Cyber security in the Maritime industry
The threat landscape
Navigating headwinds of threat

By 2028, the global maritime satellite communication market is expected to reach $8.77 billion, driven by a rising demand for broadband connections, connectivity, cloud and IoT applications across the maritime sector.

Greater connectivity coupled with increased reliance on digitisation, integration, automation and network-based systems was highlighted by the International Maritime Organization (IMO) five years ago.

Concurrently, maritime cyber attacks had reportedly increased by 900%.2

An increase in connectivity and in cyber attacks sets a bleak tone for the sector, where...

The average time it takes to identify a cyber attack in a ship’s system is 140 days3

Reported cyber attacks on the maritime environment are up by 68%4

A single cyber attack on the major Asia-Pacific ports could cost $110 billion5

Only 55% of organisations offer regular cyber security safety training6

---

Cyber security vulnerabilities

In this landscape of rising risk, which cyber security vulnerabilities must the maritime sector address?

Phishing

Connectivity at sea has rocketed with offshore data usage among shipping container companies, for example, increasing by 108\%\(^7\).

Seen through a cyber security lens, growth in internet usage increases the risk of a phishing attack or data breach.

One crewmember tricked to take the bait hidden in a work email could trigger a ransomware attack.

For example

**DNV**

**DNV’s ShipManager** software suffered a large-scale, disruptive cyber attack in January 2023. Some 1,000 vessels were impacted by the ransomware attack, which saw ShipManager defend itself by immediately shutting down its IT servers.

**Port of Lisbon**

In January 2023, the **Port of Lisbon** suffered a ransomware attack that took down its website and internal computer systems\(^8\).

Financial reports, audits, budgets, contracts, cargo information, ship logs, and port documentation were reportedly stolen in the attack.

The hacking group LockBit claimed responsibility for the incident and demanded a $1.5 million ransom.

**IT supply chain risk**

In 2021, several Greek shipping companies were hit when ransomware spread through the systems of an IT consulting firm\(^9\). External customers of Danaos Management Consultants had their files encrypted by the ransomware attack.

The cyber attack caused communication disruptions between companies and their ships and suppliers, and some files with correspondence were lost.

\(^7\) Inmarsat, ‘Surge in maritime data usage as shipping industry seeks increased connectivity,’ August 2022.

\(^8\) Bleeping Computer, ‘LockBit ransomware claims attack on Port of Lisbon in Portugal,’ December 2022.

\(^9\) Maritime Executive, ‘Cyberattack hits multiple Greek shipping firms,’ November 2021.
Cyber security awareness

The International Chamber of Shipping (ICS) continues to stress the critical importance of cyber security threat awareness and secure working practices in maritime.

Training and awareness within the maritime sector should be tailored, they recommend, to appropriate levels for onboard personnel, including master, officers and crew, and shoreside personnel, who support the management, loading and operation of the ship.

Vulnerabilities at sea

While maritime companies are using more data at sea, they are also transforming how they operate. Maritime IoT, ship digitalisation and maritime digital applications may offer cyber threat actors new attack vectors to access ships’ IT systems.

Organisations must raise awareness of the vulnerability to attack of their vessels’ onboard systems, including:

- Automatic Identification System (AIS)
- Cargo handling and management systems
- Communication systems
- Internet of Things (IoT) devices
- Electronic Chart Display and Information System (ECDIS)
- Engine room systems
- Global Positioning System (GPS)
- Navigation systems

Spotlight on IoT

In the current threat environment, security vulnerabilities must be addressed when vessels:

- Use legacy systems and equipment that may not be compatible with newer IoT devices
- Implement inadequate security measures in their IoT devices
- Have a large number of IoT devices, which can be difficult to manage and secure

How TSC can help

At TSC, we are experts in security training and behavioural change. We can support you to address the threats you face in the current cyber security landscape, and help you reduce the human error risk.

If you would like more information about how The Security Company can help, please contact us via: enquiries@thesecuritycompany.com or call on 01234 708456.

Cyber risk in the maritime sector: don’t let it sink your reputation.