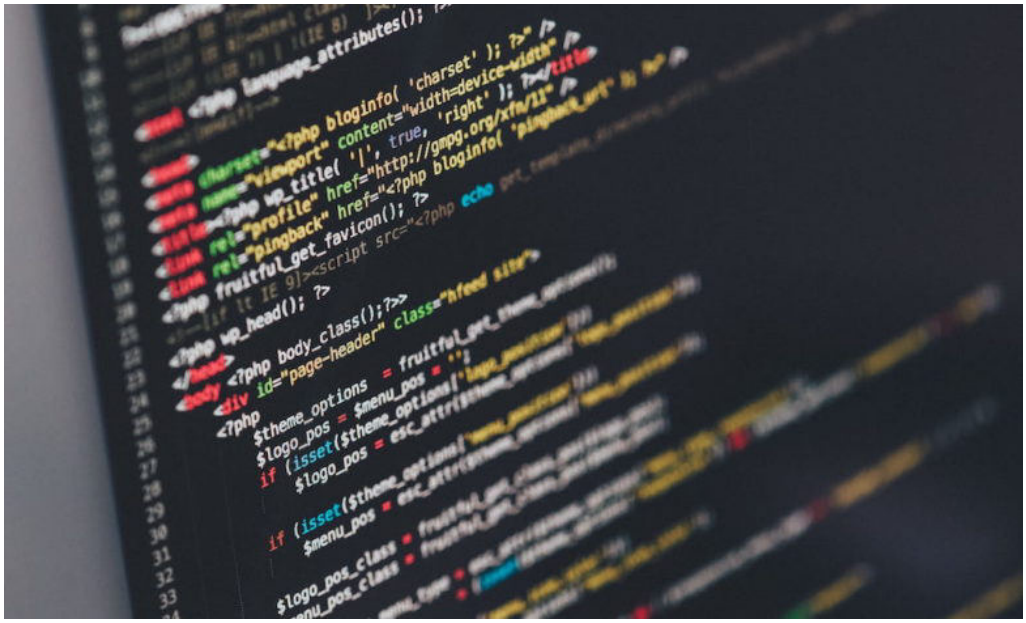
Operations Tech

Cyber ransom payments have ‘skyrocketed’ over the past 12 months

Sam Chambers • October 17, 2023 0 333 2 minutes read



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 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 $550,000 – up from $182,000 in 2022.

It also shows that demands for ransom have increased by more than 350%, with the average ransom payment now $3.2m – up from $3.1m 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. The research was carried out by the maritime technology research agency Thetius.

Key findings in the 59-page study include the statistic that 24% of the victims of cyberattacks were tricked into transferring funds to criminal organisations while 25% of survey respondents said their organisation does not have insurance to cover cyber risk.

Tom Walters, a partner at HFW, commented: “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.”

Daniel Ng, CEO of CyberOwl, wrote in an introduction to the report: “Shipping is an exciting yet relatively easy target for cyber hackers who are looking for a quick thrill with the potential for big ransom payments.”

Reviewing cyber incidents of vessel systems that have occurred so far in 2023, analysis by the CyberOwl team concludes that a typical fleet of 30 cargo vessels experiences an average of seven cyber incidents a month, or over 80 incidents a year. Whilst the majority of these incidents are low impact, the larger issue is the time it takes to resolve them. The average cyber incident on a vessel system took 57 days to resolve.

Other startling statistics contained in the report include If global cybercrime was a nation state, it would be the third largest economy in the world after the US and China.

Shipping might struggle to attract the right candidates to count the cyber threat, the study suggested.

Cyber practitioners are expensive and the cyber security job market is booming with an unemployment rate of less than 1%. This means that in reality, shipping would have to pay top dollar to secure these professionals.

Maritime cyber security presents different challenges to managing enterprise IT cyber risk, the report makes clear. One example is

practitioners often have to deal with legacy and “mandrolic” systems onboard vessels. In addition, putting in place restrictive cyber security controls, such as strict login procedures, does not work practically, as shipping operations often require pragmatic flexibility to complete tasks.

#United Kingdom