SEMAPHORE

Newsletter of the Maritime Law

Association of Australia and New Zealand

Cyber-Risk Management Beyond Compliance

Maritime industry proactivity in preventing and mitigating the impact of cyber attacks is being encouraged through the *Beyond Compliance – Cyber Risk Management After IMO 2021* report.

Compiled by maritime innovation consultancy Thetius and published as part of the Inmarsat Research Programme, the report calls for diligence above and beyond the framework provided by the International Maritime Organization (IMO) 2021 cyber risk management code.

Inmarsat maritime president Ben Palmer emphasised that assuring data resilience and cyber security should be “key preoccupations” for the shipping industry.

“The IMO guidelines on maritime cyber risk management have helped stakeholders to address cyber threats, but the nature of digital attacks continues to evolve due to advances in computing technology and developing geopolitical conflicts,” he said.

“Over the 12 months between May 2020 and May 2021, cyber-attacks targeting the maritime sector increased by 168% in the Asia-Pacific region alone.

“To ensure the resilience of their digital infrastructure, shipping companies need to look beyond regulatory compliance and be more proactive in their approach to cyber-risk management.”

Inmarsat is championing its Fleet Secure UTM (Unified Threat Management) solution as a “cornerstone” to the approach, given it combines firewalls, antivirus programs, content filters, and intrusion and detection systems into a single hardware and software package.

The company also describes its Fleet Secure Cyber Awareness training programme as providing “everything the crew needs to know to be aware of vulnerabilities and suspicious online behaviour”.

“Effective cyber risk management must consider multiple assailants and diverse lines of attack – targeted and random,” stated Inmarsat.

“Threat actors make continuous efforts to update strategies, by developing malicious coding, seeking out vulnerabilities in hardware and software, and by responding to human behaviour. Only by being proactive can shipping stay ahead of the cybercriminals.”

September 2022