ACICE
ADMM Cybersecurity and Information Centre of Excellence

# UPDATE ON THE CYBER DOMAIN

Issue 10/23 (October)

## Maritime Cyber Security – Why It Matters

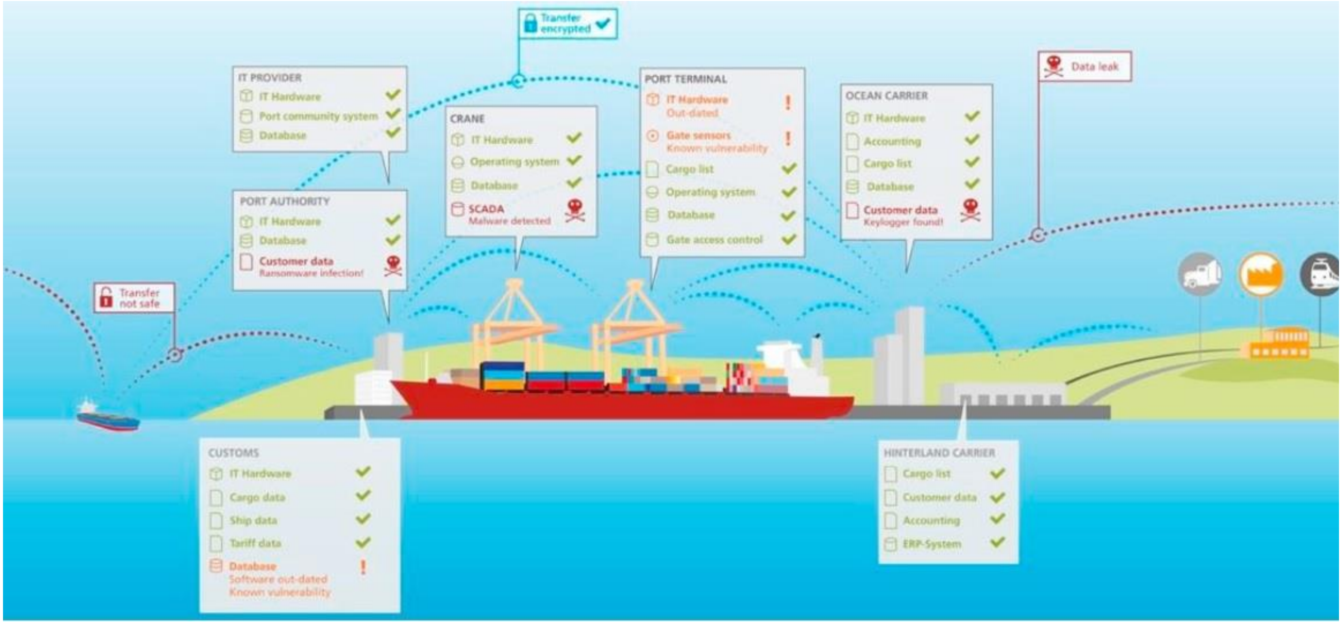
### OVERVIEW

1. The maritime industry is responsible for transporting and delivering more than 95% of global trade by volume – approximately 11 billion tons annually. As an important part of the global economy, any disruptions can cause shockwaves throughout the economy.

**Case in point:**
**In Mar 2021, the Suez Canal, one of the world's busiest trade routes was blocked by the *Ever Given*, a container ship that had run aground in the canal. The blockage caused significant slowdowns to global trade as it held up an estimated US$60 billion worth of global trade during those six days.**
**Although the grounding was not a result of a cyber-attack, this incident underscores the magnitude of disruption should a cyber incident result in the flow of maritime traffic or port operations**

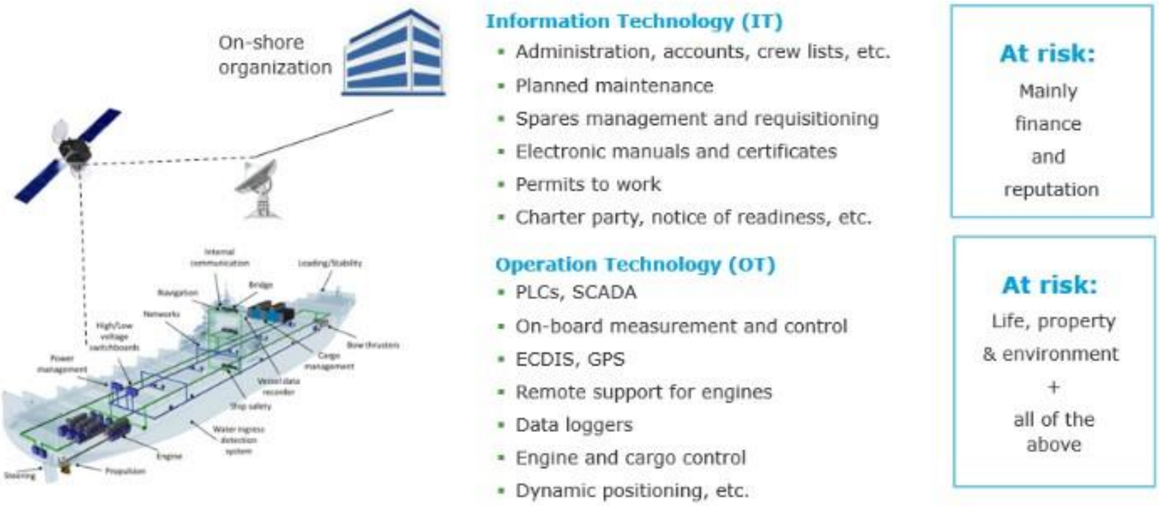
### RISING TIDE OF MARITIME CYBER RISKS

2. The size of the global economy has expanded over the years. Consequently, the maritime industry needs to scale up its operations to match the growing maritime activity. Many nations leverage advancements in technology to enhance efficiency in the maritime trade. Today, the shipping eco-system is highly integrated – from the IT operating systems of the ports and ships, to vessel traffic control, handling of cargo and passengers, transport operators and logistics chain and so on. These systems are also reliant on critical national infrastructures, such as satellites for communication. As the maritime sector becomes more integrated and digitised, the cyber-attack surface area expands which leads to the increase in cyber-attack vectors. The attacker can target any part of the ecosystem – from the ships to the shipyards, ports and shipping companies, as seen below:



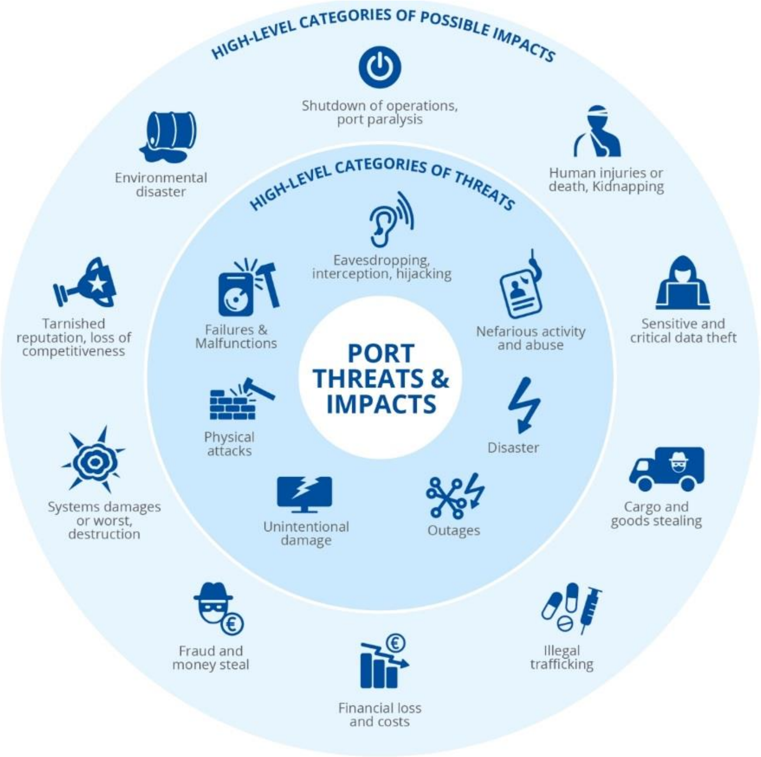
A global image of the possible threats and the spectrum of threats and their various cascading effects that are associated with security incidents. Source: (CyberRoad, 2015).

3. **Ships**: As the global maritime industry embraces smart shipping and becomes more digitised, the information technology (IT) and operational technology (OT) systems onboard ships can become possible cyber-attack vectors. A breach of IT systems can have significant reputation and financial impact while disruption of OT systems may impose significant risk to the safety of onboard personnel, cargo, damage to the marine environment and impede the ship's operation.


On-shore organization
Internal communication
Loading/Stability
Bridge
Navigation
Networks
High/Low voltage switchboards
Bow thrusters
Power management
Cargo management
Vessel data recorder
Ship safety
Water ingress detection system
Engine
Steering
Propulsion
Information Technology (IT)
Administration, accounts, crew lists, etc.
Planned maintenance
Spares management and requisitioning
Electronic manuals and certificates
Permits to work
Charter party, notice of readiness, etc.
At risk:
Mainly finance and reputation
Operation Technology (OT)
PLCs, SCADA
On-board measurement and control
ECDIS, GPS
Remote support for engines
Data loggers
Engine and cargo control
Dynamic positioning, etc.
At risk:
Life, property & environment
+
all of the above

IT/OT Systems onboard a typical ship and associated cyber risks. Source: (DNV, 2023).

4. Ports: Port operations comprises port IT/OT assets, systems, supporting infrastructure and data, which can become attack vectors for malicious cyber threat actors. Port operations are a crucial part of the global supply chain and a cyber-attack can cause supply chain disruptions and financial loss


HIGH-LEVEL CATEGORIES OF POSSIBLE IMPACTS
Shutdown of operations, port paralysis
Human injuries or death, Kidnapping
Sensitive and critical data theft
Cargo and goods stealing
Illegal trafficking
Financial loss and costs
Fraud and money steal
Systems damages or worst, destruction
Tarnished reputation, loss of competitiveness
Environmental disaster
HIGH-LEVEL CATEGORIES OF THREATS
Eavesdropping, interception, hijacking
Nefarious activity and abuse
Disaster
Outages
Unintentional damage
Physical attacks
Failures & Malfunctions
PORT THREATS & IMPACTS

High-level categories of port threats and impacts. Source: (ENISA, 2020).

**Case in point:**
**On 5 Jul 2023, the Port of Nagoya, Japan's biggest maritime and container port, suffered a cyberattack allegedly by Russian threat actors which disrupted cargo packing procedures and forced the suspension of operations at the container terminal. LockBit 3.0, a Russian-based hacker group had demanded a ransom to be paid in exchange for the recovery of the system.**
***"Given that the Port of Nagoya is Japan's busiest port, handling approximately 10% of the country's total trade volume, the effects of this disruption are likely to be far-reaching and could possibly ripple through the global economy. The impact may be especially significant considering the current global supply chain issues already exacerbated by the Covid-19 pandemic."*** **- Craig Jones, Vice President of Security Operations at Ontinue**

5. **Maritime Industry**: Besides ship operations and port operations, the maritime industry encompasses activities like shipbuilding, repair and maintenance, and marine engineering. It is a complex eco-system with many interdependencies consisting of both public and private organisations with various networked systems. A weak cybersecurity link in this ecosystem can cause problems that can affect the global supply chain.

**Case in point:**
**On 27 Jun 2017, Maersk, one of the world's biggest shipping companies suffered a cyberattack caused by the "NotPetya" ransomware, losing most of its data, with 49,000 laptops and 4,000 servers destroyed. For three days, all tracking and logistics operations were offline, causing major shipping delays.**
**Although Maersk rebuilt their entire IT infrastructure in 10 days, they incurred losses of over US$200 million and suffered reputational damage due to the extensive media coverage on the attack.**

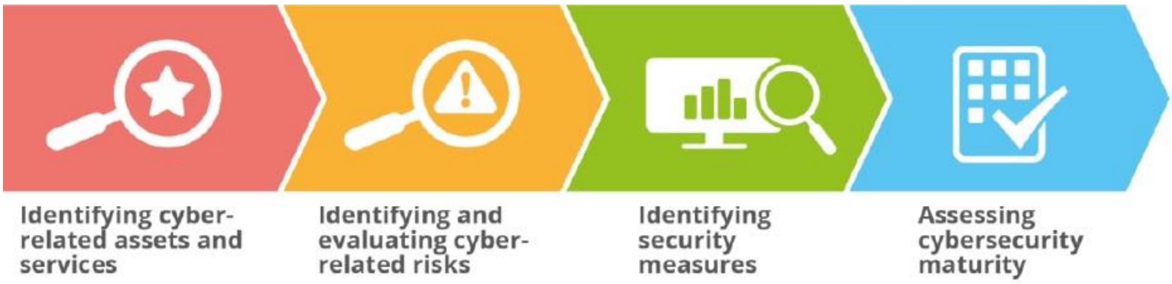
6. According to the Maritime Cyber Priority 2023 published by DNV, more than six in 10 industry professionals expect cyber-attacks to cause ship collisions (60%) and groundings (68%) within the next few years. More than three-quarters (76%) believe a cyber incident is likely to force the closure of a strategic waterway.

***"All four of the largest shipping companies, Maersk, COSCO, MSC and CMA CGM have been victims of cyberattacks in recent years." – According to Allianz***

## CYBER RISK MANAGEMENT GUIDELINES

7. While the ecosystem of the maritime industry is unique, the application of cyber risk management is universal and below is a four-phase approach for managing cyber risk that can be used on any framework or methodology that the system owner wish to adopt:

a. Phase 1: Identifying cyber-related assets and services
b. Phase 2: Identifying and evaluating cyber-related risks
c. Phase 3: Identifying security measures
c. Phase 4: Assessing cybersecurity maturity


Identifying cyber-related assets and services
Identifying and evaluating cyber-related risks
Identifying security measures
Assessing cybersecurity maturity

Cyber risk management phases. Source: (ENISA, 2020).

## BEST PRACTICES FOR MARITIME CYBER RISK MANAGEMENT

8. In response to the rising maritime cyber risks, maritime organisations such as the International Maritime Organisation (IMO), the Baltic and Maritime Council (BIMCO), Cruise Lines International Association and International Chamber of Shipping (ICS) published technical guidelines for maritime cybersecurity. The IMO has stressed that "the goal of maritime cyber risk management is to support safe and secure shipping which is operational resilience against cyber risks.".

9. Some of the best practices for implementation of cyber risk management for the maritime industry as referenced from IMO's Maritime Safety Committee Guidelines (MSC-FAL.1/Circ.3) include:

a. Update the safety and environment protection policy to include reference to the risk posed by unmitigated cyber risks.

b. Using existing company procedures, identify any training which may be required to support the incorporation of cyber risk management

c. Assess all identified risks to ships, personnel and the environment and establish appropriate safeguards.

d. Update procedures, plans and instructions for key shipboard operations concerning the safety of the personnel, ship and protection of the Operational Technology (OT) environment.

e. Update emergency plans to include responses to cyber incidents.

f. Update procedures for reporting non-conformities, accidents and hazardous situations to include reports relating to cyber incidents.

g. Update procedures for implementing corrective actions to include cyber incidents and measures to prevent recurrence.

h. Include creation and maintenance of back-ups into the ship’s operational maintenance routine.

## CONCLUSION

10. Cyber-attacks on the maritime industry can have significant impact to global trade, maritime traffic and even the environment, leading to significant financial losses and even potentially loss of human lives. Hence, it is crucial that the maritime sector take immediate steps to enhance their cyber risk management measures.

# Contact Details

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE, at ACICE@defence.gov.sg.

Prepared by:
**ADMM Cybersecurity and Information Centre of Excellence**

••••

# REFERENCES

## News Articles

1. Why Is The Maritime Industry So Important? - Chiltern Maritime
[Link: https://www.chilternmaritime.com/why-is-the-maritime-industry-so-important/#:]

2. Maritime cybersecurity attacks on the rise – MarPoint
[Link: https://marpoint.gr/blog/maritime-cybersecurity-attacks-on-the-rise/]

3. Maritime cyber security – DNV
[Link: https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/index.html]

4. Shipping industry expects cyber-attack deaths and collisions
[Link: https://www.seatrade-maritime.com/technology/shipping-industry-expects-cyber-attack-deaths-collisions-and-groundings]

5. Maritime Cyber Security: A Comprehensive Approach
[Link: https://www.missionsecure.com/maritime-security-perspectives-for-a-comprehensive-approach]

6. The Guidelines on Cyber Security Onboard Ships
[Link: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships]

7. Why is Cyber Security so important to Mariners? – MITAGS
[Link: https://www.mitags.org/why-is-cyber-security-so-important-to-mariners/]

8. Cybersecurity in the Maritime Sector: ENISA Releases New Guidelines for Navigating Cyber Risk — ENISA
[Link: https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-maritime-sector-enisa-releases-new-guidelines-for-navigating-cyber-risk]