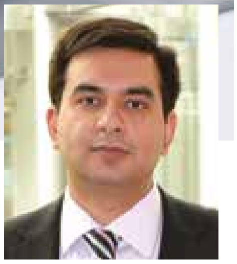

THE INTERNET OF THINGS

PIRACY AND INCREASED MARITIME CYBER EXPOSURE

Capt. Rahul Khanna, Global Head of Marine Risk Consulting,
Allianz Global Corporate & Specialty, London, UK

Pirates infiltrate a shipping company's systems to identify ships with valuable cargoes and minimal onboard security. The vessel is hijacked and only the containers with valuable cargoes are taken. Pirates hand-pick their shipping targets online by tracking the navigation of a vessel through an Automatic Identification System (AIS).

Smugglers hack into networked systems to locate containers with drug contraband and cleanly confiscate the drugs without detection. They attempt to delete the data for the entire shipment to avoid a trail. Hackers infiltrate an energy company's systems and tilt an oil rig, shutting it down. They also penetrate the networked computing systems on another rig with malware. Trained personnel take almost three weeks to clear the system.

THE SCOPE OF CYBER RISK

With the emergence of big data and increasingly interconnected technologies, a revolution of efficiency and speed is overtaking the shipping and logistics industry. As always, with improvement comes considerable risk, one of the most worrisome of which is the growing threat of cyber-attack.

Most experts agree maritime cyber incidents are a real threat and will continue to intensify over the next five years. Proving it is quite another thing, as incidences are vastly underreported. Companies opt to deal with breaches internally for fear of worrying stakeholders. When reports of attacks do surface, details are vague, making it difficult to gauge the headway the industry has made in strengthening online security.

To make matters worse, in addition to exposures caused by technology running ahead of the industry's structural readiness to fully assimilate it, pirates, like those in the above example, have begun abusing holes in cybersecurity to target specific types of cargo.

Pirates appear to have access to refineries and are able to find out who is carrying the fuel they want. Then they just need to look at the AIS information for the ship, go alongside it, overpower the crew and take over the ship, disable communications, siphon off the cargo and leave the ship adrift. It has been reported that some ships switch off their AIS systems when passing through waters where pirates are known to operate, or fake the data to make it seem they're somewhere else. Taking necessary measures to beef up network and telecommunications security is a priority.

CYBER-RISK EDUCATION

From the perspective of risk consultants, insurers, legal authorities and other industry safety veterans, cyber is not a traditional maritime threat like weather and traffic. There is no historical framework from which to operate or recommend action. The shipping industry must work closely with IT vendors – who have more experience recognising and remedying firewall breaches when they are attempted – so they can begin to track and quantify them. The influx of information coming in and going on is difficult to trace.

Many ships no longer carry a dedicated radio operator onboard and therefore shipboard cybersecurity can become a secondary or tertiary concern – an extra and often overlooked duty to be performed by the crew. Everything starts from shoreside operations. The ship's crew plays an important role, however, shoreside operations needs to be proactive; when they are talking with the crew they should ask them what steps they take to protect the ship? Do they understand the extent of cyber-threat? They should provide feedback on the crew's overall performance.

Also, shipping companies must have the same robust firewalls and security systems as their ships, even at the most remote local offices as much as at corporate headquarters. It only takes one instance to get behind the firewall and hackers then have access to the company's operations, even to the shipboard operating systems in some cases.

Other security risks can result from improper integration of cyber-systems, as well, such as the unaccounted and unintended consequences of system updates and the interactions between the cyber-systems of ships and ports. Ongoing implementation of electronic navigation is also a potential conduit for cyber incidents. The cyber impact cannot be overstated; it goes hand in hand with electronic navigation – the simple fact is that you cannot hack a sextant.

Shipping companies must recognise the overall global aspect of the "Internet of Things" and understand that they need to carry out controls across all lines within their network.

REGULATORY ACTIONS

Of all of the defensive efforts to thwart cyber-attacks, one of the most important is a united front among all shipping companies; their vessels and their governments must confront the problem head-on.

Maritime organisations recognise the importance of guidelines to inform and protect increasingly vulnerable shippers, as the risk continues to evolve far beyond a loss of data. Cybersecurity is high on the agenda of the IMO. Its Maritime Safety Committee (MSC) will take up the topic at its next meeting later this year, urging member states and international organisations to "collaborate on proposals for guidance on maritime cybersecurity".

Acknowledging the threat to safety, environment, hull, machinery and surveying, the International Association of Classification Societies (IACS) has created a cyber-system safety framework in support of the ongoing IMO work.

FUTURE CYBER-RISK OUTLOOK

Shipping is still a long way from where it needs to be in terms of protection and security. While we as insurers can try to raise awareness and provide insurance solutions, generally the risk is not well understood and the consequences can be disastrous. All cyber-related incidents will continue to be a problem as long as they are relatively easy to engineer and remain under the radar. One of the best deterrents is active participation in the safety of vessels by ship-owners and crew, themselves. More awareness training is needed for the crew and the tendency to cost-cut by reducing crew numbers should be avoided.

The greatest step any company can take to reduce losses aboard vessels is to improve the crew retention. That is crucial. Ship operators have to realise that their most valuable asset is the crew which mans the vessel and ultimately protects it. If we don't give to the crew proper recognition and support, then we are going to face a greater shortage than we already have. People are as important to the equation as either the flow of data or the flood of new technology that is sure to keep coming at the industry.

While the likelihood of a cyber event that cuts off a significant portion of world trade is low, exposure is growing. More in-depth analysis needs to be conducted into how to improve systems and people. The potential rise of cyber piracy is just another example of how this risk can quickly evolve. The industry may only have a few years to prepare for the risk of a cyber-related hull and machinery loss.

ABOUT THE AUTHOR

Captain Khanna joined Allianz in 2011 and was previously a Senior Risk Consultant at Allianz Global Corporate & Specialty in London within the Marine line of business. Out of his 21 years of operational and risk management experience in the shipping and marine industry Khanna spent 14 years at sea as captain on tankers and bulk carriers.

ABOUT THE ORGANISATION

Allianz Global Corporate & Specialty is the Allianz centre of expertise for global business insurance and large corporate and specialty risks. With a worldwide network in more than 160 countries, we are one of the very few global insurers with an exclusive focus on the needs of global corporate and specialty clients.

ENQUIRIES

https://www.allianz.com/en/