Cyber 08 Apr, 2021

Under Attack - Waypoints Feature Article

Cyber exposures and the consequent losses can affect anyone in the maritime community at any time, *write Astaara CEO Robert Dorey and West's Christopher South*

No one is likely to forget 2020 in a hurry. The pandemic had a seismic effect on all our lives and livelihoods, exerted a significant impact on trading and, out of urgent necessity, transformed working practices the world over. The availability of high-speed, high-quality connectivity has been an invaluable asset, enabling organisations to maintain their business continuity.

The corresponding downside has been an alarming escalation in the incidence of cybercrime, and some very high-profile shipping companies have recently borne the brunt of these attacks. Already suffering from the disruption caused by lockdown measures and market volatility, an additional setback was extremely unwelcome and costly for these companies.

The regrettable fact is that the same critical pressure which forced organisations everywhere to rapidly move so many aspects of their operations online conversely represented a golden opportunity for hackers. All four of the most prominent container operating firms fell victim to malware or ransomware attacks within months of each other, in effect compromising almost 60% of the world's container traffic.

Vulnerabilities

These exceptional circumstances only exacerbated a problem which was already growing long before the pandemic took hold – namely, that the maritime industry has been conspicuously slow to fully acknowledge the vulnerabilities that accompany the digital revolution. Companies which view the cyber realm as too complex and nebulous to engage with can often fail to grasp the financial, operational and reputational damage a cyber event can wreak until their own businesses have already been impacted.

Underestimating their own susceptibility, usually through a lack of understanding at management level, is a recurrent issue. Many shipowners assume that since their vessels can operate independently from shoreside teams, then the cyber risk is negligible. However, ships communicate to shore via mobile phones, emails, Zoom calls, etc, and these are all vectors of infiltration into a ship's onboard network.

Such vulnerabilities actually stem from head office; this is where the patching is driven from, where upgrades in IT and technology originate, and where shipowners exchange data with engine manufacturers, fuel suppliers, clients and financiers. Most importantly, it is also where training and education programs are organised. If that side of the equation is poorly managed, there's a fair chance that the vessels won't be optimally managed from a cyber perspective either.

Consistent benchmark

The salutary experiences endured even by the ‘big scalps’ mentioned earlier have sent shockwaves throughout the industry, prompting a significant intensification of threat awareness. In addition, the introduction on January 1 of the 2021 IMO Cyber Security Guidelines [see sidebar] can only have a beneficial influence upon the take-up of effective maritime cyber risk management programs.

Importantly, these guidelines provide a consistent benchmark, a framework within which companies can measure their cyberattack preparedness. No one yet knows how punitively the new rulings will initially be enforced, but setting an example by detaining vessels for insufficient cyber protection might be the most bluntly effective means of getting the message across.

The US Coast Guard has already issued three tiers of detention for cyber deficiencies, by which any vessel arriving in a US port with a malfunctioning critical system will be detained until the issue has been resolved. (For more details, see here) This will inevitably take time, and a detained ship won’t be making any money while it’s off-hire. The resultant lost earnings whilst the vessel is detained would not be recoverable by loss of hire or delay insurance, which usually specifically exclude delays when the detention relates to non-compliance with international or national regulations.

Whilst the Nordic Marine Insurance Plan, for example, advises that a delay caused by a cyber attack could be covered under clause 5.1.B (Hull and Machinery perils) as, de facto, it would stop the ship from operating, this may not be true under other underwriters’ policies. As the vessel is technically damaged, the costs of fixing it would be recoverable less the applicable deductible. However, if the H&M Policy contains a Cl. 380 exclusion clause, computer breakdown due to a cyber attack would not be covered. If the breakdown occurred because of an ordinary bug in a software update, it would be covered regardless of a Cl. 380-style exclusion clause. If the breakdown was covered under the H&M, LoH (Loss of Hire) would respond unless there was also a Cl. 380 exclusion in the LoH policy.

A further complication for insured parties is the LMA 5403 clause, introduced by Lloyds in November 2019. In order to establish whether or not they are covered in the event of a cyber incident, attribution/causation must now be pursued to ascertain whether the incident arose from negligence or deliberate interference by a malicious insider or third party; and, if deliberate, whether this was a state sponsored move or an act of terrorism. We are of the view that the market approach is not constructive and creates uncertainty.

Due diligence

Where the Hague-Visby Rules oblige shipowners to exercise due diligence in making their vessels seaworthy prior to the commencement of any voyage, it is now incumbent upon them to prove that they are also applying cyber due diligence – everything from updating patches and running security checks to making sure passwords aren’t glued under keyboards, ensuring that crews are properly trained in cyber security and aren’t, for example, letting visitors charge their phones through USB ports on the network, and so on.

BIMCO has now also issued a cyber clause for charterparties, which in essence says that not only will parties use their best efforts to prevent cyberattack, but will also make sure that subcontractors do likewise. Liability could be problematic to establish here, particularly for charterers in terms of confirming which standards the parties will be judged against.

Underwriting

From an underwriting perspective, P&I Club mutual policies currently have no cyber exclusions, so if an assured were to have a collision, say, because they'd been hacked and lost control of their ship, they'd still be covered. The exception to this would be where a ship's systems are hacked by terrorists or a belligerent power; such instances would then fall to war risk underwriters, not cyber underwriters – an important distinction.

As mentioned above, Cl. 380 or the more recent market standard cyber exclusion clauses are generally applied to other insurance policies. The assured's options are either to simply "buy out" the exclusion or consult specialist providers like Astaara who can provide a global package cover that is far more comprehensive than alternatives which just reinstate the Cl. 380 or similar exclusions.

The key for all concerned is to plan and proceed methodically. Cyber risk management is about doing the basics well, which doesn't necessarily require a huge investment. By making it a priority, driven by the Board from the top down so that factors such as using multi-factor authentication and ensuring antivirus software is up to date become an ingrained daily habit for all employees, companies will address what might look like minor issues, but which could otherwise have a disproportionately large impact on their business.

The 2021 IMO Cyber Security Guidelines: what you need to know

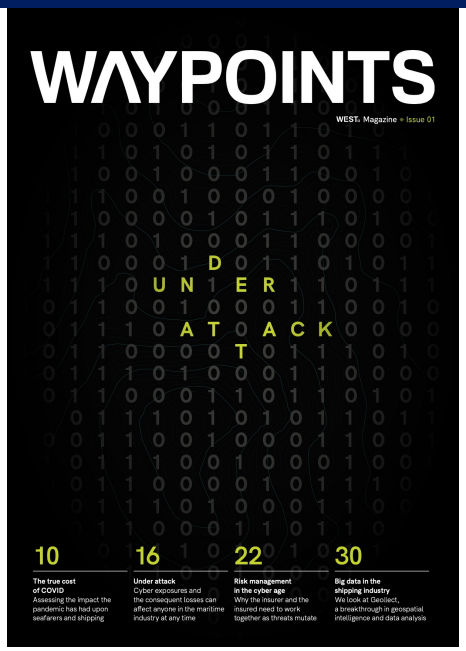
In practice, shipowners will need to demonstrate a full understanding of mandated cyber security protocols by conducting a comprehensive inventory of all at-risk onboard and offshore systems, including IT and OT equipment.

Vessels will then be subject to a cyber risk analysis and evaluation to assess their vulnerability and the mitigation measures which have been or need to be applied on board.

Thereafter, shipowners can implement the cyber risk management program best suited to their vessels and equipment, establishing crisis management strategies and incorporating crew training procedures which clearly demarcate their specific roles and responsibilities.

Based upon the National Institute of Science and Technology cyber framework, the 2021 IMO Cyber Security Guidelines involve five basic steps.

1: Identifying risk
2: Detecting risk
3: Protecting assets
4: Responding to risk
5: Recovering from attacks.



This article was taken from *Waypoints*, Issue 01.

You can read more expert opinion on industry developments with West P&I Waypoints Magazine.