Maritime Cyber Attack – A Clear and Present Danger

By Nick Gooding FCII, IUMI Alternate Officer at the IMO

Abstract from Nick Gooding's speech, presented at the Insurance Sweden Conference on the 6th May 2015, in Stockholm

Cyber risk is the most talked about topic in the insurance industry worldwide and is becoming an increasingly significant threat to the shipping industry. It is no surprise considering the real threat level to the business community and to nation state infrastructure. No one is immune from cyber threat and there are many attacks daily. The International Union of Marine Insurance (IUMI) understands that the risks of a maritime cyber security attack represent a challenge to underwriters for two key reasons. First, there is a challenge to properly understand the exposures and secondly the underwriters' products need to be tailored to meet their clients' needs.

To gain a better understanding of the implications of a cyber-attack on the wider maritime community, it is important to look at a paper issued by Canada to the International Maritime Organization entitled "*Ensuring Security in and Facilitating International Trade*". The paper recommends the development of voluntary guidelines on cybersecurity practices to protect and enhance the resilience of cyber systems supporting the operations of ports, vessels, marine facilities and other elements of the maritime transportation system. Cyber security is defined as measures taken to protect cyber systems or any data contained therein against unauthorized access or alteration.

Here are a number of examples of cyber security breaches with relevance to the maritime industry.

1) Researchers from the University of Texas demonstrated in 2013 that it is possible to change a vessel's direction by interfering with its GPS signal to cause the onboard navigation systems to falsely interpret a vessel's position and heading.
2) A hacker caused a floating oil platform located off the coast of Africa to tilt to one side thus forcing it temporarily to shut down.
3) Hackers infiltrated cyber systems in a port to locate specific containers loaded with illegal drugs and remove them from the port undetected.
4) Somali pirates employed hackers to infiltrate a shipping company's cyber systems to identify vessels passing through the Gulf of Aden with valuable cargoes and minimal on-board security which, directly, led to the hi-jacking of a vessel.

Studies by the Brookings Institution and the European Union Agency for Network and Information Security both concluded that there is very little awareness of cyber security issues in the maritime transportation sector and few initiatives underway to enhance cyber security.

As the global maritime community moves further into a digital environment, ports, vessels and facilities are increasingly connected to and dependent on cyber systems. This includes almost every facet of their operations, such as financial and human resources management, security systems, navigation, communications and the operation of key systems and equipment.

Insufficiently robust cyber security practices could lead to loss of life, increased criminality in the maritime sector, and given the importance of the maritime sector to international trade and supply chains, an operational disruption with significant adverse economic consequences.

All of this is very alarming but it is encouraging to note that through the combined efforts of the International Chamber of Shipping, BIMCO, INTERTANKO, and INTERCARGO there is ongoing work to develop guidelines on cyber security on board ships. Draft guidelines are in place and it is hoped the final guidelines will be presented to the International Maritime Organization for consideration in 2016.

The draft guidelines have been split into nine individual headings covering:

1) Awareness and education for all stakeholders
2) Establishing a generic risk-based framework drawing on existing standards and guidelines augmented by current intelligence and best practice.
3) Addressing the integrity, confidentiality and availability of cyber systems
4) Establishing clear guidelines on the management of key information in order to retain operational cyber capability
5) Looking at how to integrate elements of both physical and software security to ensure safety and business continuity.
6) Acknowledging the importance of identifying and mitigating third party interfaces that could compromise cyber security.
7) Investigating cyber security monitoring systems and network management
8) The development of contingency plans
9) Continued review and assessment of cyber systems to ensure their continued robustness.

This work on the guidelines is very necessary and should be seen against the background of e-navigation, which is an IMO project. In simple terms, it looking for commonality of all IT systems that control shipping from on board, ship to shore, external navigation, coast guard and search and rescue.

So where does this leave marine underwriters who are asked to cover this danger? I think at an individual risk level it is possible to offer cover, but my fear, which I believe is shared by the Franchise Performance Management department at Lloyd’s, is about managing the aggregation of cyber exposed risk and understanding where that aggregation will come from. Furthermore I believe that underwriters should follow closely the work being done by the industry and be robust in their requests for appropriate information from clients as to their risk management of the cyber threat to their business. In addressing the threat, the protection against the malicious insider should also be taken into account as should the threat from hostile use of social media. Marine underwriters also need to consider geographical areas as potential flashpoints such as the Straits of Hormuz, the Suez Canal and the Panama Canal.

The London Market Committees are all working on this issue, and it is on the list of current issues for the IUMI Political Forum – only time will show how we will be able to fight this clear and present danger.