

MARITIME SAFETY COMMITTEE
95th session
Agenda item 4

MSC 95/4/1
5 March 2015
Original: ENGLISH

MEASURES TO ENHANCE MARITIME SECURITY

Industry guidelines on cyber security on board ships

Submitted by ICS, BIMCO, INTERTANKO and INTERCARGO

SUMMARY

Executive summary: This document informs about the ongoing work to develop industry guidelines on cyber security on board ships and outlines the content of these guidelines

Strategic direction: 6.1

High-level action: 6.1.1

Planned output: 6.1.1.1

Action to be taken: Paragraph 20

Related document: MSC 94/4/1

Points which we must and can intervene

Background

1 In their submission (MSC 94/4/1), Canada and the United States recommended the development of voluntary guidelines on cyber-security practices to protect and enhance the resiliency of cyber systems supporting the operations of ports, vessels, marine facilities and other elements of the maritime transportation system.



2 In response, BIMCO advised the Committee that it had been working with partners on guidance for shipowners and ships' crews on operational aspects of cyber security and as this work was ongoing, committed to providing an update to MSC 95.



3 The industry guidelines on cyber security on board ships are, as the working title indicates, mainly focusing on providing guidance to ships and will also address cyber-security issues for the shore-side organization where relevant.



4 The co-sponsors believe that the guidance will help to introduce safe practices on board ships, which will help to avoid damage to ships and systems. If ships' officers, for example, identify a risk of introducing a virus to the Electronic Chart Display and Information System (ECDIS) via the onboard networks, they will be able to introduce safe practices to



avoid this taking place. Further, the safety management system should ensure that a contingency plan is in place so that the ship can also be navigated safely, even if a virus disrupts the functions of the ECDIS.



5 It is also recognized that perpetrators may use a ship to launch a cyber attack against companies ashore, authorities and other stakeholders by exchanging electronic data directly with the ship.



Risk scenarios

6 The purpose of the industry guidelines on cyber security on board is to provide methods of establishing risk-based measures for owners, managers and seafarers on maritime cyber security.



7 The threats to computer systems come in many different forms. Today, some of the most common threats consist of software attacks, theft of intellectual property, theft of equipment or information, sabotage, and information extortion to steal money. Viruses, worms, phishing attacks, and Trojan horses are a few common examples of software attacks.



8 The exchange of electronic data between ship and shore has increased significantly in the past decade. The shipping industry's use of remote monitoring of systems, diagnosis and remote maintenance will continue to increase, as will the information exchange between ships and authorities, service providers, charterers and owners/operators.

9 The augmented use of electronic data exchange increases the likelihood of cyber-attacks in variety, frequency and sophistication. These may be from a USB stick that introduces malware aimed at acquiring sensitive commercial information, from an email with detailed ship itineraries sent to unknown people, to the full-scale subversion of a company's shore-based IT system, or the potential compromising of systems on board ships. The number of potential risk scenarios is significant and keeps growing. Criminals employ whichever hacking technology is the most applicable and often tailor it to specific targets.



10 Some organizations, ships and systems may be more at risk than others, depending on the type and value of data they store. However, experience has shown that criminals will generally gravitate toward the easiest parts of a potential victim's network, and choose systems which can be easily breached or accessed. As such, it is essential that companies prepare for a cyber attack and expeditiously address identified vulnerabilities both ashore and on board ships.



11 Onboard systems can be compromised by different sources and on different occasions during their lifetime:

- .1 When there is no control over who has had access to the onboard systems. This could, for example, happen during dry-docking or when taking over a new ship.
- .2 When insiders, e.g. seafarers or service personnel either deliberately or by mistake upload malware into systems via direct access to the onboard systems.
- .3 Through remote access.



12 During dockings, upon delivery of a newbuilding or when taking over used tonnage, it is impossible to know if malicious software has been left in the onboard systems. All systems should, therefore, be considered uncontrolled at time of takeover and all such uncontrolled systems should be examined and reset before they can be classified as controlled.

13 The internal cyber-threat is significant and should not be underestimated. Therefore, an urgent priority for companies is to be fully aware of what information they have on their systems, who has legitimate access to it and who is actually accessing it and why. Employees, even with the best of intentions, can be careless, for example by using USB sticks to transfer data from computer to computer without taking preventive precautions; data can be mishandled and files disposed of improperly.



14 Anyone can be tricked into divulging confidential information or authorizing what turns out to be a fraudulent disbursement. Common tactics used are phishing and spear phishing emails. The goal of these is to get victims to open attachments or click on links in an email. While the phishing approach is more scattershot, spear phishing generally focuses on specific people within an organization. Attackers might comb social media sites such as LinkedIn or Facebook to impersonate senders, who are either well known to recipients or otherwise considered trustworthy. Once the victim opens the attachment or clicks on the link, malware or ransomware may be introduced.



15 A standalone computer with no access to a network is a safe computer. Unless it has a very specific and limited purpose, it would also be rather useless. Most computers on board, be they personal computers, control computers and even programmable logic controllers (PLCs) will therefore be connected to a network. Remote access and access by insiders to internal networks on board call for a network security policy as part of a risk-based framework. The risk-based framework will describe the architecture of the onboard networks and include a policy for data access, web browsing, use of passwords, encryption and use of email as well as access by service providers, system monitoring, etc.



16 The guidelines for owners, managers and seafarers on how to mitigate maritime cyber-security risks is based on risk management. It should be kept in mind that increased levels of cyber security come at the price of having to potentially modify business processes, which may result in more complicated daily operations. The larger the risk, the more effective the mitigating measures that should be implemented.

17 A brief outline of the industry guidelines on cyber security on board ships can be found in the annex.

Further work

18 The industry guidelines on cyber security on board ships will be progressed during 2015 and it is the intention to submit the finalized guidelines to MSC 96 for the consideration of the Committee.

19 The co-sponsors are aware that the implementation of e-Navigation solutions will need to consider cyber-security issues. It is hoped that these guidelines may help to avoid duplication of work and to avoid possible future confusion.




Action requested of the Committee







20 The Committee is invited to consider the foregoing in addition to the information set out in the annex and take action as appropriate.

ANNEX

GUIDELINES ON CYBER SECURITY ON BOARD SHIPS

The industry guidelines on cyber security on board ships will include guidance on the following:

- 1 Awareness and education for all stakeholders
 - .1 Establishing awareness of why owners, seafarers and other stakeholders should spend time and attention on cyber security is essential.
 - .2 Guidelines for the personal use of email, software, and social media to keep sensitive information in safe custody must be addressed. For example, information about cargo or a ship's movements may be of interest to criminals. So it is essential for cyber security that everyone concerned is educated on how to avoid such vital information being intercepted. 
 - .3 Further, education and training should address software systems which are critical to the safety of the ship such as navigation, steering control, communication and cargo systems and how to protect them against introduction of malware. Safe use of such systems in manual mode must be trained. 
 - .4 Education and training should be tailored to the appropriate levels for:
 - Master, officers and crew
 - Organization including management ashore
 - Major stakeholders in the supply chain such as charterers, classification societies and service providers
- 2 A generic risk-based framework drawing on existing standards and guidelines augmented by current intelligence and best practice
 - .1 Cyber security in a business like shipping must be based on risk management. Risk management is the ongoing process of identifying, assessing, prioritizing and responding to threats in order to minimize monitor and control the probability and/or impact of unfortunate events. 
 - .2 To manage risk, seafarers and owners should understand the probability that an event will occur and the resulting impact. With this information, they can determine an acceptable level of risk for when to take action. Risk can be handled in different ways, such as mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, all of which depend on the potential impact to critical services.
 - .3 The risk management process will make it possible to inform and prioritize decisions regarding cyber security, and support recurring risk assessments and validation of business drivers to help select and target essential cyber-security activities. Those on board and the organization ashore need to develop a risk-based cyber-security framework. The framework should rely on a variety of existing standards, guidelines, and practices to ensure the resilience of critical infrastructure providers.

- .4 Some organizations may choose to engage an expert to conduct penetration testing and a thorough review of security protocols to determine the sensitiveness of data; where that data is and where it goes; and what processes are utilized and why. 
- 3 Cyber systems (business critical and ancillary delivery systems) addressing their integrity, confidentiality and availability
- .1 Integrity involves maintaining the consistency, accuracy, and trustworthiness of data (software integrity) both when stored on board but also when transmitted to and from the ship. Steps must be taken to ensure that data cannot be altered or intercepted. 
- 4 Establish clear guidelines on the management of key information in order to retain operational cyber capability
- .1 Key information should be protected and kept confidential. In order to ensure confidentiality, measures have to be taken to protect sensitive information from reaching unauthorized people.
- .2 Access must be restricted to people authorized to view the sensitive data in question. In order to make this effective, data needs to be categorized according to the risk of damage that could occur if criminals obtained access to the systems on which the data resides. Mitigating measures should be more or less stringent according to these categories. Accessibility to systems is imperative on board a ship and hardware should therefore be maintained and repaired quickly when so required. Furthermore, operating system environments should be kept up to date and held free of software conflicts. 
- 5 How to integrate elements of both physical and software security to ensure safety and business continuity
- .1 The physical implementation of security measures deals with how to manage hardware and internal networks in a way which ensures that they operate within a controlled environment. Also software version control should be used to prevent erroneous changes or accidental deletion. In addition, it may be necessary to have systems in place, which can detect any changes in data stored in the system. 
- 6 Importance of identifying and mitigating third-party interfaces that could compromise cyber security
- .1 In a business environment such as shipping, access to onboard systems is granted to various stakeholders. Suppliers and contractors are a risk because often they have intimate knowledge of the ship's operations as well as access to key information systems. They can also unwittingly introduce malware where their systems intersect with those of the ship. 
- .2 Recovery after malfunctions is essential and worst case scenarios should be included in the planning process of onboard systems. Protection measures such as firewalls and proxy servers are tools which can be used to avoid attacks and downtime. 

- 7 The consideration of cyber-security monitoring systems and network management
- .1 The monitoring and management of systems is important in order to ensure that the information technology staff, in conjunction with the teams in the organization ashore and on board the ship, are aware of the status of the network(s). If a system is compromised, this will then help isolate exactly what happened and when, which in turn will assist recovery efforts.
 - .2 Network management also addresses the necessary redundancy to retrieve lost data in accordance with the frequency of server backups and data preservation time.
- 8 Development of contingency plans
- .1 Contingency plans should always be available in case of a security incident. The simple fact is that no one is immune to an attack. Unfortunately, without such a contingency plan, decisions can be made that inadvertently compromise evidence and make recovery work immeasurably harder when trying to resolve matters. These plans should be constantly evolving and tested.
 - .2 When an information security issue is discovered, the proper response depends on first ascertaining:
 - When did the security breach occur? Is it still happening?
 - Where did it originate – internally or externally?
 - How and why did the incident occur? For example, did a malicious intruder exploit network access privileges to steal data for financial gain, or did an employee accidentally disclose sensitive information via email?
 - What was compromised – intellectual property, personal data, network operations, etc.?
 - How can an attack of this nature be avoided in the future?
 - .3 To avoid spreading malware throughout the network or destroying the trail of evidence, the organization and its IT department should not try to "fix" a suspected problem on their own without the assistance of experts. Experienced cyber-security investigators are skilled in conducting interviews and retracing the behaviour of people who had access to protected information. Likewise, computer forensics and data recovery specialists may help to ensure no digital evidence is overlooked and can assist at any stage of a digital forensics investigation or litigation.
 - .4 As time is of the essence when a breach is uncovered or suspected, establishing a relationship with an incident partner before a cyber attack occurs ensures quicker response time.
 - .5 When a security incident involves systems which are critical to the safety of the ship such as navigation, steering control, communication and cargo systems, the contingency plan must take into account how to operate those systems in manual mode.

9 Continued review and assessment of cyber systems to ensure their continued robustness.

- .1 Cyber-security systems should be reviewed and assessed in order to check their robustness to handle the current level of cyber-security threats. New threats are evolving all the time, so new protection measures and new procedures may have to be developed either by IT department or experts.