Maritime Cyber Risk report: Shipping industry remains “easy target”, pays average US$3.2m in cyberattacks

October 17, 2023

New research has found that the maritime industry remains an "easy target" for cybercriminals and that the cost of attacks and demand for ransom payments across the sector have skyrocketed over the past 12 months.

The report, which was produced by global, sector-focused law firm HFW and maritime cyber security company CyberOwl, reveals that the average cyberattack in the maritime industry now ends up costing the target organisation US$550,000 – up from US$182,000 in 2022.

It also shows that demands for ransom have increased by more than 350%, with the average ransom payment now US$3.2 million – up from US$3.1 million last year.

The report is based on a survey of more than 150 industry professionals – including C-suite leaders, cyber security experts, seafarers, shoreside managers, and suppliers – and reveals significant gaps in cyber risk management that exist across shipping organisations and the wider supply chain, despite progress made by IMO 2021.

The research was carried out by the maritime technology research agency Thetius.

Key findings include:

1. The financial cost of a maritime cyberattack can be extreme:

- they now end up costing the target organisation US$550,000 on average (an increase of 200% from 2022)
- ransom demands have increased by more than 350% over the past 12 months, with the average ransom payment now US$3.2 million (up from US$3.1 million in 2022)
- 24% of the victims of cyberattacks were tricked into transferring funds to criminal organisations

2. Despite these eye-watering costs, most shipping organisations significantly under-invest in cyber security management:

- a third spend less than US$100,000 per year
- 25% of survey respondents said their organisation does not have insurance to cover cyber risk

3. Although overall levels of preparedness seem to be improving:

- 80% of survey respondents understand what actions would be required of them in the event of a cyber security incident (up from 74% in 2022)
- 64% said their organisation has cyber risk management procedures for dealing with suppliers (up from 55% in 2022)

"Our findings show that while maritime cyber security has improved, the industry remains an easy target. Shipping organisations are being subject to more cyberattacks than ever before, and the cost of attacks and demand for ransom payments have skyrocketed. And as the use of technology continues to increase across all aspects of shipping – from ship networks to offshore installations and shoreside control centres – so does the potential for cybersecurity breaches," stated Tom Walters, partner, HFW.

He further added, "Maritime operational technology and fleet operations management are now almost entirely digital, meaning that a cyberattack could compromise anything from vessel communication systems and navigation suites to the systems managing ballast water, cargo management, and engine monitoring and control. Failure of any of those systems could result in a vessel being stranded and potentially grounded, and we saw from the *Ever Given* the impact that can have on global supply chains. This is a critical issue for all parties involved in the shipping sector, and it's clear that the industry has to do more to protect itself against cyberattacks."

"The good news is that the conversation on vessel cyber risk management has clearly shifted away from the 'why' towards the 'how'. There is less scepticism about the need to manage the risk, more thoughtfulness on how best to spend each dollar in shoring up defences," noted Daniel Ng, CEO, of CyberOwl.

Daniel Ng added, "The challenge for the change agents in shipping is that they are dealing with new risks in a new domain under sector-specific constraints. All of this is in an environment where shipping companies are still too secretive to share benchmarks and best practices widely. The sector must make the most of the specialist expertise available. And those with specialist maritime cyber security knowledge must do more to share knowledge of risks and best practices."

"Our research shows that the industry has improved dramatically in a short space of time. But it also shows that cybercriminals are evolving faster. The costs of cyber-attacks are growing. The impact that can be created in the global supply chain by exploiting a single easy target means the entire maritime industry needs to raise the bar," explained Nick Chubb, managing director, of Thetius.