News 01 Aug, 2022

Are shipowners covered against likely cyber-attacks?

When it comes to cyber-attacks, shipowners should assume the worst and expect to be hit at some point.

Bill Egerton
Chief Cyber Officer (Astaara)

These concerns are backed by a report from March 2022 showing that shipping companies pay an average US$3.1 million in cybersecurity ransom payments per incident due to gaps in their risk management. Attacks on the maritime industry range from phishing and ransomware to targeting infrastructure or ship systems for financial or political reasons.

More than half of shipowners spend less than $100,000 a year on cybersecurity management, which the organisations behind the report – maritime consultancy firm Thetius, law firm HFW and shipping cybersecurity company CyberOwl – believe isn't enough.

Additionally, around two-thirds of respondents aren't sure whether their insurance covers cyber-attacks. Other eye-raising results show that only 55% of industry suppliers are asked by shipowners to prove they have cyber-risk management procedures in place, while 25% of seafarers don't know what's expected of them if involved in a cyber incident.

The big worry is that shipping companies haven't invested enough time or money to shore up their defences, leaving them exposed to attack and short of meeting IMO 2021, the International Maritime Organization's requirements for cyber-risk management.

Cyber-attacks and vessel safety

Failing to establish safeguards against any cyber risks to vessels, personnel and the marine environment can prove damaging to shipping companies from an operational perspective.

The rapid pace of maritime digitalisation provides shipowners huge benefits in terms of improved efficiency, safety and asset tracking. Such technology has been around for some time and is now an established part of vessel operation.

One example can be found in navigation. Paper charts have long been replaced with digital alternatives on most vessels, to the point where traditional navigation techniques are rarely, if ever, practised by seafarers. Today, some shipowners have gone further and implemented shore-based dynamic route management, to fully optimise vessel efficiency and safety.

A cyber-attack on one of these onboard systems could have dramatic implications on vessel safety. If navigation controls are altered, or charts deleted, it can become very difficult for a crew to safely operate a vessel. The impact could be even more dramatic for digital systems connected to engines or ballast pumps.

Since January 2021, cyber threats have been included in the ISM Code's risk management protocols. Under the updated protocol, cyber risks must now feature in a vessel's Safety Management Systems.

This reform means that shipowners must identify and create an inventory for their critical technology and data assets (both hardware and software, IT and operational technology) on board their vessels and linked to their onshore systems. They should also assess the cyber risks to those assets and establish specific risk-mitigation measures to manage and guard against any threats. Additionally, any cyber-security policies must ensure that crewmembers receive the appropriate training to understand the threats, and that the roles and responsibilities for addressing those risks are clearly defined.

A properly formulated Safety Management System should cover worst-case measures to ensure that a vessel and its crew remain safe should a system fail, which may include hard-copy back-ups or manual overrides. It should also include regular audits to ensure new risks are identified, and a commitment to continuous improvement.

It is important that shipowners work proactively to ensure that their Safety Management Systems are fully up to date and fit for purpose, yet it can be a complex task. Such systems are inherently technical, and an owner may need outside support to properly evaluate and understand vulnerabilities.

West's Loss Prevention department can provide vessel and issue specific guidance and support in improving Safety Management Systems – both to meet regulations and to improve the safety of a vessel. Our expert team is ready to give practical advice to any Member, and can help ensure a vessel stays safe and P&I cover remains valid.

Major commercial risks

Vessel safety is not the only cyber risk shipowners face. Phishing attacks, where cyber-criminals posing as legitimate institutions send individuals or companies emails to obtain sensitive information, are perhaps the biggest concern for most owners.

Cyber whaling, a particularly dangerous variation of phishing, is becoming more common. In these attacks, emails target a group of senior executives or digital gatekeepers using personal vocabulary and information to trick them into cooperating. Messages are usually from fake email accounts that look almost identical to a genuine sender's address.

The criminals behind cyber whaling aim to socially engineer their victims, to trick them into making financial transfers or sharing confidential material. Anyone duped into doing either usually has no idea until it's too late – which would be incredibly disruptive to shipowners' shore-side and sea-based operations.

An attacker could gain access to the organisation's computer system, forcing the shipowner to take the entire office function offline. In this instance, the company would have to painstakingly organise hundreds of paper, rather than electronic, records and forms.

The ramifications can extend to ships, with vessels stuck at ports or unable to secure bunkers. Payment, logistics and planning systems could be completely decimated, while compliance paperwork may force some owners to temporarily cease some trades.

How to plan for cyber-attacks

Some of the principles inherent in the ISM Code can guide a shipowner across other parts of their business. IT and digital teams should regularly identify and conduct an audit of all potential cyber threats, while staff need training to spot the warning signs and understand the systems in place for blocking hackers.

Staff within the organisation should never share any personal information in an open, online public forum. For example, an attacker could verify an employee's identity by using their birthday, after sourcing that information from the victim's LinkedIn profile.

Given that even the best defences can be breached, owners should also plan to mitigate the impact of any successful attack. This may include maintaining back-up systems and servers where appropriate to keep office functions online if under attack.

It is also important to protect against worst-case scenarios through proper, specialist insurance. Where cyber risks onboard a vessel are covered by P&I, other commercial risks are not – and must be insured separately.

West is proud to have partnered with Astaara, the only specialist marine cyber insurer in the market. Astaara can cover a client's entire business, including shoreside operations, and provides unique business interruption cover on a tailored basis.

Astaara also offers marine cyber-risk management consultancy services, working with clients to measure and improve their cyber-risk profile through a five-stage process. By building a comprehensive picture of an organisation's cyber enterprise risk management and increasing resilience, they can dramatically improve security. The process also covers business continuity planning to ensure rapid recovery should an event occur.

Ultimately, shipowners are responsible for building and maintaining strong defences to deter or prevent cyber incidents. Building resilience is critical, both for vessels and backroom functions. Yet, even the most secure systems are vulnerable – and shipowners must work closely with insurers, including their P&I insurer, to ensure business continuity if the worst were to happen.

Astaara's website

More information on Cyber security cover can be found via Astaara's website.

Visit here →