Getty Images: 5079921

Contingency plans

Insurers are looking to shipowners to prove they have assessed the risk of cyber attacks and have taken steps to prepare for them. Classification societies can help in this

Tanya Blake, *SAS* editor

Shipping companies must improve and strengthen their cyber security system to prevent or limit damage caused by cyber breaches

At a cyber-security conference in London a couple of months ago, a central message emerged from the various talks: shipping must move beyond awareness and take real steps to prepare for potential cyber attacks and breaches. This is vital not only to protect businesses but because insurers may soon ask shipowners to prove they are cyber-prepared.

Speaking at the conference, Adrian Durkin, North P&I Club's director of claims, said that while in 2016 it was commonly said that the shipping industry "needs to start thinking" about cyber security, today there needs to be real evidence that companies have taken action to prevent or limit damage that could occur from a cyber breach.

He added, "Now we can point to products and people who can provide an audit of systems to make a self-assessment. [Companies can] then make programs more resilient and fill as many gaps as possible".

"This has other impacts," said Durkin. "If I'm thinking about what a prudent shipowner should be doing, then a claimant's lawyer will too. If a shipowner is doing nothing, it could be seen as an imprudent owner and a club may not cover it. We would not want to do that but a claimant's lawyer would have no problem doing so. If a shipowner says it did everything it could and the situation had arisen despite being seaworthy, it will say 'show me'. It is not good enough to just have a system. It must also be operated properly."

It is important for shipowners to take active steps to assess cyber preparedness, on the ship and shore, with hardware and software, said Durkin. For its own part, North P&I has partnered with Hudson Analytix, a maritime security company, to offer its members a discounted cyber-risk assessment tool that will aid in assessing preparedness. "This gives a person at operational level the chance to go to senior management and get them to commit time and resource to ensure protection against the threats out there," said Durkin. "We are not expecting perfection but we do expect a level of preparedness and diligence starting to be exercised by shipowners."

He added that he hoped class would take a lead in cyber, so shipowners could test their systems against "something that is internationally regulated. Shipowners can then say, 'our cyber preparedness level is in line with the DNV GL or Lloyd's standard' to give us a benchmark and avoid claims, as lawyers can then test against that benchmark."

Class on cyber

Classification societies are developing cyber guidelines and providing support for shipowners seeking to improve their cyber-security provisions and help identify gaps that need to be closed. Rick Scott, ABS senior technical adviser, told *SAS* that while malicious cyber attacks were a cause for concern, a much greater number of non-malicious cyber incidents were caused by human error, exacerbated by a lack of training and awareness.

To counter this, ABS provides guidance for "standing up" maritime IT and operational technology (OT) programs and assesses existing programs. It has collaborated with Stevens Institute of Technology in New Jersey, the United States, the US Department of Homeland Security, and the US Coast Guard to create a new risk model that makes "maritime OT risk easier to understand, observe, measure, and reduce", Scott explained.

This has led ABS to research and produce what Scott describes as "methods and tools for risk identification, assessment, and reduction". These create a risk management index number for the asset. "This index number is in turn useful for focusing cyber-security activities on specific risk sources and comparing the relative risk associated with individual assets across a fleet of vessels. It centres on proactive management of digital systems and access to those systems."

Meanwhile at DNV GL, Patrick Rossi, maritime cyber security service manager, ISDS approval engineer, and "certified ethical hacker", said his organisation regularly helped shipowners and managers to assess their "cyber-risk situations.

"Different companies have different strategies and are situated on different steps of the maturity curve," said Rossi. Taking this into account, DNV GL trains them in how to assess cyber security risks, as well as how to train others. It also performs vessel risk assessments, penetration testing, and runs cyber drills, which involve "incident handling and 'friendly' phishing attacks to help provide levels of awareness within the organisation".

However, while it is clear that class is supporting shipowners in becoming more cyber-resilient, there is some difficulty in defining exactly what is meant by 'cyber-prepared'. Unfortunately for Durkin, the creation of a class-standard benchmark may be some way off.

Rossi explained that there were different levels of preparedness for crew (training and maintaining cyber hygiene), shipowners (percentage of crew trained, cyber policies and compliance with regulations, and stakeholder interests), and operational teams (analyses of latest risk assessment of a vessel or fleet). DNV GL has guides and training for all three and Rossi revealed it was currently "working with insurance companies and underwriters to help them assess and raise awareness".

Meanwhile, Scott said the "highest level" of being cyber-prepared "means that cyber-security risks have been systematically identified and verifiably managed in a reasonable and prudent manner", but he added that "when we peel back the layers of the term, 'cyber prepared' for insurance and certification purposes, it is not so simple, but it is understandable".

Rossi said, "Cyber-preparedness is quite complicated and can possibly be characterised mathematically by multivariate analysis – but I'm not yet convinced that it can." The variables would include inherent asset risk, organisational awareness of that risk, and organisational risk tolerance, and security protections (technology and processes) in place. Rossi said that ABS was making "some progress" in understanding how to quantify cyber preparedness and it could eventually be possible to create a benchmark, but said it is "not practical" right now.

The particular challenge holding back benchmarking, Rossi stressed, is that it requires an in-depth knowledge of each company's cyber-security solutions to mitigate risk and an understanding of the cost or benefit conditions underpinning each organisation's "risk tolerance calculus". Both of these issues have deep roots in the business priorities of an enterprise and are highly proprietary to each organisation.

Adding to this, the huge variations between each vessel's industrial control systems and the risk landscape varies hugely, as does the kind of protections that are required, and the way in which class could assess the effectiveness and performance of that asset.

Rossi said that developing a single or "small-set solution" for cyber preparedness was not only "extremely challenging" but could hold back progress in improving cyber security in the industry. At this point, ABS will focus on risk awareness and management and possibly a guiding cyber-risk benchmark, although Rossi stressed that it was down to individual organisations to determine which preparedness solution suited it best. ◘

✉ tanya.blake@ihsmarkit.com