Insuring cyber risk

DIGITALISATION Shipping is a constantly evolving industry and with technology developing at a rapid rate the maritime industry is no stranger to a raft of worldwide trends such as globalisation, digitalisation, increased interconnectivity, and automation. These global innovations are having a significant impact on the marine insurance sector, going well beyond traditional underwriting expertise, writes Lars Lange, secretary-general at the International Union of Marine Insurance (IUMI).

The move to increased digitalisation in ships and logistics means that there is now a heavy reliance on high levels of data flow which is exposing the industry to potential cyber attacks. With vessels continuing to increase in size, the idea of hackers breaching the systems of a VLCC, capesize bulker or 20,000-TEU container ship is now a real possibility and the results could be catastrophic. Loss of life, personal injury, pollution, damage to property, business interruption, production downtime, loss of data and reputational damage are just some of the ways insurance providers could be affected by a successful cyber attack.

As marine insurers, IUMI's role is to protect its clients against the "perils of the sea". The recent 'Petya' ransomware attack on shipping giant A.P. Moller-Maersk is just one example of the impact and damage that can be caused. This major strike on Maersk's core business IT systems affected its computer servers across Europe and India at the end of June – and weeks after the initial attack, the company was still recovering.

Maersk is one of the biggest shipping companies in the world with a fleet of more than 600 vessels. Unquestionably, its cyber security measures were top-level but even so, its systems were still compromised. So how can marine insurers and underwriters assist the maritime industry to protect itself more effectively against this emerging risk?

IUMI is investing in educating and informing its members on key trade issues by taking an active role in industry initiatives aimed at enhancing safety at sea. It is using its accumulated knowledge and expertise through partnerships with a variety of other organisations to ensure accurate risk assessment of cyber issues and to identify and implement best practice solutions.

As an active member of the joint industry working group spearheaded by BIMCO, IUMI is part of the group that has recently published a second edition of "The Guidelines on Cyber Security Onboard Ships" (see box). This new version includes information on insurance issues, as well as a new subchapter examining a shipowner's insurance coverage following a cyber incident. This is an important part of the risk assessment which shipowners should now take into consideration.

Within these Guidelines it is stated that the term "cyber", when related to insurance, spans a variety of definitions and scenarios and it is important to distinguish between them to understand fully how the insurance cover is affected. Significantly, insurers generally understand that there is no systemic risk to ships arising from a cyber incident and that the impact of an incident is expected to be confined to a single ship.

Other members of this industry working group included Cruise Lines International Association (CLIA), International Chamber of Shipping (ICS), International Association of Dry Cargo Shipowners (Intercargo), International Association of Independent Tanker Owners (Intertanko), and Oil Companies International Marine Forum (OCIMF).

On this issue, IUMI is also working closely with the classification societies as marine underwriters rely strongly on the judgement of class about a ship's condition and quality, as well as design approvals. Underwriters and class have always enjoyed a close collaboration, particularly in enhancing the safety of shipping in general.

The International Association of Classification Societies (IACS) introduced a cyber panel in 2015. In addition, IACS formed a "Joint Working Group on Cyber Systems" with industry stakeholders supporting the cyber panel in its work. IUMI was invited to participate in this working group. The initiative was created to enhance the Association's ability to address cyber safety concerns while supporting the protection of human life, property and the marine environment. A new bilateral body has also been created recently – the IACS IUMI Technical Cooperation Group – where issues such as cyber safety and the future of autonomous shipping are discussed, giving even stronger collaboration between classification societies and marine insurers.

Alongside all of this, we are also engaged in the transparent lobbying of the cyber risk threat. At the International Maritime Organization's (IMO) Maritime Safety Committee (MSC) 98 Meeting in June, it was considered that cyber risk management onboard ships should become part of the ISM Code. Accordingly, it would be part of the ship's mandatory Safety Management System.

Currently, IUMI members have to rely on a shipowner's voluntary efforts to perform a proper risk assessment (based on the rules and guidelines developed by industry associations). But it is anticipated that this new IMO initiative will deliver a much better risk assessment, as long as the industry's interests in appropriate risk assessment procedures are duly taken into account. The BIMCO Guidelines of Cyber Security Onboard Ships have also been aligned with the IMO's recommendations.

Cyber risk also represents new business opportunities for marine insurers. The emerging risk has created new demand for intelligent and innovative insurance products tailored specifically for individual clients. Similarly, the entire concept of digitalisation is a positive step for the shipping industry as it allows for more efficient and cost-

effective operations, as well as increasing safety at sea.

IUMI members are keeping abreast of this fast-moving issue and are already working on insuring cyber. A number of its member associations, such as Gesamtverband der Deutschen Versicherungswirtschaft eV (GDV – the German insurance association), already have unbinding recommendations for general insurance conditions for cyber risks in place. IUMI's involvement with these industry initiatives is to prepare marine underwriters more effectively by giving them knowledge and expertise to deal with this emerging risk which, after all, has to become "insurable".

There is certainly a mixed response within the market on how best to insure cyber. Some marine insurers, for example, want to address the accumulation risk that automatically comes with a cyber attack and which is likely to have much wider ramifications. What can be said for sure is that each situation must be assessed individually and policies tailored to the client's specific needs.

Marine insurers are service providers and collectively with other industry organisations are working together to address this issue. From an underwriter's perspective, the job is to identify and quantify the risk and then offer an insurance solution that is comprehensive and offers good value-for-money.

› UPDATED CYBER SECURITY GUIDELINES NOW AVAILABLE

A joint industry group headed by BIMCO has released the second edition of The Guidelines on Cyber Security Onboard Ships. The latest edition, available to download free of charge, incorporates additional information on insurance issues, the effective segregation of networks, practical advice on communications and managing the ship-to-shore interface, and ensuring safe systems during port calls.

The industry group has expanded with two new members – the Oil Companies International Marine Forum (OCIMF) and the International Union of Marine Insurance (IUMI). They join the existing group which, besides BIMCO, consists of the Cruise Lines International Association (CLIA), the International Chamber of Shipping, Intercargo and Intertanko.

The second edition has been aligned with the recommendations given in the International Maritime Organization's Guidelines on cyber risk management which were adopted in June 2017. The chapters on 'Contingency Planning' and 'Responding to and Recovering from Cyber Incidents' have been re-written to reflect the fact that the guidelines are aimed specifically at ships and the remote conditions prevailing if a ship's defences have been breached.

Importantly, the subchapter on insurance looks at coverage after a cyber incident. This is a priority for ship operators because cyber risks and possible resulting damage are not necessarily covered in either hull and machinery, or P&I insurance policies. This has become an important risk assessment priority, therefore.

Angus Frew, BIMCO secretary general and CEO, commented: "Cyber security is certainly a hot topic for all of us now, and this latest guidance includes valuable information, applying a risk-based approach to all of the areas of concern, highlighting how an individual's unwitting actions might expose their organisation. In the light of recent events, we urge everyone across the industry to download it – it's available free of charge – and to consider the risk cyber crime may pose to their ships and operations. Ignorance is no longer an option, as we are all rapidly realising."

The Guidelines on Cyber Security Onboard Ships can be downloaded at http://bit/ly/2tmwGZ3