Cyber insurance mitigating risk

Lawyer **Nic van der Reyden** recently addressed a Melbourne Shipping Australia breakfast on maritime cybersecurity, mitigating risk and cybersecurity. This article is based upon his presentation

Cyber threats and risks are increasing, and will continue to do so as technology keeps advancing. Cyberattacks cause business disruption, loss of sensitive information and damage to a company's corporate reputation. Transport and logistics businesses have specific vulnerabilities given their interlinked roles in the supply chain, which make it all the more important for them to defend their operations.

WHY IS THE MARITIME INDUSTRY VULNERABLE?

The interconnectedness of supply-chain players is a key factor. Moving goods across borders involves not only exporters and importers, but port operators, customs, forwarders, port agents, container yard operators, hauliers, biosecurity services, surveyors, warehouses and distributors.

Then there is the matter of under-resourced supply chain participants: the large number of small-to-medium-sized enterprises networked in the supply chain are insufficiently resourced to use

the latest security patches, or have not upgraded their antivirus protection, or have not undertaken adequate staff training. The value of goods and the business interruption implications of the supply chain being broken or stopped are many times a multiple of the cost of the services being provided and/or the earnings of the individual SME participants.

Potential consequences of a cyberattack:

- financial costs, including loss of revenue, drop in share price and remedial costs;
- loss of IP and confidential information both to organisation and of third parties;
- business disruption;
- reputational and brand damages; and
- operational and infrastructure impact.

There is a clear incentive for a hacker to try and attack the logistics industry with its high-value assets, passenger data and the movement of expensive cargoes. The broad consensus from the maritime industry seems to be that approaches to cybersecurity should be company and ship-specific, albeit guided by national legislation and industry guidelines. Companies will be required to take a proactive approach in assessing the risks, taking into consideration the public guidance on addressing and managing cybersecurity.

There is a clear incentive for a hacker to try and attack the shipping/logistics industry with its high-value assets, passenger data and the movement of expensive cargoes.

Cyber-risk insurance policies are structured to remedy the inadequacies of traditional insurance by dealing with cyber risks specifically and broadly. Insurance should be part of a cyber-risk management strategy. As with any commercial insurance product, a typical underwriter – in determining whether to offer cover, and if so, on what terms – will want to know what risk management systems the prospective insured has in place.

WHAT SHOULD BUSINESSES DO?

Businesses should review their current policy to see whether some or all cyber risks are covered under their transitional property, all risk or liability policies. The insurance industry has responded to the growing risks and costs that are faced by businesses as a result of cyber breaches and attacks. The industry has developed specific cyber liability or network security and privacy insurance to cover these new and evolving risks. Companies need to know what risks you are faced with and what they want covered; what risks can be satisfactorily addressed, mitigated or managed; and what are the remaining or residual risks.

EXCLUSION CLAUSES

Exclusion clauses are the big issue in many cyber insurance policies. Because the risks that are being protected against are often difficult to predict and are in new and inherently complex areas, insurers go to some lengths to exclude risks. Most insurance policy covering ships, shipyards and cargo-handling facilities include some kind of clause excluding liability for cyberattacks. This usually says that any losses caused by the use of or operations, as a means for inflicting harm, of any computer, computer system, malicious code or virus are outside the terms of cover.

Some of the most common exclusions and exemptions generally are:

- failure by the company to ensure employees and contractors are aware of security issues and the risks their behaviours can create for company and customer data;
- failure by the company to maintain an adequate regime to ensure basic security controls are current and are consistent with best practice; and
- failure to disclose pre-existing risks that have been revealed in vulnerability assessments or penetration testing exercises but have not been fully or effectively rectified.

GOOD CYBER HYGIENE

While insurance can help, coverage will be impacted unless self-help and prudent self-management can be demonstrated. To reduce the costs of a cyber incident, companies should progressively improve their systems and training. Staff awareness and training are key to avoidable cyber threats. Employees, crew, passengers and suppliers must be made aware of, and understand, the potential cybersecurity risks and the policies and procedures that are put in place to manage those risks, including what to do in the event of a breach. Some 50% of cyber breaches come from within an organisation through deliberate or inadvertent acts or omissions of employees.

Measures to promote cyber hygiene include:

- IT policies dealing with use of technology, access, password and login protocols, information security, internet usage, email usage, social media and networking tools, and remote access;
- data security, storage and breach policies;
- privacy policies including notification requirements;
- third party management policies;
- what an employee should do if he or she suspects a security breach, or if there is an actual breach; and
- how to recognise risk.

Nic van der Reyden, partner, HFW

NEED FOR A ROBUST CYBERSECURITY FRAMEWORK

Organisations should have a robust cybersecurity framework in place to identify the information to be protected, protect the information and ensure the company is able to detect, respond and recover from a data breach.

Companies should ensure the cybersecurity strategy is tailored to the risk faced by the organisation, its critical assets, and the third-party vendors that are relied upon. It is important to take into account the likely types of digital, physical and social security risks to the organisation, including worst-case scenarios in terms of costs, downtime, and damage. Companies should be undertaking a thorough assessment of the equipment, software and processes of the entire infrastructure, including IT resources, data storage and architecture, physical perimeter security, social and media activities, industry specific concerns. Companies should update anti-virus software, firewalls and other software and ensure security policies respond to new threats and developments.

The Office of the Australian Information Commissioner, ASIC and APRA have each published guides on data breaches and cyber-risk that contain a wealth of information about the risks posed to organisations and steps that may be taken to manage risk. ■

PROJECT CARGO AND MARINE RISK

Captain Joseph Alphonse, Marine warranty surveyor, AlmarcoMaritime

■ Captain Alphonse spoke to the Melbourne Marine Insurance Forum recently, addressing key themes including the role of the marine warranty surveyor, the challenges of project cargo and the management of critical items.

PROJECT CARGO

Regarding project cargo, Captain Alphonse explained how the remoteness of many construction sites presented challenges and the risk of damage to equipment throwing entire projects under potential jeopardy.

"A large portion of the equipment on large projects comes from outside of Australia, essentially due to cost. To bring it to Australia, for example, you have got to be wary of the constraints and limitations from the marine point of view of the environment as well as from the site itself.

"Australia is a large country and some of these places where the projects are located are quite remote," he said.

"Sometimes they don't even have proper infrastructure in place to actually manage the equipment's coming in. In some cases, they actually have to start from scratch in building the required infrastructures first."

CRITICAL ITEMS

Captain Alphonse explained that, because of the long lead times that may be required in getting a replacement, "marine warranty risk management" comes into play in mitigating the impact to a project if "critical items" incurred damage in transit.

Marine warranty operates under an independent marine risk management framework that conducts technical reviews and approves operations or movements of equipment from the planning stage right up to its final execution. This process provides the required safeguard against damage to critical items on a project.

A "critical item" is something of high value that requires special consideration in terms of how it can be transported in a safe and timely manner. It's usually defined explicitly in the marine covers and acts as a trigger for the marine warranty clause requirements.

"For example, on some projects, if you were to have a total loss of a key piece of customised equipment – you can't just go and get another replacement the next day," he said.

"Some of the lead times for key equipment can range between six months up to two years to build one from scratch. Any loss of one or more of key equipment during its transportation phase would obviously have an impact on the scheduled commencement date of the plant, which in turn would have an impact on the project financiers and owners."

That is why, Captain Alphonse explained, there is usually a marine cover that applies for the marine cargo and another that also provides cover on the projected revenues that is anticipated from the scheduled commencement date – delay in start-up cover (DSU cover).

"It provides some risk management protection to financiers and project owners, with respect to delays to the commencement of operations, if some damage occurred to critical equipment"

TYPICAL QUESTIONS

In managing the risks associated with marine operations or critical items, the marine warranty surveyor will typically ask for a range of information.

Questions typically will relate to such areas as methods of packaging, the type of vessels involved, a ship's performance history, sailing routes, contingency plans for dealing with piracy and plans for compliance with local, national and international laws and IMO codes among other areas.

"There are various areas that we will be looking at in terms of assessing the risks associated with transportation of a critical item," Captain Alphonse said.

"As part of marine warranty works, when the assessment is done on various plans and procedures with respect to marine transportation, the marine warranty surveyor will see whether there are any blind spots or grey areas.

"We will examine as to whether there are any particular areas where the risk has not been properly mitigated and whether there may be some unanswered questions with the methodology used or on some of the concepts proposed."

Captain Alphonse explained that marine warranty surveyors engage in many risk management discussions aimed at identifying hazards and risks.

"Amongst others, we would conduct peer reviews and brain-storming sessions on whether we have actually thought through the process properly or not," he said.

By David Sexton

HPW, Almarco Maritime