beazley

Article

A clear and present risk to operations and assets

Kelly Malynn • November 29, 2023

Kelly Malynn, Product Leader & UW Cyber Phys Dam Marine & Emerging Strat Lead

Maritime businesses are exposed to the same enterprise cyber risks which every business sector now has to grapple with. They are threatened with data breaches, ransomware and wiperware attacks by cybercriminals who are constantly evolving their modes of attack and their targets. While there is nothing to suggest that cyber criminals are zeroing in on the marine sector, they are no less exposed than their counterparts in other industries to these land-based enterprise risks.

Operational Technology (OT) on board a vessel is possibly a less attractive target, or less well known to financially motivated cyber threat actors, however with a significant amount of Information Technology (IT) on board and increasing connectivity availability and demand, what does this mean to the risks to vessels and business operations? Public examples of such events are currently limited. However, this does not mean the risk does not exist, or that there won't be a direct attack of this type.

Suggesting that mariners will not be targeted or that their defences will be impenetrable seems overly optimistic. The industry itself is not bullish. According to our Risk & Resilience research 30% of businesses, globally, in the transportation, cargo and logistics sector feel unprepared for the threat posed to their businesses from cyber risks.[1] So, the answer has to be that it has to be inevitable that at some point shipping companies will fall victim to a cyber incident that affects how one or more of their vessels operate. If this is the case, then why is appropriate insurance penetration so low? With a palpable threat and growing concern, why has the translation towards increased risk transfer been so slow? The answer to this is less straightforward.

Perfect storm

In recent years the maritime sector has undergone a vast transformation. It has digitised its processes and become highly sophisticated in its use of technology. With this relentless pace of digitisation, exposure to cyber risks increases. Initiatives to improve supply chains and efficiencies also increase reliance on technologies. But addressing the accompanying cyber risks has been playing second fiddle to more pressing threats to their businesses' viability.

As a sector, maritime organisations have been continually buffeted by a seemingly endless series of global crises and headwinds. Initially, it was the requirement to reduce sulphur omissions, one of the largest changes to environmental regulations in the shipping industry for decades. These new rules to reduce the sulphur content of marine bunker fuels came into force at the start of January 2020, and represent the greatest reduction in the sulphur content of a transportation fuel that has ever been undertaken at one time[2]. No mean feat. However, it has required intense focus from the industry.

Cyber was due to be front and centre with the International Maritime Organisation's Cyber Risks Management Guidelines coming into effect from January 2021.[3] Then came COVID-19. Still grappling with its new environmental requirements, the marine industry faced a decline in global trade greater than that of the financial crash of 2008[4] - port closures, stranded crew precipitated an overhaul of supply chains globally. Meanwhile, the industry focused on crew welfare and finding solutions to keep global commerce moving.

As the industry adapted and the impact of the pandemic subsided, the cyber threat would likely have been front and centre of maritime businesses' risk agendas, but attention was diverted by targets on carbon emissions and the Russian invasion of Ukraine and the resulting sanctions, which have challenged risk managers across the global marine industry.

Beefing up physical cyber risk

Despite a seemingly endless cycle of near-existential threats, the maritime sector is not ignoring cyber risks, and mariners are evolving their defences. Our Risk & Resilience research identified 31% of the transportation, cargo and logistics businesses we surveyed (compared to 37% of all other industries) are planning to invest further in cyber security. And, nearly one in four (39%) of these businesses surveyed plan to explore the insurance options available, compared to 35% across other industry sectors.[5]

The fact that mariners are seeking to invest more in insurance is welcome news, and the insurance industry can do much to assist the increasing standards across the marine sector when it comes to 'enterprise cyber' risk and loss or use of physical assets. Appropriate cover for assets, loss of hire, equipment damage, and vessel physical damage from a cyber-attack remains largely non-existent or inappropriate.

While the likelihood of a vessel being hacked and the marine company losing all control is still largely the stuff of poor movie sequels (apologies to any Speed 2 fans!). The potential for an attack or third

party error which causes damage to a vessel, Floating Production Storage and Offloading (FPSO) or terminal is remote, but, it exists.

It is, however, the risk of seemingly more minor incidents which should be focusing minds. For example, the potential impact of a phishing email leading to malware affecting a ship's bridge systems or ballast. An update from a trusted service provider that contains an error impacting navigation capabilities or availability even slightly can have significant consequences on the ship's ability to operate, delays and system replacement costs.

Typically, it only takes one incident to have a knock-on effect on cyber insurance buying patterns across an entire sector or industry. However, for the marine sector, given the stakes, waiting to see the potential consequences of an attack is a risky option due to the ever-evolving threat landscape. It is not the worst-case scenario that maritime organisations should be concerned about, but the more run of the mill financially motivated cyber events and third party error or breach risks that should be on their risk radars and insurance budgets. The maturity of the enterprise cyber market can provide effective risk transfer to the maritime industry for typical insured cyber risks. However, the balance of exposures is different, with the additional operational exposures including asset availability requiring mature capacity that understands the risks and can manage claims and assist with live incident management.

Glossary

Data breaches - a data breach is a security incident in which unauthorised parties gain access to sensitive data or confidential information, including personal data (Social Security numbers, bank account numbers, healthcare data) or corporate data (customer data records, intellectual property, financial information).

Ransomware - is a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files. A criminal group will then demand a ransom in exchange for decryption.

Wiperware - Malware intended to erase ("wipe") the hard drive or other static memory on the computer it infects deleting data and programmes.

Enterprise Cyber Risks – Cyber risks to an organisation including:

- Cyber extortion loss
- Data recovery loss
- Business interruption and dependent business interruption resulting from security breaches and system failures
- Data and network liability
- Third party liability including regulatory defence and penalties
- eCrime

Kelly Malynn

Senior Risk Manager

[1] Risk & Resilience research - Methodology - Cyber/Tech report 2023 | beazley

[2] https://www.digitalrefining.com/article/1002503/imo-2020-meeting-the-challenge

[3] MSC-FAL.1-Circ.3-Rev.1.pdf (imo.org)

[4] https://www.nature.com/articles/s41598-021-97461-7

[5] Risk & Resilience research

beazley