Cybersecurity
Guidelines for Shipowners

Cybersecurity elements as a part of ship safety management. Guideline on implementation of cyber-secure oriented procedures.

PRS
1936

As per requirements of IMO resolution MSC.428(98), starting from January 1st, 2021 new IMO requirements, concerning verification of implementation of cybersecurity issues both in shipowner's office and on board of ships enter into force. Requirement of checking whether the procedures are implemented properly, cyber risk analysis has been performed and various means of mitigation of cyber-attacks and user's imperfection have been applied, IMO decided to delegate to the entities being already responsible for the verification of proper implementation of the ISM Code.

Therefore, to help the Shipowners to implement the cybersecurity and at the same time to help the ISM auditors in their appraisal if cybersecurity has been properly addressed in the safety management system in office and on board, MMS Bureau prepared the below guidelines and preparatory materials.

The below instruction should give the general view on the thing that the shipowner should have done by January 1st, 2021 at the latest.

Step 1 – Determination of information value

First of all, the Company should properly begin the risk analysis by identifying the **critical information** and the **value of the information** at all. Any information may present the **great value to the hacker** wanting to compromise the system for any of various purposes, which are mainly financial ones – blackmail or stealing the data in order to sell it. At this point the procedures should also address the **proper and frequent training** of the personnel to make the employees virtually immune to attacks with use of **social engineering**.

Second thing is the identification of **the data** the Company is working with. The questions the Company should ask when identifying the matrix are:

- Are there **financial or legal penalties** associated with exposing or losing this information?
- How **valuable** is this information **to a competitor**?
- Could we **recreate this information** from scratch? How long would it take and what would be the associated costs?
- Would losing this information have an **impact on revenue or profitability**?
- Would losing this data impact **day-to-day business** operations? Could our staff work without it?
- What would be the **reputational damage** of this data being leaked?

Step 2 – Identification and prioritization of assets

Having done the above the Company needs to identify assets to evaluate and determine the scope of the assessment. This will allow to **prioritize which assets should be assessed**. Not necessarily all of the buildings, employees, electronic data, trade secrets, vehicles, and piece of office equipment needs assessment. **For each asset the following information is applicable**:

- Software
- Hardware
- Data
- Interface
- End-users
- Support personal
- Purpose
- Criticality
- Functional requirements
- IT security policies and architecture
- Network topology
- Information storage protection
- Information flow
- Technical security controls
- Physical security controls
- Environmental security

Step 3 – Identification of threats

First of all, the threat is any vulnerability that could be exploited to breach security to cause harm or steal data from your organization. While hackers, malware, and other IT security risks leap to mind, there are many other threats:

- **Natural disasters**: Floods, hurricanes, earthquakes, lightning and fire can destroy as much as any cyber attacker. You can not only lose data but servers too. When deciding between on-premise and cloud-based servers, think about the chance of natural disasters.
- **System failure**: Are your most critical systems running on high-quality equipment? Do they have good support?
- **Human error**: Does your organization have proper education around malware, phishing and social engineering? Anyone can accidentally click a malware link or enter their credentials into a phishing scam. You need to have strong IT security controls including regular data backups, password managers, etc.
- **Adversarial threats**: third party vendors, insiders, trusted insiders, privileged insiders, established hacker collectives, ad hoc groups, corporate espionage, suppliers, nation-state

Some common threats that affect every organization include:

- **Unauthorized access**: both from attackers, malware, employee error
- **Misuse of information by authorized users**: typically, an insider threat where data is altered, deleted or used without approval
- **Data leaks**: Personally identifiable information (PII) and other sensitive data, by attackers or via poor configuration of cloud services
- **Loss of data**: organization loses or accidentally deleted data as part of poor backup or replication
- **Service disruption**: loss of revenue or reputational damage due to downtime

The above may be achieved by means of such techniques as:

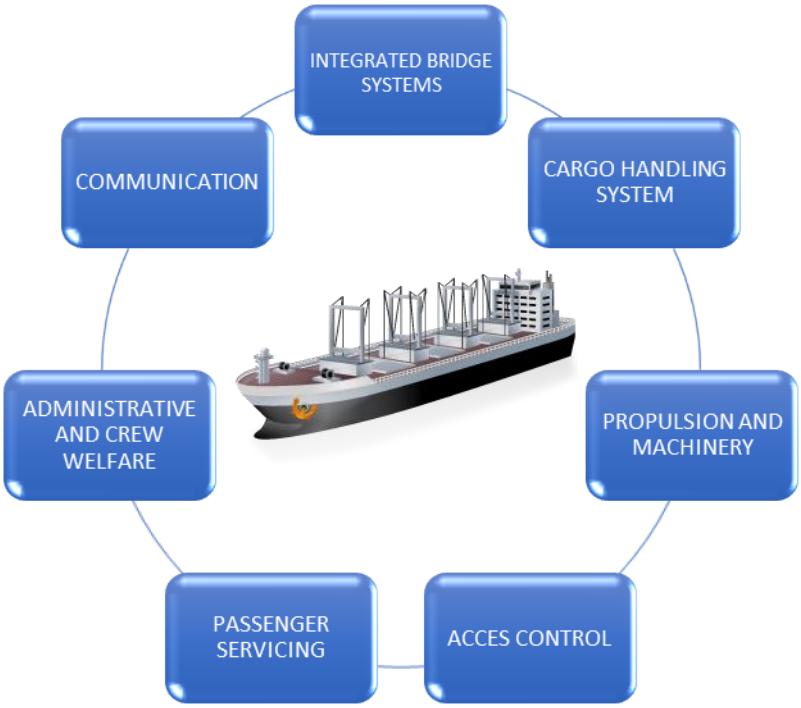
- **Phishing –** deceiving the recipients into sharing the sensitive information
- **Botnets** – any internet-connected devices, such as PC's, servers, mobile devices or any virtual devices controlled by a common type of malware,
- **Bugs** – an error, fault tor flaw in any computer program or a hardware system,
- **Insider attack** – a malicious attack perpetrated on a network or computer by a person with authorized system access,
- **Jamming** – transmission of radio signal to disrupt communication by decreasing the signal-to-noise ratio, resulting in the loss of the link's reliability, increased Energy consumption, extended packet delay and disruption of end-to-end routes,
- **Ransomware** – a malware program that infects, locks or takes control of the system and demands ransom to undo all the changes,
- **Spoofing** – fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver,
- **Spyware** – software that infiltrates and secretly monitors unsuspecting users. It can enable a hacker to obtain sensitive information, such as passwords, from the user's computer. Such spyware software is usually attached to the free online software downloads or to links that are clicked by users.

After all the threats have been identified their impact has to be assessed.

Step 4 – Identification of vulnerabilities

Nowadays ships are more and more dependent from information and communication technology. These systems are not only the crew facilitation, but also supports them and improves the comfort of work. There are some ships systems, that can be especially vulnerable for cyber-attacks.

A vulnerability is a weakness that a threat can exploit to breach security, harm the organization, or steal sensitive data. Vulnerabilities are found through strict risk analysis, audit reports, the National Institute for Standards and Technology (NIST) vulnerability database, vendor data, incident response teams, and software security analysis.



The organizational software-based vulnerabilities may be reduced with proper patch management via automatic forced updates. But there are also physical vulnerabilities – the chance of someone gaining access to an organization's computing system can be reduced by implementation of keycard access.

The most popular vulnerabilities connected to critical ships systems and possible attacks, which should be considered during Cybersecurity Risk Analysis preparation are:

1. GPS SIGNAL JAMMING
2. GPS DEVICE FAILURE OR POOR QUALITY TRANSMISSION
3. AIS DEVICE POWERED DOWN
4. AIS DEVICE MALFUNCTION
5. AIS PROGRAMMMING ERROR
6. AIS RADIO SIGNAL JAMMING
7. AIS RADIO TRANSMISSION ERROR
8. AIS VESSEL SPOOFING
    - Message injection (spoofing)
    - Message deletion (denial of service)
    - Message modification
9. AIS TRAFFIC EAVESDROPPING
10. AIS INFORMATION MODIFICATION (position, course, cargo, flagged country, speed, name, MMSI)
11. AIS SYSTEM FLOODING
12. GHOST VESSEL (the hacker modifies AIS data to create the vessel, which is physically located in different location which she really is)
13. CPA/AIS-SART SPOOFING
14. VESSEL DISAOOERABCE
15. Aids-to-Navigation SPOOFING (creating of modifying entries – buoys/lighthouses, which lead to blocking entrance to harbor, causing the ship to wreck)
16. DATA DIDDLING
17. WAETER FORECAST SPOOFING
18. MODIFYFING ENGINE PROPERTIES
    - COMPROMITATION OF THE INJECTING SYSTEM
    - COMPROMITATION OF THE “KNOCKING CONTROLLER”
    - COMPROMITATION OF THE OIL PRESSURE “DUAL FUEL CONTROLLER”
    - COMPROMITATION OF TURBO COMPRESSOR PROPERTIES
19. COMPROMITATION OF ECDIS
    - ABILITY TO READ, DOWNLOAD, REPLACE OR DELETION ANY FILE STORED ON THE MACHINE HOSTING ECDIS
    - UNAUTHORIZED ACCESS
    - INSERTION OF USB KEY
    - NOT UPDATED ECDIS - ATTACK CONNECTED WITH GPS FAILURE

Step 5 – Analysis of existing controls and implementation of new controls

Analysis of controls that are in place to minimize or eliminate the probability of a threat or vulnerability. Controls can be implemented through technical means, such as hardware or software, encryption, intrusion detection mechanisms, two-factor authentication, automatic updates, continuous data leak detection or through nontechnical means like security policies and physical mechanisms like locks or keycard access.

Controls should be classified as a preventative or detective controls. Preventative controls attempt to stop attacks like encryption, antivirus or continuous security monitoring, detective controls try to discover when an attack has occurred like continuous data exposure detection.

The example of the proper handling should come from the highest levels of organizational structures. The top management of the Company accepts the fact that cybersecurity is a very real threat and conducting a thorough risk analysis can make a hacker attack only attempt to do so.

Step 6 – Calculation of likelihood and impact of various scenarios on a per-year basis

In other words, it is assessment of the financial costs of data loss or financial loss stoppage in operation of the Company, together with the likelihood of such incident. It should have the reflection in the yearly budget of the Company.

Step 7 – Prioritization of the risks, basing on the costs of prevention vs. value of the information

Risk level should be used by senior management or other responsible individuals as a basis for determining the actions to mitigate the risk. The general guidelines:

- High risk - corrective measures to be developed as soon as possible
- Medium risk - correct measures developed within a reasonable period of time
- Low risk - decide whether to accept the risk or mitigate

Now the value of the asset has been determined and also it has been estimated how much money can be spent to protect it. The next step is to answer the question: if it costs more to protect the asset than it's worth, it may not make sense to use a preventative control to protect it. On the other hand, it needs to be remembered that there could be reputational impact not just financial impact so it is important to factor that in too.

What needs to be also considered:

- Organizational policies
- Reputational damage
- Feasibility
- Regulations
- Effectiveness of controls
- Safety
- Reliability
- Organizational attitude towards risk
- Tolerance for uncertainty regarding risk factors
- Organizational weighting of risk factors

Step by step instruction for Cyber security threat and vulnerability assessment

For this assessment, numeric rating scales are used to establish impact potential (1-6) and likelihood probability (0-5).

	Impact scale		**Likelihood scale**
1	Impact is negligible	**0**	Unlikely to occur
2	Effect is minor, major operations are not affected	**1**	Likely to occur less than once per year
3	Organization operations are unavailable for a certain amount of time, costs are incurred or organization's confidence is minimally affected	**2**	Likely to occur once per year
4	Significant loss of operations, significant impact on organization's confidence	**3**	Likely to occur once per month
5	Effect is disastrous, systems are down for extended period of time. Systems need to be rebuilt and data replaced	**4**	Likely to occur once per week
6	Effect is catastrophic, critical systems are offline for an extended period of time. Data has been lost or irreparably corrupted. Safety of people or environment is affected.	**5**	Likely to occur every day

When determining impact, consider the value of the resources at risk, both in terms of inherent (replacement) value and the importance of the resources (criticality) to the organization's successful operation.

Factors influencing likelihood include: threat capability, frequency of threat occurrence, and effectiveness of current countermeasures (security controls). Threats caused by humans are capable of significantly impairing the ability for an organization to operate effectively.

Human threats sources include:

Insiders – employees, owners, stock holders, etc.;

General contractors and subcontractors – cleaning crew, developers, technical support personnel, computer and telephone service repair crew;

Former employees – employees who retired, resigned or were otherwise terminated;

Unauthorized users – computer criminals, terrorists, intruders (like hackers or crackers) who attempt to access the organization's resources for any reason.

Human threats			Impact (1-6)	Probability (0-5)	Score (Impact x Probability)
1	Human error				
		Accidental destruction, modification, disclosure or incorrect classification of information			
		Ignorance, inadequate security awareness, lack of security guidelines, lack of proper documentation, lack of knowledge			
		Workload – too many or too few system administrators, too much workload on users			
		Users may inadvertently give information on security weaknesses to attackers			
		Incorrect system configuration			
		Security policy not adequate			
		Security policy not enforced			
		Security analysis may have omitted something important or be wrong			

2	Dishonesty, fraud, theft, embezzlement, selling of confidential organization's information			
3	Attacks by social engineering			
	Attackers may use telephone to impersonate employees to persuade users/administrators to give user name, password or any other sensitive information, such us employee ID number, initials, room number, etc.			
	Attackers may deceive or persuade users to execute trojan horse programs			
4	Abuse of privileges or trust			
	General threats	Impact (1-6)	Probability (0-5)	Score (Impact x Probability)
1	Unauthorized use of not protected computers/laptops/smartphones			
2	Mixing of test and production data or environments			
3	Introduction of unauthorized software or hardware			
4	Time bombs – software programmed to damage the system on a certain date or time			
5	Operating system design errors – systems not designed to be highly secure			
6	Protocol design errors – protocol weaknesses in TCP/IP can result in:			
	Source routing, DNS spoofing, TCP sequence guessing, unauthorized access			
	Hijacked sessions and authentication session/transaction replay, data is changed or copied during transmission			
	Denial of service (due to bombing, flooding or large packet pinging the servers, etc.)			
7	Logic bomb – software programmed to damage a system under certain conditions			
8	Viruses in programs, documents, e-mail attachments			

Identification authorization threats			Impact (1-6)	Probability (0-5)	Score (Impact x Probability)
1	Attack programs masquerading as normal programs (trojan horses)				
2	Attack hardware masquerading as normal commercial hardware				
3	External attackers masquerading as valid users or customers				
4	Attackers masquerading as helpdesk or support personnel				
Privacy threats			Impact (1-6)	Probability (0-5)	Score (Impact x Probability)
1	Eavesdropping				
		Electromagnetic eavesdropping or Van Eck phreaking			
		Telephone/fax eavesdropping (via "clip-on" telephone bugs, inductive sensors, or hacking the public telephone exchanges)			
		Network eavesdropping. Unauthorized monitoring of sensitive data crossing the internal network, unknown to the data owner			
		Subversion of ONS to redirect email or other traffic			
		Subversion of routing protocols to redirect email or other traffic			
		Radio signal eavesdropping			
		Rubbish eavesdropping (analyzing waste for confidential documents, etc.)			
Integrity/accuracy threats			Impact (1-6)	Probability (0-5)	Score (Impact x Probability)
1	Malicious, deliberate damage of information or information processing functions from external sources				
2	Malicious, deliberate damage of information or information processing functions from internal sources				
3	Deliberate modification of information				

Access control threats		Impact (1-6)	Probability (0-5)	Score (Impact x Probability)
1	Password cracking (access to password files, use of bad-blank, default, rarely changed passwords, etc.)			
2	External access to password files, network sniffing			
3	Attack programs allowing external access to systems (backdoors visible to external networks)			
4	Attack programs allowing internal access to systems (backdoors visible to internal networks)			
5	Unsecured maintenance modes, developer backdoors			
6	Modems easily connected, allowing uncontrollable extension of the internal network			
7	Bugs in network software, which can open unknown or unexpected security holes, that can be further exploited from external networks to gain access. (This threat becomes bigger and bigger with more complexity of the software)			
8	Unauthorized physical access to system			
Repudiation threats		Impact (1-6)	Probability (0-5)	Score (Impact x Probability)
1	Receivers of confidential information may refuse to acknowledge receipt			
2	Senders of confidential information may refuse to acknowledge source			

Legal threats			Impact (1-6)	Probability (0-5)	Score (Impact x Probability)
	Failure to comply with regulatory or legal requirements (e.g. to protect confidentiality of employee data)				
2	Liability for acts of internal users or attackers who abuse the system to perpetrate unlawful acts (e.g. incitement to racism, gambling, money laundering, distribution of pornographic or violent material, etc.)				
3	Liability for damages if an internal users attacks other sites				
Service reliability threats			Impact (1-6)	Probability (0-5)	Score (Impact x Probability)
1	Major natural disasters (fire, smoke, water, earthquake, storm or hurricane, power outage, etc.)				
2	Minor natural disasters of short duration, or causing little damage				
3	Major human-caused disasters (war, terrorist incident, bomb, civil disturbance, dangerous chemicals, radiological or biological accidents)				
4	Equipment failure from defective hardware, cabling or communication system				
5	Equipment failure from airborne dust, electromagnetic interference or static electricity				
6	Denial of Service				
		Network abuse – misuse of routing protocols to confuse and mislead systems			
		Server overloading (by processes, swap space, memory, temporary directories, overloading services, etc.)			
		Email bombing			
		Downloading or receipt of malicious applets, active x controls, macros, postscript files, etc.			

7	Sabotage – malicious, deliberate damage of information or information processing functions				
		Physical destruction of network interface devices or cables			
		Physical destruction of computing devices or media			
		Destruction of electronic devices and media by electromagnetic radiation weapons (EMP/T gun, HERF gun)			
		Deliberate electrical overloads or shutting off electrical power			
		Viruses or worms			
		Deletion of critical system files			

Each score from the above table has to be assessed as described below:

Score	Risk level	Risk occurrence result
1 – 10	Low risk	Occurrence may result in minimal loss of tangible assets, information, or information resources. May adversely affect the organization's operation or reputation. For example, authorized users aren't granted access to supportive data for an hour.
11 – 20	Medium risk	Occurrence may result in some loss of tangible assets, information, or information resources. May disrupt or harm the organization's operation or reputation. For example, authorized users aren't able to access supportive data for several days.
21 – 30	High Risk	Occurrence may result in significant loss of major tangible assets, information, or information resources. May significantly disrupt the organization's operations or seriously harm its reputation.

After completing a review of current security controls and along with a review and rating of potential threats/vulnerabilities, a series of actions should be determined to reduce risk (threats exploiting vulnerabilities) to and acceptable level. These actions should include putting into place missing security controls, and/or increasing the strength of existing controls.

Security controls should ideally reduce and/or eliminate vulnerabilities and meet the needs of the business. Cost must be balanced against expected security benefit and risk reduction. Typically, security remediation efforts and actions will be focused on addressing identified high-risk threat/vulnerabilities.

The below table examples of remediation activities designed to focus on the commonly identified High risk threats and vulnerabilities. Actions are ranked in priority order of effectiveness.

	Remediation action	Cost	Benefit	Risk
1	Develop a foundation of Security Policies, Practices and Procedures, especially in the area of Change Control	Low	High	High
2	Establish and enforce a globally-accepted password policy	Low	High	High
3	Address vulnerability results in order of high risk to low risk	Low	High	High
4	Establish an Operations group facilitated discussion to improve processes and communications, and to eliminate any misunderstandings	Low	High	High
5	Establish router configuration security standards, forming baseline practices	Low	High	High
6	Harden servers on the internal network	Low	High	High
7	More closely integrate worker termination activities between HR and IT. Incorporate new-hire orientation and annual security “refresher” for all employees.	Low to moderate	High	High
8	Redesign the internet perimeter, incorporating concepts of N-tier architecture and “defense in depth” into the redesign of the Internet perimeter and Enterprise Architecture	Low to moderate	High	High
9	Migrate to a more centralized and integrated model of operations management, including centralized logging, event correlation, and alerting	Low to moderate	High	High
10	Complete the intrusion detection infrastructure	Moderate	High	High
11	Install encryption on mobile computers to protect the confidentiality and integrity of data.	Moderate to expensive	High	High
12	Perform data classification to determine security levels to protect that data	Moderate to expensive	High	High
13	Institute vulnerability scanning as a regular scheduled maintenance task	Moderate to expensive	High	High
14	Reclassify email as a mission critical application	Low	Moderate	Medium
15	Complete security staffing for the ISO Security Group	Expensive	High	High
16	Complete Computer Security Incident Response Team (CSIRT) capability	Moderate to expensive	High	High

What will be checked/verified during the external audits?

Procedures referring the cyber security should as a minimum envelop:

- designation of person or persons responsible for investigation and mitigation,
- Identification of sensitive and non-sensitive data,
- process for creating retrievable backups of the vital data,
- physical control and authorization of access to facility, rooms, computers,
- training of personnel in human element based attacks (so called social engineering), keeping their passwords safe and computers protected while away,
- physical prevention or special precautions regarding use of external data storage devices (most popularly used pendrives),
- reporting and responding to cyber incidents, with the proper follow-up procedures,
- designation of person or persons responsible for investigation and mitigation,
- consideration of windows for online connection between the ship and shore terminals
- program for regular revisions of procedures and improvement plans,
- tests of the security systems and drills for the personnel.

Further information:

12 IACS RECOMMENDATIONS ON CYBER SAFETY MARK STEP CHANGE IN DELIVERY OF CYBER RESILIENT SHIPS

http://www.iacs.org.uk/news/12-iacs-recommendations-on-cyber-safety-mark-step-change-in-delivery-of-cyber-resilient-ships/

IMO GUIDELINES ON MARITIME CYBER RISK MANAGEMENT MCS-FAL.1/Circ.3

http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

BIMCO

https://www.bimco.org/-/media/bimco/about-us-and-our-members/publications/ebooks/cyber-security-guidelines-2018.ashx

Thank you and Good luck!

In case of any questions
please contact PRS
Marine Management Systems Bureau
e-mail: kz@prs.pl