, including ship radar systems, GPS systems, onboard networks, proprietary software, port logistics systems, and freight company customer records.

DDoS attacks on important communication or information systems will delay deliveries or, in the worst case, make them undeliverable.

Local communications systems are also vulnerable and may render a ship or a port useless if it cannot communicate properly with its customers.

Systems important to the shipping sector:

In the shipping sector, there are many vital systems. There are radar systems, GPS systems, networks, internal infrastructure, proprietary software, logistics systems for ports, land and sea-based freight, and company customer records and orders database. All of these are critical to the industry they are present in. If a ship loses its radar system, they do not know what other ships are nearby or if they are on a collision course towards a danger. Similar events can occur with the GPS systems on ships or in freight trucks. If they don't know where they are going, the chances are that they will be delayed, end up in the wrong place or get stuck.

Larger ports rely heavily on GPS and radar systems and automated on and offloading systems. Automated cranes can be a desired target since attackers can route containers full of valuables to a truck they control and create mayhem by sending containers on trucks they aren't supposed to be on, resulting in delayed shipments.

Recommended Incident Response Training Scenarios:

- Phishing
- Ransomware
- Credential theft
- Systems failure
- Weak open networks
- IoT devices
- Network breaches

Important review focus:

Awareness training

Make the employees aware of what to look after in potential phishing emails or people that look out of place. Question even those who look like they belong

General computer etiquette

An unlocked computer with the journal system open or access gives an attacker ample opportunity to plant malware, reverse shell, or a "command and conquer" (C2) beacon.

Recommendations for adapting the scenario to the sector:

To make the game more immersive, it is recommended to adapt the scenario by adding names familiar to the organization. This will bring more value to the exercise as the players can relate and get involved. This can, for instance, be (but is not limited to):

Industry-specific systems	Important Vendors of Equipment	Other People not in the game
Communication systems	Device vendors (Radar, GPS, logistics etc.)	Cleaning personnel
GPS systems		Janitors
Logistics systems	Software vendors (proprietary software, logistics software, etc.)	Secretary
Radar systems		Dockworkers

General info about Implementing an Incident Response Plan Into a Custom Scenario

Using the current incident response plan, working out how it fits the scenario, and creating “injects” based on this can make the game more immersive. The “injects” need to be realistic and pertain to the organization as well as the sector the organization is located.

The incident response plan should contain information on whom to contact, how to handle media, and any reputation-saving exercises. The plan should also have a clear recovery time objective (RTO), and recovery point objective (RPO) lined out, so the leadership knows how fast the employees can get up and running in the event of a total disaster.

In case of an information leak, there should also be a media campaign running or some PR mitigation. It should be clear who will be the media contact and the customer contact if those data are lost. If this is not in the incident response plan, it is a good learning experience to test out what the incident handlers will do under stress.