MARITIME CYBERSECURITY

Information is the key and the vulnerable asset

GMCG
GLOBAL MARITIME CONSULTANTS GROUP

"The crime is not simply stealing your information but using it against you to damage your business."

INDEX

MARITIME CYBERSECURITY

Information is the key and the vulnerable asset

"The crime is not simply stealing your information but using it against you to damage your business."

Author: ***Mr Ionut Paris,***
Managing Director, GMCG Romania

INTRODUCTION

Time moves on and from 1 January 20201 there is a new IMO Code to help combat cyber-crime in the maritime world.

Crime has also moved on: in the 21st century the simple theft, the stealing of property and goods seems so far in the past to the modern breed of cyber-criminals. Today's crimes against business operations are centred on intellectual theft; on the damaging corruption of electronic systems; the hacking of sensitive databases; the desire to damage both reputation and confidence in business brands and often, just the hijacking of business systems to cause mayhem and financial damage.

The cyber-criminal, the cyber-crime and the resultant thefts and damage are not confined to one industry. Maritime operations of every kind are at risk and so is the health and safety of those working on ships, offshore rigs, in office locations, in transport networks and any other operations that have network and electronic links. For shipping the risks are amplified by the very nature of its operations across the globe; away from land; reliant on electronic communications and many of the processes in shipping dependent on digital technology.

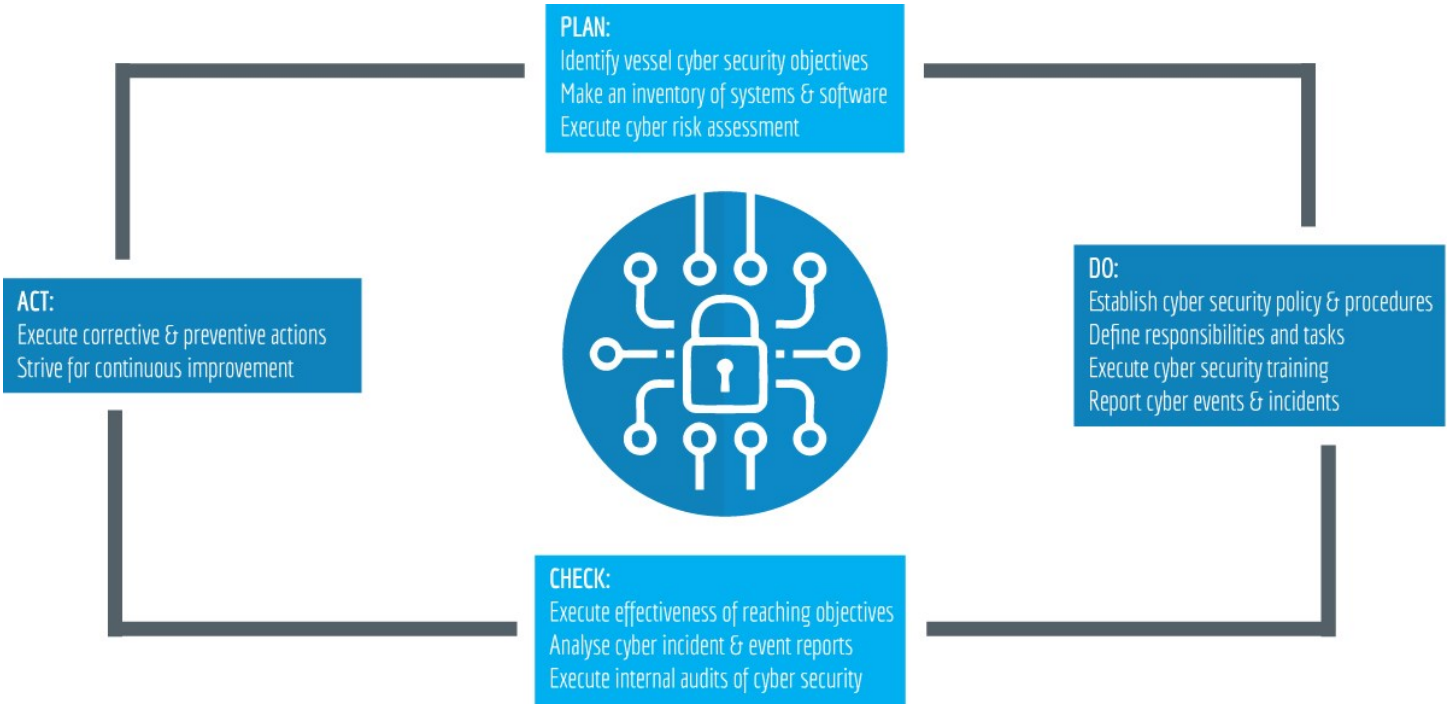
With this very much a real concern, the International Maritime Organisation (IMO) has introduced The ISM Code, supported by the IMO Resolution MSC.428(98) which will require ship owners and managers to assess cyber risk and implement relevant measures across all functions of their safety management system, until the first Document of Compliance after January 1, 2021.

This is a rallying call to the shipping world to firstly understand the risks and cyber threats and secondly, to calculate the response in terms of investment in future cyber security measures. It is a process that requires commitment from the top down: from the owners and managers across to those at the sharp end of shipping operations – the seafarers.

THE THREATS

The experts – and there are many of them in the shipping world – will tell you that it is not a matter of if you will be attacked, but when you will be attacked from a cyber-criminal. The attacks are often sophisticated and sometimes almost undetectable; simple to put into practice and yet often devastating in their deployment. One of the simplest ways of threatening and corrupting a ship's system is for an employee to open an infected email. In doing so it can cause the recipient of the targeted email to become an infected member of the maritime supply chain. This can then result in the electronic virus being downloaded and passed on through the systems associated with the ship, its land-based operations and often with financially crippling effects.

Most of these fraudulent emails are designed to make recipients hand over sensitive information or trigger malware installation on shore-based or vessel IT networks. Add into this, the threats of financial blackmail and it is hard not be alarmed by these day-to-day cyber-threats facing the maritime industry. As with the current global Covid-19 pandemic, criminals are fast to react to defensive actions and recent studies suggest cyber-criminals are now researching their targets to enable them to tailor emails for staff in specific roles. Regardless of the tactics, the threat from hacking is not going to diminish in an industry moving quickly to more remote digital operations.



WEAK SPOTS AND DANGERS

There is nothing general about cyber attacks but mainly they fall into two categories: untargeted attacks and targeted attacks, both of which are serious and preventable. An untargeted attack will seek out potential ‘cyber weak’ spots in companies and ships. A targeted attack will be one that is directed toward a specific company or ship and it can be much harder to detect and deter. The real issue is that with any of these attacks, all they need is the use of the Internet to look for and exploit weaknesses in systems.

Cyber attacks can take many forms with the most common being some of the following:

Phishing: This is often the most common cyber-crime when criminals target a mass number of people with a general message. The hope is that at least a percentage will open the message which will then allow them to hack your system to gain valuable information through email. This is the attack that is dependent on human interaction.

Malware: This is simply harmful software designed to damage a computer system without the knowledge of the owner. Other names for it are spyware, viruses, worms and trojans which embed themselves into a system. Mostly these attacks get into a system through links in emails and through visiting untrustworthy websites.

Social engineering: This occurs when cyber-criminals attempt to contact and influence people to break company and organisation protocols and supply information that could be used to damage the company through social media postings.

Subverting supply chains: An increasing danger which sees cyber-criminals attempting to compromise an organisation’s electronic systems before they reach a company or ship.

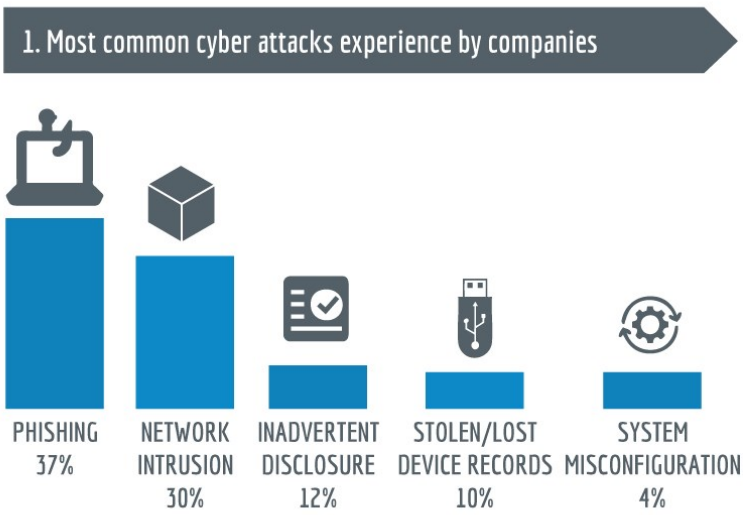
WEAK SPOTS AND DANGERS

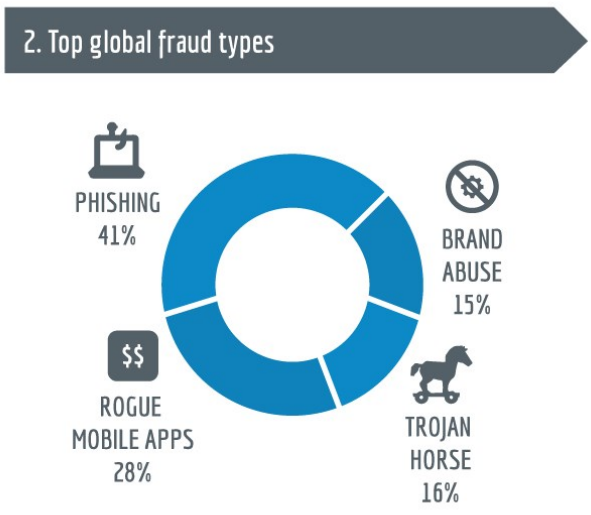
Denial of service: An early criminal technique that has been around for some time. The idea is to flood a company network with data and overwhelm the system which prevents legitimate users from accessing the programs they need. Very damaging as these attacks can take quickly control of many computers at once and infect entire servers.

Spear-phishing: This type of attack is aimed at a person or company by using personalised email requests or offering links that infect your system and then steals your valuable data. This is often called a breach.

Impersonation: A worrying trend when criminals impersonate an employee or official to gain access to your vessel or company's systems to obtain valuable information.

Identifying a cyber-attack is the first step to resolving the issue but there are certain aspects of ship operations that require more





detailed examinations. Among the most important onboard systems that need to be checked are:

- **Communication systems:** The use of Internet and satellite communications increase the vulnerability of a ship's systems and extra security and protection against cyber threats requires more than the standard provision of **safeguards.**

- **Ship propulsion and power control systems:** The world's shipping relies on electronic programs to control the ship's operations. These are particularly vulnerable to a cyber-attack and threaten the ship's controls when they are connected to remote condition-based monitoring as well as being integrated with navigational systems.

- **Ship cargo management systems:** Any system used for the loading and unloading of cargo will be vulnerable to cyber-attack due to their connections with the ship's electronic data systems.

- **The ship's bridge system:** A very vulnerable and highly prized target for cyber-attacks. The reliance on electronic navigational equipment makes them vulnerable. These risks are also of significant concern as many of them are connected to onshore servers.

- **Passenger services:** Those systems used for passenger boarding contain sensitive passenger data and much of this is collected and collated using small digital products. If there is an attack on the network server, then this data is at risk.

- **Public networks:** Although the Internet is vital for ship communications, especially when passengers are involved,

it is vital that these public connections are separate from the ship's and land-based networks as they are used for visiting unsecured networks.

In assessing the pitfalls and problems with networks and digital communications, it is also important to recognise the common flaws in many marine systems. The age and use of the ship will have a great impact on the vulnerability factors and these can include:

- Old operating systems that are no longer able to be updated
- A lack of or poor anti-malware software. It is vital that modern threats are dealt with by modern security programmes
- Poor management of employees with access to networks. Education and training are important as the first safeguards for seafarers
- Integrated computer systems that do not have safeguards and separation of network operations
- A lack of access controls for service providers and contractors who are important factors in keeping systems operational but need regulating and monitoring

SAFEGUARDING SYSTEMS

Cyber security is a critical risk area with so many ships dependent on the effectiveness of software-based systems for their operations. In general, the cyber systems for ships are classified as either IT (standard information systems) or OT (operation and control systems). There are distinct qualities and protocols for each: with IT there are usually established procedures, technology and training to avoid attacks, but any breach of an IT system can have a significant reputational and financial impact. Usually, it does not impact the safe operation of ships.

On the other hand, with OT, an attack on a ship's OT systems may threaten the vessel's operation and safety of the crew. Both systems have their weak points and cyber-criminals understand these. It is for this reason that diligence and an understanding of your vulnerabilities is of paramount importance.

To enhance general maritime cyber defences and forestall cyber threats, clear lines of responsibility for individual IT & OT systems, appropriate policy for interaction between ship and shore-based systems, established communication/alerts for cyber incidences and concerns, and appropriate cyber awareness training specific to ship installed systems must all be adopted.

BIMCO has developed the Guidelines on Cyber Security Onboard Ships, which are aligned with the NIST Cybersecurity Framework. The overall goal of these guidelines is the building of a strong operational resilience to cyber-attacks. To achieve this goal, maritime companies should follow these best practices:

- Identify the threat environment to understand external and internal cyber threats to the ship
- Identify vulnerabilities by developing complete and full inventories of onboard systems and understanding the consequences of cyber threats to these systems

- Assess risk exposure by determining the likelihood and impact of a vulnerability exploitation by any external or internal actor
- Develop protection and detection measures to reduce the likelihood and the impact of a potential exploitation of a vulnerability
- Establish prioritized contingency plans to mitigate any potential identified cyber risk
- Respond and recover from cyber incidents using the contingency plan to ensure operational continuity

THE IMO RESPONSE

In response to the growing threats from cyber-crime in the maritime world the IMO has been on the case for the past three years. The IMO has introduced the ISM Code and in combination with the resolution, the IMO also released guidelines on Maritime Cyber Risk Management (MSC-FAL.1/ Circ.3) in July 2017. In respect of this code there is still some uncertainty among ship owners and operators as to the correct actions to take, particularly as the regulations leave much of the interpretation to the company responsible for the safety management system.

Ship owners need to ensure they comply with the IMO requirements and recommendations to combat cyber-crime and remain in-step with the IMO Code. Here the IMO agreed that cyber risk management should be integrated into existing management systems under the ISM Code and ISPS Code. This means ship owners need to act on the PDCA processes (PDCA =plan–do–check–act or plan–do–check–adjust) which is an iterative four-step management method used in business for the control and continuous improvement of processes and products.

MAKING PLANS

For any ship owner the first step is to have a recognised plan that identifies cyber-security objectives that are relevant for safe ship operations. These checks and balances should also encompass anyone connected with the ship's operations, both in-house and external. It is also vital to create an inventory list of all safety and business-critical systems and software which will be needed in the first instance to define and create a cyber risk assessment.

Cyber-attacks can take so many forms that it is challenging to define the processes they use or the targets for each vessel. But the initial assessment of any cyber-threats should consider the following issues:

- What will the loss of confidentiality, integrity and operation of each system cause in terms of operational and financial terms?

- How vulnerable is the system that could be targeted and how many times could it be attacked?

Defining the cyber-security risks and ranking them in terms of damage and potential actions

As with any land-based crisis management plan, there should be a similar one for dealing with attacks and implementation on ships and offshore installations. Despite the fact they are at sea, they are as vulnerable as any other operational location to a cyber-attack.

There should be a defined and easily accessible security management plan with a defined cyber security policy with defined levels of authority. All those at sea (and working in land-based offices) need to understand the lines of communication between those on land and those working at sea. No matter what level these people are at, they should all understand the procedures for

MAKING PLANS

checking, monitoring, reporting and preparing for any cyber incidents.

According to one maritime body these systems that need checking and monitoring on a regular basis should include:

- The evaluation of the success in meeting defined cyber security objectives
- An analysis of a cyber incident and event reports
- The careful evaluation of all logs, reports and notifications, along with the operations of fitted intrusion detection systems
- The use of internal audits dealing with cyber-security
- The execution of cyber-security response drills when operated because of an attack

CONCLUSION

The importance of compliance with the new IMO requirements will be of even greater importance as 2021 begins. To achieve peace of mind and more importantly, to be certain your vessels are cyber-secure, everyone connected with your maritime operations needs to understand the importance and threat levels in these issues.

Land based and your ships should have a cyber-security plans that will identify the external and internal threats in all operational systems. There will always be vulnerable parts in operations but by identifying them and understanding how cyber -criminals might use them to gain access to systems or information, then it will be easier to plan your defences.

Consider the exposure of your vessels and installations to attacks along with the impact in terms of operational and financial stability. Cyber criminals can destroy your business as well as causing disasters to both equipment and personnel: these are avoidable with the right assessment, plans and people who can control the threats.

As we move into a new era for shipping: one with remote operations and interconnectivity in every aspect of maritime performance, it is no longer simple enough to watch the ships leave port and hope they make it to their destinations on time and in good condition.

The threats from cyber-criminals will only grow and we all need to take a real interest in what they are looking for in maritime operations – and prevent any damaging breaches that can sink your business.

GLOBAL MARITIME CONSULTANTS GROUP

About Us

Established in 1988, Global Maritime Consultants Group (GMCG) provides expert technical, legal, training and management consultancy for diverse stakeholders in the shipping and offshore sectors.

With offices and agents in over 100 cities and ports around the world, we serve national and international clients from ship builders, owners, agents and seafarers, to offshore operators, to bankers, underwriters and lawyers with an extensive portfolio of professional maritime services.

Our Mission Statement remains:

To uphold exceptional quality of service in delivering progressive and exact professional, technical and operational solutions to the maritime industry.

Values:

Motivation

Supporting all our people to bring energy and enthusiasm to their daily work

Ownership

Empowering all our people to take ownership of their actions and sharing the fruits of success.

Values

Encouraging and rewarding honesty, loyalty, hard work and sincerity.

Enterprises

Empowering and rewarding innovative thinking, and drive to design and deliver services that exceed customer expectations.

CONTACT US

HEADQUARTERS OFFICE

Zenas Kanther 2B, Alta Building, Ag. Triada 3035, Limassol, Cyprus
admin@gmcg.global
Tel: +357 25 747638
Fax: +357 25 747894

CHINA

SHANGHAI Suite 2006, Shanghai Rui Feng International Tower, No.248, Yangshupu Road, Shanghai, 200082, China T: +86 21 6886 0181, F: +86 21 6886 0182 shanghai@gmcg.global
DALIAN Suite 2203, Friendship Building No. 158, Friendship Road, Dalian, China T: +86 411 3982 2783 dalian@gmcg.global

EGYPT

ALEXANDRIA 26 (B) Fawzy Moaaz St., Office No. 903, Mefco Helwan Building, Smouha, Alexandria, Egypt T: +20 3 425 0155, F: +20 3 425 0955 alexandria@gmcg.global

GHANA

ACCRA GMCG-DAVCON,P.O BOX KN 257, Kaneshie - Accra, Ghana Tel: +233-541439943 accra@gmcg.global

GREECE

PIRAEUS 4-6 Efplias Street, 18537 Piraeus, Greece T: +30 2104293837, F: +30 2104293502 piraeus@gmcg.global

GUYANA

GEORGETOWN Lot 162-163 Lamaha Street North Cummingsburg, Guyana T: +592 503-9991 +592 659 7357 georgetown@gmcg.global

INDIA

COCHIN 1st Floor, CICFS, Old Aanavathil Junction, ICTT Road Udyogamandal P.O, Kalamassery, Cochin Pin: 683501, India T: +91 484-2555939 , F: +91 484-2986023 cochin@gmcg.global
MUMBAI Mayuresh Cosmos Building, Office No 502 Plot No 37 Sector-11 CBD BELAPU R Navi Mumbai-400614 T: +91 22-497 01399 mumbai@gmcg.global

MIDDLE EAST

LEBANON BEIRUT New Rawda, Park St.Lazar Block M, Beirut-Lebanon T: +961 76723 982 middleeast@gmcg.global

NIGERIA

LAGOS 9B, Elegba Festival Drive, Oniru Victoria Island, Lagos, Nigeria T: +234 14627 759, F: +234 14627 758 lagos@gmcg.global

PANAMA

PANAMA CITY 50th Street Global Plaza Building 20th Floor Suite D & E , Panama City, Panama T: +507 2132260 , F: +507 2132264 panama@gmcg.global

ROMANIA

Mircea cel Batrin, Nr 14,1st Floor, Room 13, Constanta, Romania Tel: +40 726 380 900 constanta@gmcg.global

RUSSIA

MOSCOW Zolotorozhsky Val h.32, Building 2, 3rd Floor Office 310, 111033, Moscow, Russia T: +7 495 926 2357, F: +7 495 926 2358 moscow@gmcg.global

SINGAPORE

21 Woodlands Close #05-28 Primz Bizhub Singapore 737854 Tel: +65 6 2232203 Fax: +65 6 2262621 singapore@gmcg.global

SRI LANKA

COLOMBO Level 12 Parkland Building, No.33 Park Street, Colombo 2, Sri Lanka T: +94 11 258 1134 colombo@gmcg.global

UAE

DUBAI M-7 Wasl AL Mamzar Bldg, AL Mamzar Street P.O. Box 14751, Dubai, UAE T: +971 4 296 5595 T: +800 472 823 (Toll free), F: +971 4 296 5597 dubai@gmcg.global

USA

FLORIDA 2645 Executive Park Drive, Suite 509, Weston, FL 33331 USA T: +1 754 217 3851 miami@gmcg.global