**USD 10 TRILLION**

**PREDICTED COSTS FROM CYBER CRIME BY 2025**

# MARITIME CYBER

The cost of cyber attacks worldwide is startling, with global costs from cyber crime predicted to exceed USD 10 trillion by 2025. Although shipping remains a small part of this total, cyber attacks in the maritime industry are becoming increasingly costly. Recent data shows that a cyber attack now costs the targeted organisation an average of USD 550,000.

This is not a new threat, the International Maritime Organization (IMO) recognised this and in January 2021 mandated the integration of cyber risk management into a company's Safety Management System (SMS). This need for cyber risk management was further clarified by 'Guidelines on Maritime Cyber Risk Management', with the latest version published by the IMO in June 2022.

Technological advances are progressing rapidly. Achieving the potential gains in efficiency, operations, and safety requires a high degree of connectivity between ships and external services. The challenge lies in protecting ships, without restricting the benefits a connected ship brings.

## INFORMATION TECHNOLOGY AND OPERATIONAL TECHNOLOGY

The use of computerised systems on board a ship can effectively be split into two separate functions, Information Technology (IT) and Operational Technology (OT).

IT can be considered the typical office functions that take place on board ships; this may include the email communication and data reporting/sharing that companies use. As this technology has a longer history and experience of being connected to external sources and transmitting data, cyber security safeguards are better understood, and personnel are more alert to the associated hazards.

OT, on the other hand, is what controls many of the ships systems, such as the main engine control, or dynamic positioning. This equipment was traditionally considered safer due to the lack of external connectivity; however, this is rapidly changing and can provide an entry point for malicious activity. As the threat has become clearer and the potential for safety, environmental, and economic damage better understood, the demand for clear defensive actions have grown. As the cyber threat frequently innovates and adapts, there are no prescriptive procedures that will provide sufficient security. Therefore, it is necessary for those involved in shipping to develop cyber resilience.

**THE THREAT OF MALICIOUS CYBER ATTACKS POSES AN ONGOING AND INCREASING RISK** TO SHIPS AND THE SHORE-BASED SYSTEMS THAT SUPPORT THEM.

## INTERNATIONAL ASSOCIATION OF CLASSIFICATION SOCIETIES UNIFIED REQUIREMENTS (IACS)

The IACS has produced two Unified Requirements (UR) that will be implemented on all ships contracted for construction on or after 1 July 2024. While mandatory for new ships, the content of these UR's provides useful information and guidance for protecting ships currently in service.

UR E26 Rev1 provides requirements for a ship to be considered cyber resilient. Along with more information, it details the functional aspects that must be addressed for adequate cyber security. The five functional elements, and some considerations include:

### IDENTIFY

This involves identifying the vulnerabilities in the ship's systems. It means having detailed inventories of all computer equipment, operating systems, software, etc. Clear plans should show the location of all equipment, including any interconnections between systems. A robust management of change procedure should be established to keep systems up to date, whilst preventing any disruption.

### PROTECT

Establish fixed boundaries between critical networks to allow zero or minimal permitted traffic between these individual 'zones'. Access to networks must be limited to authorised personnel only. User accounts should be established using the 'least privilege' principle and should be deactivated once they are no longer required. Where possible, protective software should be installed to monitor and prevent unwanted interaction. Remote access must be capable of being controlled from the ship, with any failed attempts to remotely access the ships networks automatically logged.



# RESILIENCE

**ANTHONY GARDNER** LOSS PREVENTION MANAGER, BRITANNIA P&I

### DETECT

Continuous monitoring should take place for suspicious activity, such as excessive data traffic or attempted connections to networks. An alarm should be generated upon detecting suspicious activity, noting that the alarm should not result in any disruption to essential functions.

### RESPOND

A response plan should be prepared, detailing the actions required to minimise the impact of any incident and limit the damage caused. The plan should be available in hard copy and should specify the information required by on board staff, such as reporting, response options and the major consequences from loss of system functions. Systems should automatically revert to a safe condition if a cyber incident is detected.

### RECOVER

A recovery plan should be available, with clear instructions on how to return the affected systems to their full operational state, whilst minimising disruption. The plan should list the personnel responsible for certain actions, including how to request specialised external support. Systems should have a facility to revert to an earlier, uncorrupted state, following a controlled shutdown.

For all the above, any inventories, procedures, drawings, and plans should be kept up to date for the entire life of the ship. UR E27 Rev1 provides the minimum technical capabilities that systems and equipment must have to be considered cyber resilient. This provides third party equipment suppliers with clarity on the standards required to meet the approved level. Although primarily for equipment makers, it also provides certainty to shipowners when purchasing systems and equipment for their ships.

Cyber security will continue to demand vigilance from all stakeholders. This will require continuing investment in both the training of personnel and in the selection of equipment and systems used in shipping.

**FOR FURTHER INFORMATION**

**Please do not hesitate to contact the Loss Prevention Team at: lossprevention@tindallriley.com**