Cyber Security the Unknown Threat At Sea

Rahul Bhandari*, Subhasree Swagatika Mohanty**, Jordan Wylie***,

* Deck Cadet CERT HE (Nautical Science) Liverpool John Moore's University, UK

**PhD Scholar (Marine Biology) Liverpool John Moore's University, UK

*** MA, BA (Hons), Coventry University, UK

Figure (1) represents cyber security.

ABSTRACT:

Merchant vessels are becoming larger and are using more electronic systems than ever before. Currently, computer systems are being used in ships for many purposes such as navigation, rapid unloading of cargo, and handling and tracking of goods at ports. Unfortunately, these computer systems are highly vulnerable to cyber threats.

The paper presents the need to invest time, effort and capital into security measures to ensure that these cyber risks are appropriately managed in the maritime industry.

When discussing maritime safety, the term human element or human factor plays a crucial role. There is no established international definition of the term, but according to IMO (2004a), it is defined as a "complex issue affecting marine safety and security".

- 100% of IT Departments Provide No On-board Awareness or Training Programmes for Crew.
- 91% of Ship Security Officers Believe Training & Education is Required to Manage Cyber Risk
- 80% of Reported Information Security and Cyber Incidents at Sea Related to Human Error.

New Challenges & Opportunities:

- Distinct Lack of Awareness & Training, Lack of Cyber Crime Reporting, Marine Operations Immersed in the Digital Era, More Automation on the Horizon.
- Human Factor Attributable to Most Safety Incidents On-board.
- Greater awareness is needed in the industry.
- Cyber-crime is constantly developing and there is a need to keep up with it.

Technology is only as good as the end user, we can have all the best equipment but without trained and skilled end user, it is useless.

Recommendations for preventing and mitigating risk of cyber-crimes on the maritime industries are as follows:

- Educate seafarers about IT and information security alternatively, we should have a "STCW COURSE included for cyber-crime security" both on basic and advanced levels.
- A cyber-risk assessment can be conducted at frequent intervals by a qualified expert in order to thoroughly review security protocols

Keywords: Cyber-crime, Cyber risk assessment, S T C W courses, Piracy, Cyber feed, Human error.

1. Introduction

This presentation introduces the need of cyber security, the majority of vessels are extremely high-tech, and as time passes more and more depend on satellite communication and electronic control system, and by integrated bridge system. While these electronic systems have enormous benefits, it means that vessels are open to another form of attack, from persons hacking into the system of the vessel and introducing bugs, viruses and false data.
Cyber-attacks are a more feasible, low cost and risk-free option for terrorist action. While initial consideration of cyber-attack has been directed at port infrastructure, there have been reports of merchant ships having incorrect global system positioning systems (GPS) readings with suggestion that ship's equipment can be tampered remotely.

Figure (2) Represents securing digital information

The challenge for ship owners is even more complex because cyber criminals are targeting diverse facets of the shipping industry. For example, there was a well-documented case of drug smugglers subverting an IT system at a major port in order to facilitate the smuggling of contraband in containers.
The rise of targeted piracy and drug smuggling reflects how criminal organizations have become more sophisticated. They will seek detailed intelligence on potential targets and will use modern technology to source information and data to assist in their planning and execution of criminal ventures. Drug traffickers, drug and people smugglers, pirates and fraudsters of all stripes are taking every opportunity to gain information that they can turn to their advantage.
Cyber security threats today are increasing in variety, frequency and sophistication — be it from a Trojan USB stick that introduces malware aimed at acquiring sensitive commercial information, an email with detailed vessel itineraries sent to a large group of unknown people, the full-scale subverting of a company's IT system or the potential compromising of Automatic Identification System (AIS) and Electronic Chart Display and Information System (ECDIS) systems on board ships. The number of potential risk scenarios is significant and keeps growing.

Types of cyber-attack

In general, there are two categories of cyber-attacks which may affect companies and ships:

- **Untargeted attacks**, where a company or a ship's systems and data are one of many potential targets; or
- **Targeted attacks**, where a company or a ship's systems and data are the intended target. Untargeted attacks are likely to use tools and techniques available on the internet which can be used to locate known vulnerabilities in a company and on-board a ship.
-

Examples of some tools and techniques that may be used in these circumstances include:

- **Social engineering**. A non-technical technique used by potential cyber attackers to manipulate insider individuals into breaking security procedures, normally, but not exclusively, through interaction via social media.
- **Phishing**. Sending emails to a large number of potential targets asking for particular pieces of sensitive or confidential information. Such an email may also request that an individual visits a fake website using a hyperlink included in the email.
- **Water holing**. Establishing a fake website or compromising a genuine website in order to exploit visitors.
- **Ransomware**. Malware which encrypts data on systems until such time as the distributor decrypts the information.
- **Scanning**. Attacking large portions of the internet at random. Targeted attacks may be more sophisticated and use tools and techniques specifically created for targeting a particular company or ship. Examples of tools and techniques which may be used in these circumstances include:
- **Spear-phishing**. Similar to phishing but the individuals are targetted with personal emails, often containing malicious software or links that automatically download malicious software.

Stages of a cyber-attack :

Cyber-attacks are conducted in stages. The length of time taken to prepare a cyber-attack will be determined by the motivations and objectives of the attacker, and the resilience of technical and procedural cyber security controls implemented by the company, including those on-board its ships. The four stages of an attack are:

 Survey/Reconnaissance. Open/public sources used to gain information about a company, ship or seafarer which can be used to prepare for a cyber-attack. Social media, technical forums and hidden properties in websites, documents and publications may be used to identify technical, procedural and physical vulnerabilities. The use of open/public sources may be complemented by monitoring the actual data flowing into and from a company or a ship.

 Delivery. Attackers may attempt to access company and ship systems and data. This may be done from either within the company or ship or remotely through connectivity with the internet. Examples of methods used to obtain access include:

- Company online services, including cargo or consignment tracking systems;
- Sending emails containing malicious files or links to malicious websites to seafarers;
- Providing infected removable media, for example as part of a software update to an on-board system; and
- Creating false or misleading websites which encourage the disclosure of user account information by seafarers.

 Breach. The extent to which an attacker can breach a company or ship system will depend on the significance of the vulnerability found by an attacker and the method chosen to deliver an attack. It should be noted that a breach might not result in any obvious changes to the status of the equipment. Depending on the significance of the breach, an attacker may be able to:

- Make changes that affect the system's operation, for example interrupting the display of chart information on ECDIS;
- Gain access to commercially sensitive data such as cargo manifests and/or crew and passenger lists; and/or
- Achieve full control of a system, for example a machinery management system.

 Affect. The motivation and objectives of the attacker will determine what affect they have on the company or ship system and data. An attacker may explore systems, expand access and/or ensure that they are able to return to the system in order to:

- Access commercially sensitive or confidential data about cargo, crew and passengers to which they would otherwise not have access;
- Manipulate crew or passenger lists, or cargo manifests. This may be used to allow the fraudulent transport of illegal cargo; and
- Disrupt normal operation of the company and ship systems, for example by deleting critical pre-arrival information or overloading company systems. It is crucial that users of IT systems on-board ships are aware of the potential cyber security risks, and are trained to identify and mitigate such risks.

Figure (3) represents pirate attack.

Figure (4) represents Intrusion Alert.

Target systems, equipment and technologies :

This provides a summary of potentially vulnerable systems and data on-board ships to assist companies with assessing their cyber risk exposure. Vulnerable systems, equipment and technologies may include:

- **Communication systems** Satellite communication equipment; Voice Over Internet Protocols (VOIP) equipment; Wireless networks (WLANs); and Public address and general alarm systems.
- **Bridge systems** Positioning systems (GPS, etc.); Electronic Chart Display Information System (ECDIS); Dynamic Positioning (DP) systems; Systems that interface with electronic navigation systems and propulsion/manoeuvring systems; Automatic Identification System (AIS); Global Maritime Distress and Safety System (GMDSS); Radar equipment; Voyage Data Recorders (VDRs); and Other monitoring and data collection systems.
- **Access control systems** Surveillance systems such as CCTV network; Bridge Navigational Watch Alarm System (BNWAS); Shipboard Security Alarm Systems (SSAS); and Electronic "personnel-on-board" systems.
- **Cargo management systems** Cargo Control Room (CCR) and its equipment; Level Indication System; Valve Remote Control System; Water Ingress Alarm System; Ballast Water Systems; and Gas liquefaction.

CONCLUSION

Prevention is better than cure.

- Assess your existing processes and procedures - what information/assets need to be protected, what are the potential risks, how can you improve your cyber security.
- Allocate the risk posed by cyber events in your contracts appropriately.
- Regularly update your anti-virus software, firewalls and other software and ensure your security policies respond to new threats and developments.
- Carry out due diligence of the risks posed by cyber events - review your supply chain to see who is the weakest link. It is a truism that hackers target the weakest link to infiltrate an organisation. That link can exist through the supply chain. How do you know that your supply chain has the same standard of cyber hygiene and resilience as your own entity. It can be embarrassing to ask, however, it can be more embarrassing not to ask.
- Set up a strategy to respond to a cyber-event – who should be involved, what are the priorities following a cyber-event, how regularly is this strategy reviewed.

Whether large or small, specialist or global player, everyone in the shipping industry will benefit from a greater awareness and preparedness to deal with the challenges of modern IT-assisted fraud in the 21 century.

Figure (5) represents discussion on how to control cyber threats.

Bibliography

- Jordan wylie article at www.becyberawareatsea.com
- referred to website cybersail.org documents.
- referred article: Be Cyber Aware at Sea Overview (Feb 2017) at www.becyberawareatsea.com.
- referred article Joint Hull Committee Cyber Risk Information Paper at www.becyberawareatsea.com.