CYBER-RISK & INSURABILITY

Cyber-risk in marine transportation

Cyber-attacks represent one of the most significant threats facing international businesses today, and are increasing in severity. For the insurance industry, such risk represents a highly significant opportunity. Yet while many insurance companies, particularly in the UK, currently offer such products, others have shown reluctance given the risks involved.

In this article, Petra Wildemann in FTI Consulting's Insurance practice takes a look at why cyber-risk products must be very carefully considered and, using the marine transportation industry as an example, the opportunities and challenges posed by cyber-security.

Recent cyber-risk victims

2011 *Drug smugglers gain remote access to Port of Antwerp's terminal systems*

2012 *Criminal syndicate penetrates cargo systems operated by Australian Customs and Border Protection*

2013 *World Fuel Services falls victim to an online bunkering scam costing an estimated $18m*

– Source: CyberKeel, Oct 2014

A new risk category

The proliferation of digital technologies and the expansion and complexity of our IT and data systems means that the risk to business from cyber-attacks are increasing every day. 'Cyber-risk', as defined by The Institute of Risk Management, is 'the risk of financial loss, disruption or damage to the reputation of an organisation due to any sort of failure of its information technology systems.'

It was once thought that such risk was confined entirely to certain sectors, such as technology providers, defence contractors and financial services companies. However the evolution of cyber-risk means that every organisation is now under threat. It is therefore essential for these risks to be carefully measured, analysed and insured.

The transport sector is all too aware of the threat from cyber-attack and the associated business risks. For example, open Wi-Fi networks used by passengers during flights and ship journeys, is a significant area of weakness, and could have profound insurance implications. We know that passengers have already taken over the operation of onboard computers from inside the plane. In June 2015, Warsaw airport was the victim of a cyber-attack after hackers shut down its

flight plan computers, and the following month, hackers were able to gain control of a Jeep Cherokee SUV via the internet in an experiment for Wired magazine. This led to the company announcing it will update its software to protect its vehicles from such attacks.

Barring effective counter-measures, such incidents could start to occur more frequently, as airlines move to 100% reliance on computer systems.

Significance to marine transportation

This problem is of crucial significance in the marine transportation industry. Over 90% of international trade is estimated to be based on sea transport, so the safety of shipping vessels is critical to the global economy. Yet these vessels are highly dependent on e-Navigation, and cargo (and of course lives) can be lost, damaged or destroyed, by cyber-attacks. Yet the low levels of cyber-security awareness and training in this industry, especially from those on board, can make it an easy target for hackers, especially if they are working together with pirates.

The shipping industry has always factored risk into its daily business activities having sought to offset the risks posed by natural disasters, regulatory changes, and piracy and technology changes. So it is strange that it should now look the other way when faced with this new type of risk. Cyber-security may not be the first item on the agenda of ship owners and shipping companies, but as the risks mount, it can no longer avoid this problem.

Most modern cyber-attacks seek to inflict damage to the vessels, cargo and the shipping operations by taking over industrial control systems which control operations such as navigation and propulsion, cargo handling, inventories and container tracking systems. It isn't too hard for example, to imagine the devastating economic impact across the entire world if a ship passing through the Panama Canal was attacked, resulting in the blockage of the channel.

There are a number of factors at work which are opening the doors to cyber-hackers and criminals. Companies are increasingly focused on cutting costs, which has reduced not only the number of crew members, but also their depth of training. Ships are reliant more and more on technology, automation and electronic navigation, although this compromises their secure environment. Furthermore, the industry's main safety focus remains on the structural security of the cargo, the vessels and crewmen.

Yet according to Steven Jones, Maritime Director of SAMI, there is "a dawning realisation in the maritime industry" that cyber-crime is an issue which must be addressed, as it becomes increasingly dependent on electronic systems such as electronic charts. The Safety of Life at Sea Convention from the International Maritime Organisation has set out a requirement that all ships must have Electronic Chart Display & Information Systems by 2018. However, if these systems are not installed properly or isolated from the rest of the ship's IT systems by a firewall, they could be subject to hacking, and potentially divert the ship off course.

This is a prime example of how the maritime industry must ensure it carefully considers cyber-security when implementing new technology.

> *There are already standards for the installation of equipment aboard ships, but the question is whether or not they are observed. Whether the standard is complied with on board the ship is dependent not necessarily on the company that built the system but on the company that did the installation.*
>
> *– David Patraiko, Director of Projects at the Nautical Institute*

The challenge for insurers

The increasing threats of cyber-security demands a new way of thinking by insurers and those calculating the risks, pricing models and potential coverage available to clients.

This is because cyber-attacks, especially in the marine transportation industry, can lead to many different kinds of risks, including systems failure, cargo loss (either in port or at sea), or piracy. While those risks have always existed of course, the effect of a cyber-attack, whether resulting in these problems or anything else, represent a whole new category of risk, one which has not been evaluated and measured. Thus insurance companies need to revise and extend their models accordingly.

Given cyber-risk makes up a fairly new risk category, it poses a major challenge to reinsurers who attempt to give guidance on pricing and potential coverage for their clients.

> *Given the worldwide nature of our cyber exposure, we take into account factors such as sector of the insured, systems they use that may be a target, vendors they use that may pose an aggregation risk and the potential of virus or malware to affect multiple companies.*
>
> *– Geoff White, Underwriting Manager, Cyber, Technology and Media at Barbi*

Potential scenarios need to be developed to include data breaches on board, at the terminals or even at ports where interfaces with containers and confidential data can result in significant business interruption costs, notwithstanding liability or reputational losses.

Summary

Ultimately, the more we use technology the more vulnerable we become. The marine transportation industry is just one of the industries grappling with this difficulty, and how it can effectively protect itself from criminal threat whilst harnessing the undoubted opportunities offered by technological innovation.

For the insurance industry's part, the question is how it ensures it can effectively insure against these risks and the new models it needs to develop in order to do so.

We stand at the beginning of a long and difficult path, one which is paved with a great deal of uncertainty. The insurance industry must carefully consider how it can overcome these challenges and respond fully to the new cyber-world.

Petra Wildemann
Managing Director
+41 (76)322 5716
+44 (0)20 3727 1759
petra.wildemann@fticonsulting.com

Jerry McArthur
Senior Managing Director
+44 (0)20 3727 1356
jerry.mcarthur@fticonsulting.com

Jo Franklin
Marketing Manager
+44 (0)20 3727 1762
jo.franklin@fticonsulting.com