Cyber insurance failing to improve security

Marine cyber insurers say problems will be resolved as the industry matures, but getting companies to share data is hard, and companies outside the cyber world do not understand the risks

30 Jun 2021 | **NEWS**

by Declan Bush @Declan_LL | declan.bush@informa.com

A cyber insurance study finds the industry is failing to spur companies to improve their cyber security. Data sharing is poor and high opportunity costs mean cyber insurers are disinclined to cover shipping firms

INSURERS OFFER CUSTOMERS SERVICES SUCH AS STAFF TRAINING, VULNERABILITY SCANNING AND ACCESS TO SECURITY OFFICERS.

Source: Cultura Creative RF / Alamy Stock Photo

CYBER insurance is failing to spur companies to improve security, according to a report by the Royal United Services Institute.

The UK-based security think tank said the emerging industry's impact was so far "more limited than policymakers and businesses might hope" and described insurers' inability to collect and analyse reliable cyber risk data "a potentially insurmountable challenge."

"Interviewees from across government, industry and business consistently stated that the positive effects of cyber insurance on cyber security have yet to fully materialise," it said. "While there are some encouraging

signs, cyber insurance is still struggling to move from theory into practice when it comes to incentivising cyber security."

The report comes amid growing concerns about cyber attacks on shipping and companies' access to marine cyber cover.

The International Maritime Organization has adopted a resolution (IMO 2021) which requires companies to demonstrate that cyber security is an integral part of their safety management system no later than their next annual Document of Compliance check.

But the Royal United Services Institute report said most of the cyber insurance market used "neither carrots (financial incentives) nor sticks (security obligations) to improve the cyber security practices of policyholders".

"Growing losses have also emphasized that the current reality is not sustainable for insurers either," it added.

Cyber insurers faced an uphill battle in convincing mature businesses that they could provide expertise on best practices, the report noted. The effectiveness of cyber security products was also "open to question."

Insurers offered customers services such as staff training, vulnerability scanning, providing threat intelligence, such as monitoring the dark web, and access to security officers.

Reinsurance exclusions limiting cyber cover from P&I clubs

By David Osler and Declan Bush

21 Jun 2021

Steamship sees combined ratio jump to 125% after big payouts to cruise operators in wake of pandemic

Read the full article here ›

Access to attack response teams and crisis and PR managers was one of the main benefits of cyber insurance, the report said.

But it was difficult to measure the effects of these services and several insurers said customers were not using them at scale.

The report also noted concerns that insurance providers unintentionally helped ransom payments, which could be seen to encourage more ransomware attacks.

But it cautioned that the purpose of cyber insurance was to transfer residual risk, not to improve cyber security, and it should "be one of many tools" to better manage risks.

It recommended developing guidance for minimum security standards for underwriting; more data collection and sharing; mandating cyber insurance for government suppliers; and collaboration between insurers and law enforcement on ransomware.

Robert Dorey, chief executive of Astaara, the maritime cyber risk insurer, said shipping differed from other industries in that IMO 2021 embedded cyber security within the ambit of a ship's seaworthiness. He said shipowners or operators that failed to meet it would almost certainly be in breach of their insurance policies.

"Cyber security is a relatively new industry and the fact that the vast majority of incidents go unreported and probably undetected means that there are huge gaps in the risk data," he said. "This will change as cyber becomes more 'mainstream', however companies will need to be incentivised to share this information."

AXIS Insurance senior cyber underwriter Georgie Furness-Smith said demand for insurance was growing alongside understanding of the threat, adding that many insurers now set minimum security requirements prior to incepting a policy.

Thomas Brown, chief executive of cyber insurance policy provider Shoreline, said shipowners often knew more about the daily risks they faced than insurers did — but not in the cyber world.

This means they are not always willing to pay for cover or have been late adopters of cyber insurance, in turn driving insurers toward other, less complex industries.

"Consequently the shipping industry has thus far ceded insufficient premium to the market to cover the known frequency and severity of maritime cyber losses, which have in the main part been assumed by the larger self-insured shipping corporates," he said.

Ethical hacker says ships are wide open to cyber attack

By Declan Bush

27 May 2021

Ethical hacker Weston Hecker detailed the increasing risk to ships' operational technology and how basic carelessness leaves many companies vulnerable

Read the full article here ›

Some of the Royal United Services Institute's recommendations, such as minimum security requirements, partnerships with security firms and reporting of attacks to authorities, were already written into policies, he said, adding that expectations of cyber insurance differed across the industry.

Insurers whose attack losses were mitigated could be more satisfied with it than regulators or port state authorities who hoped cyber insurance would spur better cyber practices.

But he agreed the shipping industry had a poor track record on sharing claims data.

Fear of reputational damage stopped most victims of cyber crime reporting attacks. Ransomware cover tended to be shrouded in confidentiality, since companies known to have cover could make better targets.

Insurers, meanwhile, preferred to safeguard their claims data for their own commercial advantage.

"Whilst national and international regulation continues to be meted out in the form of guidance alone, most shipowners will continue to self-insure their cyber risk, rendering any objective measure of 'expectation' irrelevant for want of reliable data, unfortunately," said Capt Brown.