MARSH

Global Marine Practice

JULY 2014

THE RISK OF CYBER-ATTACK TO THE MARITIME SECTOR

CONTENT:

INTRODUCTION

Until about 2010, the majority of cyber-attacks were driven by an attempt to obtain personal or financially sensitive data. Today, the nature of the threat is changing, and companies across all business sectors have begun to experience highly sophisticated and complex attacks that attempt to inflict damage to property and operations by seeking to take control of industrial control systems.

These systems use data received from remote stations to control processes either automatically or via an operator's commands, and are designed to be closed to the outside world. Highly skilled hackers have demonstrated the ability to penetrate the systems used by the maritime industry, with potentially disastrous consequences.

Vessel navigation and propulsion systems, cargo handling and container tracking systems at ports and on board ships, and shipyard inventories and automated processes, are all controlled using software that is fundamental to smooth-running operations. If, for example, a cyber-attack disabled a vessel transiting the Panama Canal resulting in blockage of the channel, it would have significant economic impact around the globe. Cyber-attacks can also have criminal motivations (as seen in Antwerp between 2011 and 2013) to highjack, divert, or steal cargo. Events over the last four years suggest that these types of systems are growing increasingly vulnerable to attack.

Today, companies have begun to experience highly sophisticated and complex attacks that attempt to inflict damage to property and operations by seeking to take control of a company's industrial control systems (ICS).

WHY NOW?

While there have been relatively few reports of successful cyber-attacks on either shipping or on shore-based facilities, they are not unknown, and comparable industries have suffered attacks that suggest, at the very least, that the maritime sector may be vulnerable.

PORT OF ANTWERP

Hackers working with a drug smuggling gang infiltrated the computerized cargo tracking system of the Port of Antwerp to identify the shipping containers in which consignments of drugs had been hidden. The gang then drove the containers from the port, retrieved the drugs and covered their tracks. The criminal activity continued for a two-year period from June 2011, until it was stopped by joint action by Belgium and Dutch police. Cyber criminals will continue to do the unexpected, and the nature of attacks of this sort will evolve[1].

1 *www.bullguard.com*

GPS, AIS, AND ECDIS

It has been reported that significant weaknesses have been identified in the cybersecurity of critical technology used for navigation at sea. GPS (Global Positioning System), AIS (Automatic Identification System), and ECDIS (Electronic Chart Display and Information System) are all essential aids to navigation, and each has been identified as potentially vulnerable to attack.

The International Maritime Organization (IMO) is the United Nations organization with responsibility for the safety and security of shipping. It has required that AIS be fitted on board all passenger vessels and on cargo vessels of more than 500 gross tonnage (GT), and on vessels of more than 300 GT if engaged in international trade, since 2004.

The IMO regulations require that AIS will be capable of automatically exchanging information regarding a vessel's identity, type, position, course, speed, navigational status, and other safety-related information with other ships, shore-based facilities, and aircraft. AIS has come to be relied upon as a navigational tool on board ship as an alternative to radar, and is also an integral part of vessel traffic separation systems used by organizations with delegated authority for safety at sea.

Because it doesn't have an inbuilt mechanism to encrypt or authenticate signals, AIS is considered to be a soft target for cyber-attack, which was demonstrated in 2013 by cybersecurity firm, Trend Micro[2]. The firm was able to show how AIS could be compromised by preventing a ship from providing movement information, by making "phantom" vessels or structures appear, by staging fake emergencies, and by making it appear to other AIS users that a ship was in a false location. The online services that monitor AIS data to track the position of vessels were also misled by the efforts of Trend Micro. Earlier in 2013, researchers at the University of Texas were able to demonstrate that they could send a superyacht off course by generating a fake GPS signal that overshadows the genuine signal. Like AIS, GPS for civilian use is not encrypted or authenticated, and is therefore, a potentially easy target.

> "...significant weaknesses have been identified in the cybersecurity of critical technology used for navigation at sea."

2 *Bloomberg.com, Oct 29, 2013*

WHY IS THE MARITIME SECTOR PARTICULARLY VULNERABLE?

It might be argued that the relatively low public profile of most marine businesses means they are less likely to be the subject of a cyber-attack than financial institutions, energy companies, public utilities, or airlines. That may be the case, but nevertheless, the threat is real, and the results of a successful attack could be catastrophic. Certainly, the lack of any inbuilt encryption or authentication code in the critical systems used for navigation on board ship means that shipping could be seen as a soft target, and that perception alone could be enough to provoke an attack.

The *MIT Technology Review* reported that the devices used by Trend Micro and the University of Texas to identify security gaps in AIS and GPS cost €700 and US$2,000 respectively, which is not out of reach of even an enthusiastic teenager with the necessary skills. At the other end of the scale, it is not hard to imagine the consequences of a nation state indulging in cyber-warfare by targeting the container tracking software used by the ports of its perceived enemy in an attempt to disrupt commerce.

Of course, some businesses in the marine sector have a very high profile. A cyber-attack that disrupted the navigation of a large cruise ship would result in enormous media coverage and could, in the worst circumstances, lead to horrific loss of life and significant property damage.

A cyber-attack could lead to horrific loss of life and significant property damage.

The IMO identified as early as 2004 that the publication of AIS-generated data on the internet and elsewhere could compromise the safety and security of ships and port facilities[3]. It has subsequently condemned those that publish this data and encouraged national governments to discourage its publication. However, it was reported in the *MIT Technology Review* that when Trend Micro raised its concerns with the IMO following its dummy attack on AIS in 2013, the IMO replied that it could only respond to a paper submitted by an IMO member government or by an organization with consultative status. On being asked directly in June 2014, the IMO confirmed to Marsh that the cyber-threat had not been brought forward for discussion by a member and consequently, was not on its work program at this time.

In any event, updating the existing protocol and regulations to address the current potential threat would take time, while replacing the equipment on board the world's fleet with sufficiently secure new systems would take considerably longer. In the meantime, the potential threat remains and is undoubtedly increasing.

3 *www.IMO.org*

THE COVERAGE GAP

The logical response to a threat is to consider the probability of an event that could cause a loss occurring against both the expected and maximum negative outcomes if the event were to occur. Once the likelihood and the potential consequences are understood, informed decisions can be taken on risk mitigation and transfer. However, this conventional approach to risk management is not applicable to the cyber threat as described above because of a specific exclusion in insurance policies.

The risk of a cyber-attack has been around for as long as there have been computers, but increased exponentially at the end of the 20th century with the arrival of the internet and the widespread use of closed computer networks as an essential business tool. Insurers recognized that the threat existed, but did not understand it. That meant they were unable to gauge the probability of a loss which, in turn, meant they were unable to put a price on the exposure. Consequently, insurers (and their reinsurers) began excluding losses as a result of a cyber-attack from their policies.

"The risk of a cyber-attack increased exponentially at the end of the 20th century with the arrival of the internet and the widespread use of closed computer networks."

In the world of marine insurance, insurance policies that cover ships, shipyards, and cargo-handling facilities have, over the last 10 years, included the Institute Cyber Attack Exclusion Clause (CL 380) 10/11/2003, or a variant of that clause that has the same result.

CL 380 is a "paramount clause," which means it should currently be included on all marine insurance policies. The clause states:

1.1 Subject only to Clause 1.2 below, in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software program, malicious code, computer virus or process or any other electronic system.

1.2 Where this Clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1. shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software program or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.

In practical terms, therefore, and to the extent that it would be covered by the applicable insurance, any loss or damage (including consequential loss and business interruption) or liabilities attributable to a breakdown of a computer system would *prima facie* be recoverable from insurers. However, if the loss, damage, or liability was caused either directly or indirectly by the use of a computer and its associated systems and software "as a means of inflicting harm," such loss, damage, or liability would be excluded from coverage.

As is often the case, protection and indemnity (P&I) cover is an exception. P&I clubs that are members of the International Group cover P&I claims that result from a cyber-attack unless the attack is an act of war or, more likely, the work of terrorists. In those circumstances the clubs exclude cover for liability directly or indirectly caused by the use or operation as a means of inflicting harm of any computer virus. However, the clubs have partially reinstated that exclusion by establishing a special pooling facility with a limit of US$30 million per ship in the aggregate. This facility will cover the P&I liability of their members to pay damages, compensation, or expenses in consequence of personal injury to or illness or death of any seaman, and for the legal costs and expenses incurred solely for the purpose of avoiding or minimizing any liability or risk insured by the club.

Other than the limited cover provided by the P&I clubs' pooling facility, the "CL 380 type" exclusion of losses that are the result of a cyber-attack is applied universally by the marine insurance industry in its coverage of vessels and of shore-based facilities.

CLOSING THE COVERAGE GAP

From an insurance buyer's point of view, the ideal solution would be for any cyber-attack exclusion clause to be deleted from all applicable insurance policies. That will not happen, at least in the short term, because insurers themselves rely on reinsurance programs for protection, and these reinsurance programs also incorporate CL 380 or an equivalent exclusion provision.

Until recently, that left businesses with a clearlydefined risk exposure that they could not either avoid or transfer. The insurance industry can be creative in response to evolving risk exposures and now there are a small number of major insurers that are prepared to consider offering significant underwriting capacity to cover those risks excluded by reason of a cyber-attack exclusion clause. This is a rapidly evolving development, but we anticipate that before the end of 2014 it will be possible for a company to buy as much as US$200 million to US$300 million of cover against the risk of loss, damage, or liability as a result of a cyber-attack.

CONCLUSION

The computerized systems that the maritime sector now relies upon were designed to meet the needs of the 20th century, but are not equipped to meet the threats of the 21st century. The vulnerabilities within these essential systems present an open door and it is probably only a matter of time before an attacker walks through, with potentially devastating consequences.

The Institute Cyber Attack Exclusion Clause (CL 380) 10/11/2003, or a variant of that clause, has appeared on marine policies for the past 10 years, excluding any loss, damage, or liability caused either directly or indirectly by the use of a computer and its associated systems and software "as a means of inflicting harm." While there appears to be no suggestion from the industry that this clause will be withdrawn any time soon, there are now a small number of major insurers that are prepared to consider offering significant underwriting capacity to cover the risks that have been excluded since 2003.

.

MARSH

For further information, please contact your local Marsh office or visit our website at marsh.com

NICK RIDDLE
Senior Vice President
Global Marine Practice
+44 (0)20 7178 4406
nick.riddle@marsh.com

STEPHEN WARES
EMEA Leader
Marsh Cyber Risk Practice
+44 (0)20 7357 5420
stephen.wares@marsh.com