LOSS PREVENTION Briefing

NORTH SERVICE, STRENGTH, QUALITY

LOSS PREVENTION BRIEFING FOR NORTH MEMBERS SHIPS / JULY 2017

Cyber Risks in Shipping

Contents

A Definition of Cyber Risks Might Be:

'Cyber risk' means any risk of accidents, incidents, financial loss, business disruption, or damage to the reputation of an organization through failure of its electronic systems or by the persons using those systems.

In a shipping context a cyber risk may be the failure of an onboard GPS receiver due to a fault with the equipment, extending right through to catastrophe scenarios of vessel systems being attacked and the vessel being disabled, run aground or taken over by malicious third parties. Although the catastrophe scenarios are possible the likelihood of such an incident for most companies is low.

The risks of electronic equipment failure are generally well recognised in the industry and critical equipment will often be required to have redundancy, spares will be carried or manual operation will be possible should the electronics fail.

What has been less well recognised until recently is the risk of electronic systems being subject to unauthorised access or malicious attacks – let's call them 'Cyber Threats'. Recently there has been a focus on this area and the steps that might be taken to defend shipping companies from unauthorised access or malicious attacks. The defences taken to defend systems are known as 'Cyber Security'.

It is important to recognise at the outset that cyber risks should not be seen solely as the responsibility of the IT department. They have companywide implications. Any measures put in place to control the risk can affect business practice. As such cyber risks must be dealt with on a whole company basis that includes both equipment and personnel, as well as taking into account the wider business implications of any security measures.

Cyber Risks in Shipping

Cyber Risk and P&I Cover

Many market insurance policies specifically exclude losses or liabilities' arising as a result of cyber risks, but at present International Group poolable club cover does not.

This means that Members benefit from the same level of P&I cover should a claim arise due to a cyber risk, as they would from such a claim arising from a traditional risk. As always cover is subject to the Club rules.

While there is currently no internationally agreed standard as to what constitutes a prudent level of cyber risk management or protection, this does not mean that owners, charterers, managers or operators of ships can ignore the need to take proper steps to protect themselves in the belief that their club cover will always respond.

All International Group cover can be prejudiced by the failure to take all obvious steps to prevent foreseeable loss or liability, and as more and more potential cyber risks are being identified as indicated below, clubs will expect to see operation of sensible and properly managed cyber risk policies and systems both ashore and on vessels.

Cyber Security

One definition of cybersecurity is

'Cyber security' *is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.*

Until relatively recently cyber security has not really been an issue for ships. They were not connected to the outside world. Advances in technology mean that ships systems are not only being networked together but are also connected to the World Wide Web. This means that ships are now more vulnerable to cyber threats than previously.

How Does This Affect My Company?

Shipping companies are targeted by cyber criminals, just like any other company or individual might be. There are already numerous examples of companies that have been compromised by a cyber threat. It can affect a company's bottom line, damage its reputation or disrupt its business. At the more extreme end of things there is the possibility that malicious groups or individuals may seek to cause shipping accidents although the risks of this are currently thought to be low for most companies.

How Does This Affect Me?

Cyber security is everyone's responsibility. One of the main means for cyber criminals to gain access to a company's systems is via the employees. In most cases this is entirely inadvertent; the individual will have been taken in by a scam of some kind or will be unknowingly connecting a compromised device to the system. We will look at some examples later. It is therefore important for individuals to understand and abide by their companies' cyber security protocols.

The Role of the Authorities

The authorities, particularly in Europe and the USA, are concerned about the current vulnerability of shipping companies to cyber threats. The US Coast Guard is expected to publish a Navigations and Vessel Inspection Circular (NVIC) on the topic of maritime cyber risk management before the end of the calendar year.

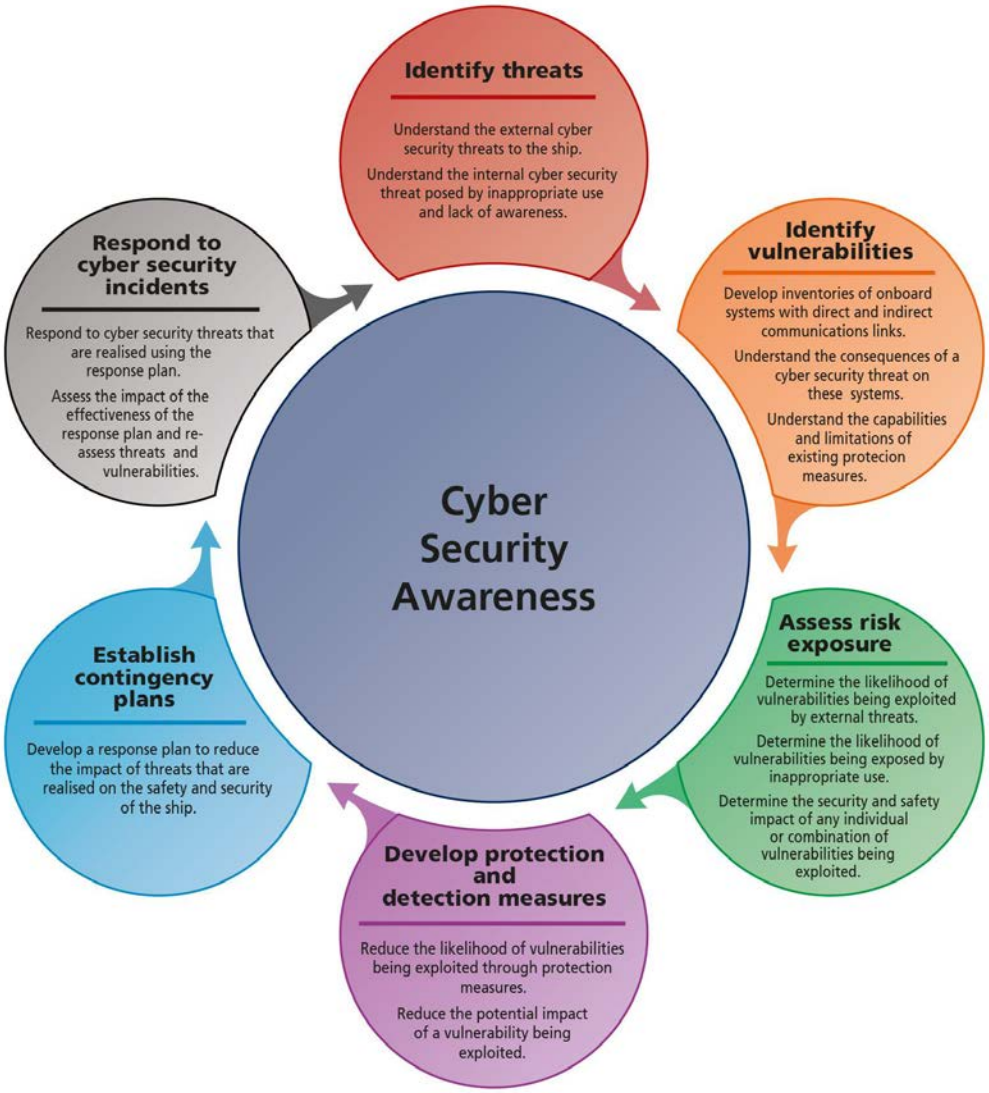
Meanwhile the industry has not been standing still and a coalition of industry bodies, including Bimco, CLIA, ICS, Intercargo and Intertanko, have published guidelines that seek to assist shipping companies with their cyber security efforts. These guidelines form the basis of much of this briefing and should be referred to by Members interested in cyber security for shipping. The IMO have also drafted guidelines on cyber security and both can be accessed below.

Interim Guidelines On Maritime Cyber Risk Management

The Guidelines on Cyber Security Onboard Ships published by BIMCO

Feels Familiar?

The prospect of dealing with cyber security will be daunting for many shipping companies. It's new, involves things that may not be fully understood, and most of us are not likely to have received any formal training in such risks. Whilst undoubtedly this is true, and many companies will require third party assistance in this area, the guidelines have a familiar feel. At their most basic they are a simple risk assessment with measures put in place to control the risk. That's a process that is very familiar to shipping companies. The image below, taken from the guidelines, shows the process. We will consider each step very briefly. The guidelines go into more detail.



Cyber security awareness - Closing the loop

From Guidelines on Cyber Security Onboard Ships Published by BIMCO

Identifying the Threats

The guidelines identify 4 groups who may give rise to a threat. They are activists (including disgruntled employees), criminals, opportunists (they like the challenge of breaking in) and states or terrorists. Each has different motivations and objectives. The table describes some possible motives and objectives.

Every company will have to consider the risk from the different groups. For example a container shipping company is probably at more risk from criminal gangs seeking to steal cargo than a bulk cargo operator, simply because the goods they ship may be portable and have high value. Similarly a tanker company may be at more risk from environmental activists than those involved in other sectors.

Cyber Risks in Shipping

Group	Motivation	Objective
Activists (including disgruntled employees)	Reputational damage Disruption of operations	Destruction of data Publication of sensitive data Media attention
Criminals	Financial gain Commercial espionage Industrial espionage	Selling stolen data Ransoming stolen data Ransoming system operability Arranging fraudulent transportation of cargo
Opportunists	The challenge	Getting through cyber security defences Financial gain
States State sponsored organisations Terrorists	Political gain Espionage	Gaining knowledge Disruption to economies and critical national infrastructure

Attacks

Companies are at risk of attack, both targeted and untargeted, in much the same way as individuals.

You may have heard terms like phishing, spear phishing, botnet and water holing. These are explained in the guidelines as are the stages of a cyber attack.

The key message in relation to an attack is that personnel are aware of these potential cyber security risks and are trained to identify them and to mitigate the risk.

Assessing the Risk

It is important when assessing cyber risks that the company also considers the risks to the business that may result from cyber security measures, and how these measures will affect business practices and relationships both internally and with customers.

The guidelines suggest that the National Institute of Standards and Technology (NIST) Cyber Security Framework can assist in developing your approach to cyber security. The stages NIST describe are Identify, Protect, Detect, Respond, Recover. These are dealt with in more detail in the guidelines.

An initial risk assessment may be thought of as a mapping exercise that should include:

- Which IT systems and operational technology systems are vulnerable and how they are vulnerable, including human factors.
- What controls are in place to protect the systems and do these cover the vulnerabilities
- Which key shipboard operations are vulnerable (talk to your equipment suppliers)
- The identification of possible cyber incidents, their impact on shipboard operations and their likelihood.

Whilst it is a good idea for every company to conduct this exercise it may be that those companies with less resources have to rely on third parties to assist them. Early identification of a reliable third party can greatly assist. Ideally, such a company would have both IT security expertise and experience in shipping.

The end result of the assessment should be a report that identifies all the vulnerabilities and assesses the risk in terms of its impact and probability. Corrective actions should be recommended that will reduce the risk.

Reducing the Risk

The steps to be taken to reduce the risk will be unique to each company.

In general there will be two types of response; technical responses, those that deal directly with equipment and systems; and procedural responses which will focus more on how systems are used and how humans interact with the systems.

The technical responses will be those that can deliver quick wins. Getting procedural control in place requires changing existing practices and attitudes and will involve awareness raising and training – something that will take time.

It is almost inevitable that your company or vessel systems will be compromised by a cyber threat in the future, if this

has not already occurred. For this reason the guidelines recommend that contingency plans are in place to deal with the various threats.

Contingency Planning

In much the same way as emergency plans are already in place for your vessels, plans will have to be developed that take into account various scenarios. The guidelines have identified a list of some of the critical elements related to ships

- Knowing what to do in the case of disabling, or manipulation, of all types of electronic navigational equipment;
- Knowing what to do in the case of disabling, or manipulation, of industrial control systems for propulsion, auxiliary systems and other critical systems;
- Knowing how to verify that data is intact in cases where penetration is suspected but not confirmed;
- Procedures for handling ransomware incidents; and
- Operational contingencies for ships in cases where land-based data is lost.

Response, Recovery and Investigation

A cyber incident will require a response; firstly it must be identified, then investigated and action taken to address the incident and any data or systems affected must be recovered. This process may involve shutting down systems, or communications links, activating software and involving persons from IT.

Recovery of essential ship or system functions related to the safe operation and navigation of the ship may have to take place with assistance from ashore. How and where to get assistance, for example by proceeding to a port, needs to be part of the recovery planning carried out by the ship in cooperation with the shipowner or operator.

Investigations should result in a better understanding of the threats facing shipping companies and the ships they operate, including lessons learned and any updates that are required to technical and procedural controls.

Investigating cyber incidents can be a complex and challenging task. Companies should consider using external expert assistance to investigate such incidents as appropriate.

Shipping Companies are Vulnerable – Some Examples

Ship's Equipment

Various ship's equipment is already known to be vulnerable:-

GPS - University of Texas at Austin researchers demonstrated that they could send a vessel (a 210-foot yacht) off course by camouflaging a genuine GPS signal by using a spoofing device to download a false signal into the vessel's GPS antennas. Once the researchers accomplished this, they then controlled the vessel. Onboard GPS neither alerted nor indicated any course changes.

ECDIS - Although ECDIS has been approved by the International Maritime Organization for use as an alternative to paper charts, the technology itself has been identified by researchers as vulnerable to hacking.

AIS - does not utilize encryption or signal authentication, and has long been recognized as vulnerable. In 2013 the security firm Trend Micro demonstrated that compromised AIS signals could be spoofed, falsifying vessel positions.

Whole Business Disruption

In 2011 the Iranian Shipping Line, IRISL, experienced a highly damaging cyber attack that resulted in business-level consequences. Hackers were able to successfully exploit vulnerabilities in the company's network to access their servers. Once in, and following a period of network reconnaissance, they moved. They accessed a range of business applications and deliberately manipulated data. What was affected? Rates, loading information, cargo-tracking numbers, and customer data. What was the result? Rates were falsified. The company lost track of where containers were physically located. Containers were delivered to incorrect destinations. Some were 'cloaked' while others were completely lost. Both IRISL's fleet and terminal operations were impacted. Months were required to recover.

Exploiting Cargo Information

Between 2011 and 2013, organized criminals recruited free-lance hackers to successfully breach the networks of targeted terminal operators in a large European port. Initial access was gained via effective deployment of targeted malware to staff, subsequent access was facilitated by physically penetrating the facilities whereby the hackers

installed key-logging devices onto networks[1]. Once inside the targeted networks, hackers gained access to the terminal operating systems responsible for managing and controlling container movements. Capturing the key-logging outputs, the criminals successfully smuggled narcotics among legitimate cargo by exploiting cargo location, manifest data and pickup times. They were eventually discovered via law enforcement action.

Though most cargo theft and data manipulation is to facilitate criminal activities, the vulnerabilities they represent are far more significant and this is perhaps the area which is of most concern to authorities. Degradation of data integrity within cargo management and terminal operating systems raises concerns around local, national and regional security on matters relating to narcotics, weapons, and human trafficking.

Persistent cyber vulnerabilities in cargo management systems leave both shipping companies and terminal operators at risk.

Human Factors

As Edward Snowden demonstrated in his exposure of US Government information, the single greatest cyber risk to any organization operating in today's interconnected world is the Human.

With the use of social media sites, smart phones, and a wide range of mobile devices it is not surprising that the most effective entry point for a cyber threat actor to access an organization is through the Human.

There are two distinct kinds of human threat organizations may be vulnerable to.

The first is via the individual who intends to cause harm to the company systems or security. This may be driven by different motivations e.g. greed, anger at a colleague or employer, blackmail by a third party, political or religious ideology.

The second threat is unintentional and arises via individuals with little or no training on cyber risks. They can leave organizations significantly and persistently vulnerable to cyber threats. Due to their lack of training or awareness these individuals may be highly susceptible to malware delivered via an innocuous appearing Email (e.g. spear-phishing), false websites (watering hole attack) and manipulation via social media and other means (social engineering).

It is accepted that the insider threat represents the greatest cyber threat to a shipping company.

One of the most common forms of unprivileged network access is through the inappropriate use of portable flash drives (e.g. "thumb drives"). Seafarers also commonly use mobile devices for entertainment purposes to help while away the time during long sea passages – e.g. the downloading of images and/or videos on networked bridge systems. These practices are very risky from a cybersecurity perspective.

In early 2016 a HudsonAnalytix client suffered a direct loss of more than USD $250,000 due to an employee that fell for a social engineering scam that resulted in a series of fraudulent transactions to the criminals. Another client paid out an undisclosed sum to restore business systems as a result of a Ransomware attack that left their headquarters network inoperable.

Time To Start Thinking About Cyber Security For Your Company

The examples demonstrate that criminals and others have already successfully targeted shipping companies via electronic systems. Technology and connectedness will play an increasing role in shipping and this creates opportunities for criminals and others. Shipping companies wishing to reduce risks to protect operational efficiency and profitably should therefore take steps to make their organisations less vulnerable to cyber risks.

North is grateful to Max J. Bobys of Hudson Analytix for his assistance with this briefing.

Max J. Bobys
Vice President, Global Strategies
HudsonAnalytix, Inc.
Ferry Terminal Building, Suite 300
2 Aquarium Drive
Camden, NJ 08103

Mobile: +1.301.922.5618
Office: +1.856.342.7500
Max.Bobys@hudsontrident.com
www.hudsonanalytix.com

[1] The hackers accomplished this by utilizing purpose-built mini computers disguised as power strips and Internet routers, called *pwnies* (pronounced "pony"). Pwnies can go unnoticed in office environments while intercepting data traffic on the organization's network.

Further Information:

Guidelines on Cyber Security Onboard Ships published by BIMCO

Guidelines on the Facilitation Aspects of Protecting the Maritime Transport Network from Cyber threats published by the IMO