The Cyber Risk and its management in the Marine Industry

Elisa CASSI [a], John Paul (JP) CAVANNA [b] and Paolo SCIALLA [c]
[a] *Lloyd's Register EMEA, Southampton – UK*
[b] *Lloyd's Register, London - UK*
[c] *Lloyd's Register EMEA, Trieste – ITALY*

Abstract. Following a number of high profile security incidents affecting both the information and operations assets of several industry and business sectors in recent years, the need to consider the risks associated with the use of innovative technologies in a number of production and business processes and environments has never been greater. The maritime sector, like many others, is exposed to a number of potential hazards that need to be assessed and addressed. On the assumption that in the last few years Information and Communication Technologies (ICT) have been widely applied in the processing of information and support operations, then passenger and cargo ships, yachts, supply and offshore vessels, as well as waterways transport, harbour facilities and infrastructures are all relevant elements in international cyber risk assessment programs. Similar to hazards associated with other technologies and activities, the 'cyber environment' needs to be considered through appropriate risk assessment processes and the subsequent risks that are identified need to be mitigated by appropriate measures. The rapid evolution of digital and information technologies that attract marine operators and owners by optimising and improving their business demands a similar continuous evolution of protective techniques and testing procedures. This paper will explore the cyber environment and focus on the management of the cyber risk in the marine industry.

1. Introduction

The maritime sector has been highly influenced in recent years by a number of transformational technologies that offer the ability to improve stakeholders' Key Performance Indicators (KPIs).

The impact of the digital age on the shipping industry is tangible in the use of modern technologies that make it possible to integrate real time monitoring and control of ship's systems and machinery and to acquire data from the weather and sea conditions and from other sources of information. The integration, analysis and processing of the massive quantity of data available from navigation systems, machinery, cargo, passengers, safety and other systems can optimise ship operations and be used to develop ships' performance models. This can be exploited to provide accurate and optimised schedules of vessels' voyages, reduce fuel consumption, warn crews of potential systems or components failures, help and support emergency decision making. Furthermore the use of advanced

automation technologies is triggered by the need to minimize hazards associated with human errors as the majority of the incidents in the shipping sector are recognised as being caused by that. (1)

The technologies that have been identified as the top drivers for the commercial shipping industry (comprising Shipbuilding, Propulsion and Powering, Smart Ships, Advanced materials, Big Data Analytics, Robotics, Sensors and Communications) over the next few years are all linked to, or influenced by, digital and communication technologies, either directly or indirectly. The majority of, if not all, the machinery and systems installed on a modern ship are monitored and controlled by Supervisory Control And Data Acquisition (SCADA) systems that transfer data from sensors to processing units, Distributed Control Systems (DCS) and Programmable Logic Controllers (PLC) combining sensors and controlling electrical, mechanical, hydraulic components and actuators.

The ships' ICSs such as navigation systems, propulsion, steering and power management, dynamic positioning, cargo handling, bilge and ballast, safety systems, use the same computer-based technology, (i.e. the same or similar processing unit technologies) as other shipboard systems such as internal and external communication, passengers entertainment, ventilation and conditioning, lighting and others.

Each of those ICS sub-systems is provided with a lower level of communication infrastructure based on a bus network. A higher level of communication is a backbone Local Area Network (LAN) often closed in a ring, sometimes duplicated and redundant, where data coming from sensors is exchanged between Data Concentrators, processed by PLC units and sent to actuators in both directions to monitor and control activities and processes. On the same communication infrastructure DCS central servers are in charge of data acquisition and control activities of processes and operations since Human Machine Interfaces (HMI) provide information to the human element (operator) and allow personnel to interface with machinery and processes. Logs generated by the readings and operations of sensors, instruments, alarms and other events generated by the sub system are stored and logged.

The above principle and architecture is common to the majority of ships' systems and this makes the interconnection of different shipboard LANs, as well as the sharing of information and data of different systems, technically easy. It also allows different HMIs to operate on different systems and to process different operations, ultimately even allowing a higher level of data management by spanning large geographical areas and connecting to remote land based operation centers. To do this, Wide Area Network (WAN) technologies are needed, and for shipboard systems this is offered by satellite technologies when at sea, mobile communication networks when in coastal navigation within the range of their coverage and WiFi networks when docked in ports. All these use a part of the infrastructure provided by Telecommunication Services Providers Companies.

It is easy to imagine the benefits that can be derived from the external connection of shipboard systems and a number of ship owners have already improved their business operations by remotely monitoring ships' data, collecting data from ship's navigation systems, fuel consumption, cargo, passengers, and then feedback ship's crew with information that optimise operations. Additionally, machinery and complex shipboard systems are remotely monitored by Original Equipment Manufacturers (OEM) that can provide 24/7 assistance on failures, optimisation of maintenance by remote diagnostics and software upgrades when required.

The *cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision* is generally defined (2) as IoT (Internet of Things). In the IoT context *Things* are physical or virtual objects capable of being identified and integrated into communication networks with the exchange of data and information being made through gateways that ensure the interoperability of things. The communication can be either wireline-based or wireless and there are a huge number of protocols for both these mediums.

The 'cyber environment' is defined as the interconnection of the networks of both information and cyber-physical systems utilising SCADA, computer-based and wireless systems, including the information, services, social and business functions (3).

Such an environment is not limited to ships' systems but extends to shore based activities of both the ships operators and the ports' cities (4) and is in general associated with two main technology families: Information Technology (IT) where data is used for information and Operation Technology (OT) where data is used for industrial processes.

Before the latest changes to the ICT environment, access to data and information and the operation of processes used to be limited to the ships' personnel only. The interconnection of systems and their connection to external communication systems that have been described above made access to information and operations available at different levels.

The extent of this data access exposes assets to new risks classified as 'cyber risks'. The causes can be associated with incorrect use or misuse of technologies, interference with communication, as well as threats from external attacks and intrusion that can generate harm to assets, persons, systems or organisations. Therefore security is one of the main concerns for the cyber environment.

2. Overview of the international and European program for infrastructure protections

The extent of cyber risks makes the defence of public interests and safety a priority for countries and it is recognised that the maritime sector, similar to other industry sectors, represents a critical infrastructure that is now exposed to these cyber risks and as such needs to be protected appropriately.

The U.S. President issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," on February 12, 2013, (5) was designed to establish the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.

In enacting this policy, the Executive Order calls for the development of a voluntary risk-based Cybersecurity Framework – a set of industry standards and best practices to help organisations manage cybersecurity risks. The National Institute of Standards and Technology (NIST) issued such a Framework (6), created through collaboration between government and the private sector, addressing the cybersecurity risk in a cost-effective way based on business needs.

The Framework focuses on using business drivers to guide cyber security activities and consider cyber security risks as part of the organisation's risk management processes.

On the other hand, the European Parliament and the Council of the European Union issued a Directive (7), also called 'NIS Directive', which relates to measures needed for a high common level of security of Network and Information Systems across the Union so as to improve the functioning of the internal market.

The above US and EU programs are based on the recognition that nowadays a number of infrastructures are considered as critical within countries and the fact that digital and communication technologies are widely used is the trigger to such programs to defend those critical infrastructures from cyber risks. The water transport sector, including ports activities but also seagoing traffic, is considered one of the critical infrastructures and as such is part of cyber security programs.

Similar to other industrial, financial, welfare, social and economic sectors, threats to the marine sector cyber environment can come from several sources, among them:

Activist groups (also known as 'hacktivists') - typically threaten operational technologies in seeking publicity or to create pressure on behalf of a specific objective or cause.

Espionage – (Commercial or State sponsored) - seeking access to sensitive information.

Organised crime – driven by financial gain and a typical activity attributed to pirates in the maritime sector.

Terrorism - aiming to attack ships or port activities to generate fear and cause physical and economic disruption.

Warfare – conflict between nation states.

National Cyber Security programs also aim to establish authorities that are to be notified of occurrences of cyber incidents (Computer Security Incident Response Teams, CISRT and Computer Emergency Response Teams, CERT) and these will have technical and organisational capabilities to prevent, detect, respond to and mitigate network and information system incidents and risks.

Within the Maritime Sector the International Maritime Organization (IMO) issued the Guidelines on Maritime Cyber Risk Management (8) providing high level recommendations and approached the risk by using the same cyber security lifecycle as mentioned in the NIST Cyber Security Framework:

Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.

Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.

Detect: Develop and implement activities necessary to detect a cyber-event in a timely manner.

Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.

Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

The above cyber security functions are the higher level of a set of Cyber Security activities that the NIST calls *Framework Core*, that are common across critical infrastructure sectors. The *Framework Profiles* represent the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. As an example the United States Coast Guard (USCG) developed a CFP (Cybersecurity Framework Profile) (9) for three maritime businesses: the Maritime

Bulk Liquids Transfer (MBLT) mission area, the Offshore Operations, and the Passenger Vessel Operations. Such profiles identify and prioritize the minimum subset of Cybersecurity Framework Subcategories tailored around the specific characteristics of those business environments. The Mission Objectives are identified for each Profile in order to prioritise and allocate the appropriate resources to the scope of the cyber security management process.

3. Identification of the vulnerabilities

Within the Cyber Risk Management and Cyber Security environment it is common practice to use a risk assessment approach to identify and quantify the risks associated with the cyber hazards. Where risks are identified and considered to be above the limit of acceptability, then there is a need to identify appropriate controls to reduce or mitigate the risk. Controls can be considered on the three levels of people, process and technology in terms of what is the most appropriate method to reduce/mitigate the risk. The technology level is addressed by technical solutions that defend from the hazards considered; the process controls are based on the reduction/mitigation of the risk by appropriate operational procedures that implement the use of the technology under consideration. Finally, the controls can relate to people where the reduction/mitigation of the identified risk is dealt with through proper personnel training and competency.

Whenever a control is missing, either because it has not been considered or because it is not implemented, that is commonly defined as a *vulnerability* in cyber security terms.

Studies performed in 2013 showed critical technology used for navigation at sea like GPS (Global Positioning System), AIS (Automatic Identification System), and ECDIS (Electronic Chart Display and Information System) created significant weaknesses in a ship's cyber security posture, despite being essential aids to navigation and critical assets for the ships.

In relation to the AIS, since no inbuilt mechanism to encrypt or authenticate signals is available on the AIS, an attacker could identify an easily exploitable entry point. To validate this, in 2013 a cybersecurity firm, Trend Micro2 was able to show how the AIS could be compromised by making "phantom" vessels or structures appear, by staging fake emergencies, and by obfuscating the ship's actual location on the maps. The online services that monitor AIS data to track the position of vessels were also misled by the efforts of Trend Micro. Moving to the ECDIS systems, which need periodic map updates and sometimes rely on physical access through a USB key to load the updated maps, it is easy to imagine a scenario where a genuine user, without realising it, could inadvertently spread malware allowing an attacker access to the underlying operating system. Needless to say a number of these systems are configured to operate with administrator rights and no password protection, increasing the risk of untargeted attacks being successful on strategic aids to navigation. GPS systems, like AIS systems, are not encrypted or authenticated, and are therefore, a potential easy entry point for an attacker. 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 overlaid the genuine signal.

4. Protection of the cyber environment

2017 saw a proliferation of cyber-attacks, showing that the cyber threat landscape is complex and constantly changing. To answer this, marine and offshore organisations need to take a more strategic approach to protecting their critical assets and business drivers. They need to build secure and scalable security postures by deploying comprehensive, multi-layered defences that are risk-based and threat intelligence-led. They need to cover not just technology but people and processes as well to ensure that technologies are properly configured so as to step up to the increasingly complex challenges that face them.

There are various approaches to reducing the exposure to both common and sophisticated types of cyber-attack on interconnected systems.

As a general principle, in order to ensure an effective protection from cyber threats, it is important to start by identifying what ultimately must be protected and then designing the perimeter security around it. Acknowledging that everything is hackable and no defense mechanism is 100% secure is the first step in defining a successful security posture. Rather than trying building an "*impregnable fortress*", the aim should be to develop effective security defenses around the critical business and the supporting infrastructure. Additionally, since the cyber threats are constantly evolving, the design of the network defenses needs to be flexible enough to scale and meet future needs.

4.1. The traditional approach to security: Perimeter Defense

Across all sectors, the traditional first line of defense against cyber-attacks is the perimeter security, which usually starts from a Firewall. The firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. The traditional firewalls are binary solutions where either traffic is allowed or it's blocked depending on the predefined rules.

The evolution of these network security devices has brought the Next-Generation Firewall, which can include application control, identity awareness and other capabilities such as Intrusion Prevention Systems (IPS), Web Filtering, and Advanced Malware Detection, all delivered from the same appliance.

Either as part of a Next Generation Firewall or a separate device, the Intrusion Prevention System (IPS) is another important perimeter defense mechanism. An IPS is an in-line device that blocks malicious traffic. Having an IPS properly optimised and monitored is a good way to catch attackers that have slipped past the first line of defense (the firewall).

As Cloud computing is becoming an increasingly popular paradigm due to new services and increased media attention, new protection services like the Cloud-based Malware Detection and the DDoS Services have become available. Unlike appliance-based solutions these are cloud-based services that sit outside the architecture and analyze traffic before it hits the network.

The perimeter-based defenses just described rely on the assumption that everything on the internal network can be trusted therefore countermeasures are deployed on a limited number of pre-defined entry points to the network.

However, this assumption is no longer valid in the maritime sector since wireless technologies onboard, the proliferation of partner connections and the need to facilitate the interaction between headquarter and vessels blur the distinction between "internal" and "external". Additionally, insiders, whether intentionally malicious or just careless,

may present a very real security threat that would go undetected by the perimeter defenses.

4.2. The new approach: Zero Trust Security Model

Originally conceived by John Kindervag and presented by the Forrester Research, "Zero Trust" is an alternative to the traditional perimeter based security model that addresses the shortcomings of failing perimeter centric strategies by removing the assumption of trust from the equation (10).

The guiding principle behind the new approach is "never trust, always verify".

In the maritime sector this means that the essential security capabilities are deployed in a way that provides policy enforcement and protection for all users , devices, applications, data resources, onshore as well as onboard, and the communications traffic between headquarters, vessels, providers and port authorities, regardless of location and user roles.

The basic concepts behind the Zero Trust approach are as follow:

Concept #1: Ensure that all resources are accessed securely regardless of location.

This suggests not only the need for an effective network segregations but also the increased use of secure access for communication to/from resources, even when sessions are confined to the "internal" network, whether this is an internal onboard network or an headquarter based one. It also means ensuring that only devices with the right status and settings are allowed access to the network. Thinking of navigation systems like the ECDIS that can be accessed through a USB stick, an online chart update, or through other electronic on-board systems it becomes increasingly important to implement a well thought access control policy covering all connected systems and the ship to shore interface. This should also be extended to the various actors in the marine supply chain.

Concept #2: Adopt a least privilege strategy and strictly enforce access control.

The goal in this case is to absolutely minimize allowed access to resources as a means to reduce the pathways available for malware and attackers to gain unauthorized access—and subsequently to spread laterally and/or infiltrate sensitive data. Lateral movement, most phishing attacks and other commonly successful cyber threat vectors affecting the marine environment are less effective where not completely blocked under the zero trust model.

Concept #3: Inspect and log all traffic.

The Zero Trust model promotes the idea that you must actively inspect traffic as well as log it. Traffic inspection can be done through network discovery tools for finding and tracking assets, flow data analysis tools to analyze traffic patterns and user behavior, network forensics tools to assist with incident response and criminal investigations and several other tools.

5. Detection of cyber incidents and attacks

Organisations in the maritime sector that store personal and financial data of clients will be forced to record and declare cyber security breaches. Starting from May 2018 the new General Data Protection Regulation (GDPR) will demand that security breaches involving data belonging to any other party must be reported to the authorities

within 72 hours from detection. Fines for failing to do so may amount to 4% of worldwide turnover or up to 20 million Euros.

However, early detection of cyber-attacks is a challenge in all sectors, not only in marine and offshore environments. It's common for successful cyber-attacks to remain undetected by organizations for 6 months or longer.

Since attackers are constantly searching for new vulnerabilities in the evolving digital environments, organizations could consider deploying Intrusion Detection Tools, which are effective tools in the early detection of cyber threats, the control of breaches and the mitigation of damages.

Intrusion detection tools are software or hardware products capable of identifying active threats and generating cyber security alerts that prompt for remediation actions.

Many different products exist in the market, from open source tools to commercial packages; some of these products will be also able to detect advanced, targeted attacks.

A first category of detection tools is based on rules and signatures.

Rules and Signature based Detection Systems identify threats such as intrusions and viruses by watching for patterns of events specific to known and documented attacks. These products perform a network traffic inspection to look for signatures matching known attacks.

A second category of detection tools is based on the analysis of anomalies in users' or systems' behaviours.

Behaviour based Detection Systems rely on the assumption that attack behaviors differ from normal activity and that malicious actions can be detected and identified by looking for deviations from the "normal" pattern of behaviour.

Differently from Rule and Signature based Detection tools, Behaviour based Detection solutions are able to identify advanced, targeted attacks without knowing their signatures in advance.

What differentiates advanced, targeted attacks from more opportunistic threats is the attackers' ability and willingness to dwell in, learn and exploit targeted networks. These are likely to be motivated and well-resourced attackers who can find ways to infiltrate enterprise networks through techniques such as social engineering, zero-day exploits as well as compromising network infrastructure or IoT devices – once inside, they can use the exploited entry point as a pivot to go deeper into the network in what is called the "lateral spread" of the compromise.

Event correlation over a long period of time and from multiple sources is crucial for the detection of advanced targeted attacks.

Even when attackers manage to successfully evade the first line of defence, when exploiting the network they inevitably generate some indicators of the attack, commonly called the "attack metadata". Correlating Attack Metadata is important because all cyber-attacks follow the same pattern: infiltrate, establish command and control, move laterally and exfiltrate data.

Failed login attempts are a common sign of infiltration; unusual resource utilization and execution of unknown processes can be correlated to command and control; increased network traffic from a particular host can be associated to exfiltration of data. Logging and inspecting metadata related to the above events over several hours, days or months enables the early detection of these sophisticated attack; recent advances in analytics technologies make this possible.

Behavioural and Predictive Analytics solutions use metadata as an input feed to create estimations of where the threats reside, making the in-depth investigation more focused and the time to discovery of the threat shorter.

For the above reasons analytics significantly enhance the detection capabilities of defenders.

6. Response and recovery from cyber incidents

F There is a precise legal requirement in having an incident response plan in place. Under the EU's General Data Protection Regulation (GDPR)(11), organisations will need to implement an effective incident response plan to contain any damage in the event of a data breach, and to prevent future incidents from occurring. Organisations with EU data subjects should meet the requirements of the Regulation by May 2018.

The Incident Response Guide from CREST (12) provides valid advice on how to prepare for, respond to and follow up an incident in a fast and effective manner. It is designed to enable organisations to determine what a cyber security incident means and build a suitable cyber security incident response capability. The guide also offers indications on how to select an appropriate supplier where the service is delegated to a third party.

The benefits of using cyber security incident response experts from commercial suppliers are actually quite evident since the need of precise skills and well defined processes for the effective management of security incidents.

After a cyber security incident is detected several activities are to be considered in order to return to normal operations and limit damage to the organization. Post-event activities span from the assessments of the causes and the effectiveness of the management of the incident to the communication of lessons learned.

Fundamental actions in the respond and recover phase are:

- Containment of the threat, preventing it from spreading laterally within the targeted network.
- Investigation to identify the size of the breach and the affected systems as well as the way the threat actor managed to exploit the network.
- Recover by restoring data and operations.
- Report the incident and the wider cyber community by sharing threat data with law enforcement and other shipping companies.

7. Conclusion

The ever increasing complexity of cyber attacks along with the expansion of threat surfaces through more interconnected technologies significantly increases exposure and therefore risk to organisations. This makes it paramount that the right security focus is given to critical business drivers and assets. No business can make itself impregnable to attacks. By creating a scalable security posture based on risk and driven by threat intelligence that seeks to protect those critical business drivers, and through the associated application of the correct security controls and technologies an organisation can position itself to temper an attack and so provide assurance to its Board and shareholders that, in the event of a breach, its effects can be mitigated and disruption and loss to the business minimised.

References

[1] Lloyd's Register Global Marine Technology Trend 2030, issue 2015
[2] ENISA, Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, November 2017
[3] IET Standards, Code of Practice Cyber Security of Ships, The Institution of Engineering and Technology, London, United Kingdom, 2017
[4] IET Standards, Code of Practice Cyber Security of Ports and Ports systems, The Institution of Engineering and Technology, London, United Kingdom, 2016
[5] The White House, Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," on February 12, 2013
[6] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity
[7] DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
[8] International Maritime Organization MSC-FAL.1/Circ. 3, 5 July 2017
[9] US Coast Guard, Maritime Bulk Liquids Transfer, Offshore Operations, and Passenger Vessel Cybersecurity Framework Profiles, version 3 Dec. 2017
[10] NIST, Critical Infrastructure Cybersecurity, Forrester Research inc, Cambridge (MA), 2013
[11] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
[12] Cyber Security Incident Response Guide, CREST (GB), 2013