CIRM Guideline

GL-002

IMPLEMENTING THE CIRM CYBER RISK CODE OF PRACTICE FOR VENDORS OF MARINE ELECTRONIC EQUIPMENT AND SERVICES

Edition 1.0
February 2020

Comité International Radio-Maritime (CIRM)
202 Lambeth Road, London, SE1 7JW, United Kingdom
Tel: +44 (0) 20 3411 8344
Email: office@cirm.org
www.cirm.org

DOCUMENT HISTORY

Version no.	Date	Details	Approved by
1.0	February 2020	First published version	CIRM Technical Steering Committee

TERMS OF USE

TABLE OF CONTENTS

INTRODUCTION

This Guideline is a companion document to Edition 1.0 of the CIRM Cyber Risk Code of Practice for Vendors of Marine Electronic Equipment and Services (the 'Code').

The aim of this Guideline is to explain how to implement the principles of the Code, by:

- directing the audience to appropriate standards, guidelines and best practice; and
- providing additional guidance where this can add value.

The following section contains specific guidance on each of the principles of the Code.

Guidance on cyber risk management for ship owners, operators and other stakeholders is already available from several sources. It is intended that, where possible, this Guideline will refer to relevant existing guidance and technical standards rather than replicating them.

CIRM firmly believes that reasonable safeguards regarding cyber risk management are an important factor to ensure that marine electronic equipment and services can be trusted.

GUIDANCE FOR VENDORS

This section contains specific guidance on each of the principles of the Code.

1. ADHERENCE TO APPLICABLE CYBER RISK STANDARDS, RECOMMENDATIONS AND GUIDANCE

1.1 Purpose

This section identifies the sources of standards, frameworks and guidelines in the maritime environment, both published and in development at the time of writing. A list of the major guidelines and standards available to support the implementation of cyber risk management in maritime electronics is provided in Appendix I.

1.2 Cyber risk standards, frameworks and guidelines in the maritime environment

1.2.1 International Maritime Organization (IMO)

In June 2017, the International Maritime Organization (IMO) adopted Resolution MSC.428(98): 'Maritime Cyber Risk Management in Safety Management Systems', which requires cyber risks to be addressed in safety management systems by 1 January 2021, based on MSC-FAL.1/Circ.3: 'Guidelines on Maritime Cyber Risk Management'.

The IMO Guidelines on Maritime Cyber Risk Management are set out in the annex of MSC-FAL.1/Circ.3 and provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and

emerging cyber threats and vulnerabilities. These Guidelines present the five functional elements that support effective cyber risk management:

.1 **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;

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

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

.4 **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;

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

According to MSC-FAL.1/Circ.3, these functional elements encompass the activities and desired outcomes of effective cyber risk management across critical systems affecting maritime operations and information exchange and constitute an ongoing process with effective feedback mechanisms.

1.2.2 International Electrotechnical Commission (IEC) technical standards

The International Electrotechnical Commission (IEC) prepares and publishes International Standards for all electrical, electronic and related technologies.

For equipment intended to be connected to an Ethernet network based on the IEC 61162-450 protocol standard, compliance with IEC 61162-460 or its principles provides further protection. IEC 61162-460 includes cyber secure methods to connect navigation instruments both within the same vessel and to shore based internet services, and authentication requirements.

General requirements for maritime navigation and radiocommunication equipment and systems will be addressed in IEC 63154, which is planned for publication in 2021. IEC 63154 will address such issues as interfaces, authentication for data access and software updates, network access and configuration management.

1.2.3 International Organization for Standardization (ISO)

The International Organization for Standardization (ISO) have initiated the process to develop a new Maritime Cyber safety standard which will be developed by TC8 / WG4 (Maritime security). The standard will provide requirements for designing, implementing, maintaining and ensuring the safety of ships operations by managing the cyber risk of operational technical systems.

1.2.4 Security Frameworks

Security frameworks are a way for an organisation to assess its cyber security maturity level.

Several security frameworks exist to support organisations in the development, delivery and maintenance of secure products and services. It is considered a core prerequisite of the delivery of secure products and services

that the delivering organisation has ensured the security of their own operations model. Several security standards and frameworks also exist to support organisations in the development of their own Information Security Management System (ISMS); the suitability of each of these will depend very much on the maturity level of the organisation from a process, technology and personnel perspective.

An example cyber maturity model is presented below and provides a series of examples of baseline measures for an organisation as part of a supply chain.

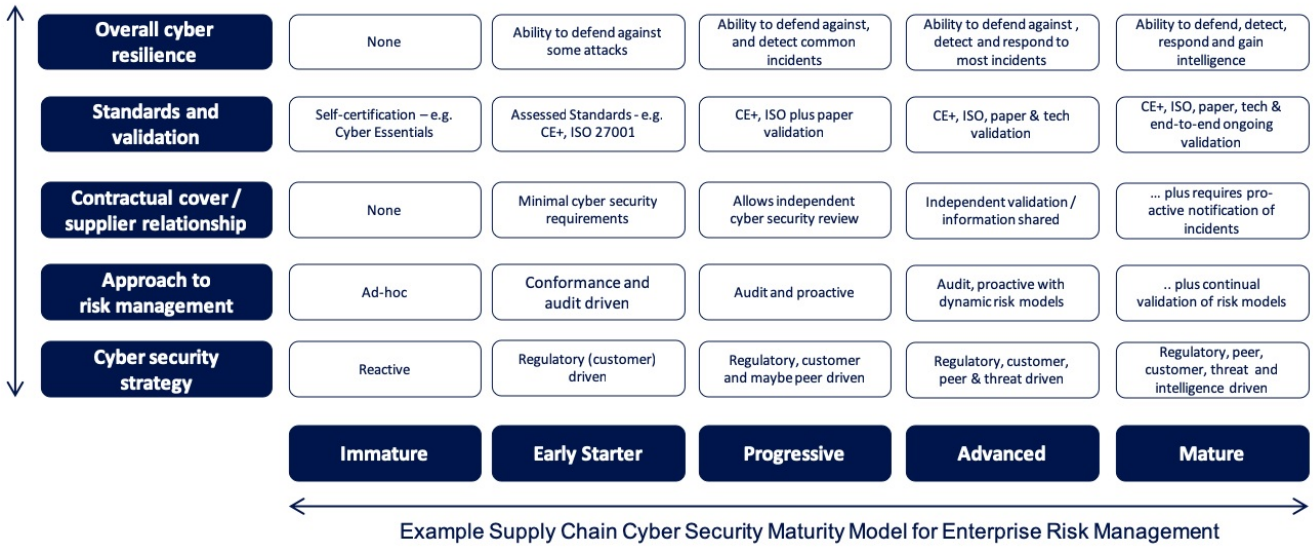

Figure 1: Cyber security maturity model

Common security frameworks include:

- **ISO/IEC 27001**: 'Information technology — Security techniques — Information security management systems - Requirements' is a standard for information security. ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation.

- **NIST Framework**: The United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the NIST Cybersecurity Framework[1]) can be used to help identify and prioritise actions for reducing cyber security risks. It is intended as a tool for aligning policy, business and technological approaches to managing cyber risks as cyber risk begins with understanding organisational risk.

  The NIST framework is one of many available frameworks. For the sake of consistency, this document will use the NIST Cybersecurity Framework and NIST Glossary of Key Information Security Terms[2] as a basis.

[1] https://www.nist.gov/cyberframework
[2] https://www.nist.gov/publications/glossary-key-information-security-terms-1

- **ENISA ISMS Framework:** The chief objective of the European Union Agency for Network and Information Security (ENISA) Information Security Management (the ISMS Framework[3]), is to support implementation of appropriate measurements to eliminate or minimize the impact that various security related threats and vulnerabilities might have on an organization. In doing so, Information Security Management enables implementation of desirable characteristics of services offered by an organization (i.e. availability of services, preservation of data confidentiality and integrity etc.).

- **Cyber Essentials / Cyber Essentials Plus:** Cyber Essentials is a scheme developed and managed by the UK's National Cyber Security Centre (NCSC), and is designed to provide a framework that can be used by organisations with limited experience of cyber security to improve their defences and demonstrate publicly their commitment to cyber security. The scheme includes two levels of accreditation: Cyber Essentials is a self-certification process, whilst Cyber Essentials Plus requires external validation by an NCSC accredited organization.

  In order to meet the requirements of Cyber Essentials, an organization must demonstrate compliance with the following five controls:

  - Use of a firewall to secure Internet connections;
  - Using the most secure settings for devices and software;
  - Controlling who has access to data and services;
  - Protecting systems from viruses and other malware; and
  - Keeping devices and software up to date.

- **Essential Eight Maturity Model:** The Australian Cyber Security Centre (ACSC) has developed prioritised mitigation strategies to help organisations mitigate cyber security incidents caused by various cyber threats. The most effective of these mitigation strategies are known as the 'Essential Eight'; they are:

  - Application whitelisting;
  - Patch applications;
  - Configure Microsoft Office macro settings;
  - User application hardening;
  - Restrict administrative privileges;
  - Patch operating systems;
  - Multi-factor authentication; and
  - Daily backups.

[3] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-isms/framework

1.3 Conclusions and recommendations

By delivering products with defined levels of cyber security and resilience, Vendors can perform their role in the chain of trust and contribute to the IMO requirement for cyber risk to be considered in safety management systems.

Organisations adhering to the Code are encouraged to stay up to date with developments in regulations and standards related to cyber security and resilience.

2. DEFAULT CYBER SECURE

2.1 Purpose

It must be assumed that there is no fully cyber secure equipment, vessel or process. There are only levels or degrees of cyber security in equipment, vessels and processes. Equipment may be put in a mode where all implemented cyber security risk mitigations are enabled, however equipment cannot be defined as invulnerable to all threats even then; it can only be considered as being in a higher cyber security mode.

This section provides guidance on approaches to building cyber security measures into products at the design stage. It looks at where the risks come from (vulnerability analysis), what product security involves, and how to build cyber security into the product development lifecycle.

2.2 Vulnerability analysis

This section focusses on the 'Identify' aspects of the NIST framework (see section 2.1.2.4 'Security Frameworks') from the point of view of Vendors. This section sets out a means to identify:

- attack surfaces and vulnerabilities within a product or system; and
- the acceptable risk levels for products and related attack vectors.

2.2.1 Sources of cyber risk

Whilst comprehensive data on cyber-attacks against marine systems and organisations is limited, a pattern of cyber risk sources can be established from those attacks that have been reported, those identified through analysis of non-cyber threats which may be enhanced using technology, and those observed across adjacent industries.

The Carnegie Mellon University Software Engineering Institutes paper: 'A Taxonomy of Operational Cyber Security Risks'[4] organizes the sources of operational cyber security risk into four classes:

- Actions of people;
- Systems and technology failures;

[4] https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9395

- Failed internal processes; and
- External events.

CIRM has identified the following additional risks:

- Secrecy / lack of sharing of information about incidents (see section 2.5.4 'Incident Reporting and Information Sharing'); and
- Physical access to equipment.

2.2.2 Threat actors

Cyber-attacks originate from groups or individuals with differing motivations and capabilities. 'The Guidelines on Cyber Security Onboard Ships', BIMCO et. al. identifies some likely threat actors, their motivations and objectives. Commercial navigation systems are not national infrastructure or defence assets and so threats originating from well-resourced nation states may be less of a concern than those from opportunists. Although cyber-criminals generally have fewer resources than a nation state, tools developed by nation states are increasingly becoming available to cyber-criminals and thus the gap between the different threat actors is diminishing.

The Not Petya ransomware attack that hit container shipping company A.P. Moller Maersk in June 2017 showed the enormous impact that one threat actor can have, and not necessarily for commercial gain. Although Not Petya was superficially related to the Petya ransomware, the motive for the Not Petya attack appeared to be to create chaos, rather than for commercial gain.

2.2.3 Threat modelling and the STRIDE model

Threat modelling provides a means to identify and analyse the security threats associated with a product or system. Threat models can be categorised by the viewpoint that they represent i.e.: attacker, asset or system.

The Attacker viewpoint frames threats from the point of view of an attacker. This approach attempts to assess the goals of an adversary and how they might be achieved. Motivations and intentions are determined from the perceived threat and then addressed. An attacker's motivations are often considered in terms such as: "A pirate wants to take control of the navigation system to make the ship more vulnerable to attack".

Models that take the Asset viewpoint identify the elements in a system that have a value and risk associated with them and consider how that value and risk may be exploited. For example, the ship and its cargo are assets that must be navigated from port to port safely.

The System viewpoint involves identifying relevant attack vectors on vulnerable subsystems of a larger system.

The **STRIDE model** is an example of this type of threat modelling; it was developed by Praerit Garg and Loren Kohnfelder at Microsoft. It provides a mnemonic to identify security threats in the following six categories:

- **Spoofing** attacks occur when an attacker pretends to be someone that they are not. For example, an attacker using DNS hijacking and pretending to be www.microsoft.com would be an example of a spoofing attack.

- **Tampering** attacks attempt to modify data toward some malicious aim. SQL injection is an example of this (see glossary).

- **Repudiation** is the denial of the truth of something. Primarily this shows up on operations like credit card transactions - a user purchases something and then claims that they did not do it.

- **Information Disclosure** threats involve an attacker viewing data that they are not supposed to view. Communication links and data stores are typically subject to information disclosure threats; if an unauthorized person can read the contents of a file, it is an information disclosure breach.

- **Denial of service** attacks prevent legitimate and authorised users from accessing information, usually by flooding a network with data.

- **Elevation of privilege** is the act of exploiting a flaw in a system that gives someone more rights than intended. It allows deeper access into the system thus exposing services and data.

2.3 Product security

2.3.1 Balance between safety, usability and security

The balance between safety, usability and security is an important design consideration for manufacturers and integrators. The ideal outcome is to deliver products and systems that allow users to do their jobs quickly, easily and safely, without leaving them open to cyber-attacks. Unfortunately, in practice, safety, usability and security are not necessarily mutually compatible. For example, from a user experience perspective, a system with little or no authentication requirements is generally easier and more pleasant to use than one with more stringent requirements. If security measures make a product or system complicated or difficult to use, then users may avoid using it or find less secure ways to use it. However, from a security perspective it is important to ascertain that only authorized users have access to the system.

The study of the link between user experience and information security is known as HCISec (Human Computer Interaction and Security). A key finding of this work is that product designers, usability and security experts should work together at the design stage to develop products that have security measures with good usability built in, rather than adding security as a separate module afterwards.

2.4 Secure Development Lifecycle

A Secure Development Lifecycle (SDLC) is broadly recognised process for the development of products, be they systems or software, in a secure fashion. Whilst there exists a range of individual SDLC implementations with variations in terminology, there is a broad consensus around the primary stages at which security considerations should be embedded into the development process; these are generally considered to be:

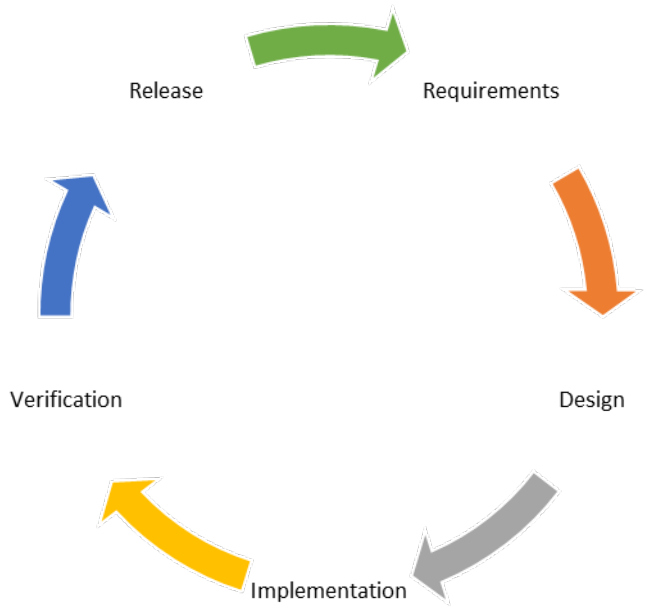

Figure 2: Primary Stages of a Secure Development Lifecycle

- **Requirements**: For a system to be considered 'Secure by Design', the requirements analysis phase considers the general and specific requirements for security within the system. Data, both user and system, in use in the system should be considered in the context of its need for confidentiality, integrity, and availability.

  During the requirements analysis phase, minimum acceptable levels of security and privacy quality should be defined to help those teams developing the product to apply standards through the lifecycle of the project.

- **Design**: During the design phase of the product lifecycle, the security aspects of the product should be considered alongside the function design aspects. This is primarily achieved using threat modelling, which maps functional components into trust zones with the risks to data transiting trust boundaries assessed against the security requirements for that data.

- **Implementation**: Embedding security during the implementation phase includes the identification and use of tools, processes and languages which embed security into the product. By identifying methods of development that embed security, be that at the method, language, or framework level, the security of data across the whole produce can be enhanced.

  Requiring the use of secure actions, such as encryption, by default will help to prevent accidental use of insecure methods of working, and continual assessment of the product through static analysis will help to identify potential vulnerabilities whilst they can be more easily remediated.

- **Verification**: During the verification phase, quality assurance processes are used to help ensure that the correct product has been built (verification) and that it has been built correctly (validation). By utilising test cases to measure the product against the security requirements identified previously, the product can be assured. The use of dynamic analysis, attack surface review, and penetration testing are recommended for the assurance of a product alongside the functional testing process.

  External verification of a product regarding functional and security requirements will provide further assurance of a product's readiness for release.

- **Release**: Once a product has been released, it is essential that security remains a focus of the post-release activity. An incident response plan to respond to reported vulnerabilities, and a robust maintenance and update process will provide surety that the product will remain secure post-deployment.

Stages for Training and Response are often included at the start and end of the cycle respectively.

2.5 Robust positioning, navigation and timing

Spoofing and jamming incidents that have already happened throughout the world point to the potential for attacks to ships on their positioning and navigation systems. Such actions can lead to piracy, theft, fraud, collisions, accidents, loss of property and life.

The IMO Maritime Safety Committee (MSC) has approved an MSC circular on 'Guidelines for shipborne position, navigation and timing (PNT) data processing' (MSC.1/Circ.1575), which provides guidance on enhancing the safety and efficiency of navigation by improved provision of PNT data to bridge teams (including pilots) and shipboard applications (e.g. AIS, ECDIS, etc.).

IMO PNT data processing or other intelligent means may be used to monitor sensors and data sources to provide a consistent and resilient ship data set. This supports measures against jamming and spoofing of data.

2.6 Account management

Vendors should be transparent with their customers with regards to the accounts present on equipment and systems. If accounts are needed for capabilities such as remote maintenance, the presence and use of such accounts should be subject to awareness and agreement with the customer. Vendors are encouraged to establish effective management processes for managing user privileges and limit the number of privileged accounts. User privileges should be limited to those that are appropriate for their role. This principle is sometimes referred to as 'least privilege'. The carefully controlling, management and granting of highly elevated system privileges support these principals.

2.7 Documentation and training guides

Documentation and training should identify proper operation with relation to security and highlight modes of operation that could leave the product vulnerable for the installer, support engineer, and operator.

2.8 Supply chain hardening

Additional cyber security measures could address the supply chain, supplementary to existing supply chain controls such as counterfeit measures, incoming quality control measures, supplier audits etc.

Resources to support cyber risk management for supply chains could include but are not limited to:

- NIST's Technology Cyber Supply Chain Risk Management Project[5]
- The UK's National Cyber Security Centre's Supply Chain Security Guidance[6]

2.9 Conclusions and recommendations

It is preferable that cyber security is built into products at the design stage rather than added on afterwards. Making a product or service cyber secure by default involves understanding the risks and vulnerabilities and considering them in the design and development of products.

Organisations adhering to the Code are encouraged to:

- conduct vulnerability analysis on their products and services to identify sources of cyber risk and threat potential threat actors;
- use threat models such as STRIDE to identify potential threats in the design, development; installation and support of marine electronic products and systems;
- consider how security can be incorporated into all stages of the product development lifecycle;
- be transparent with their customers with regards to the accounts present on equipment and systems; and
- choose, implement and use a Secure Development Life Cycle model to ensure that appropriate security is maintained in their products.

3. CONFIDENTIALITY

3.1 Purpose

Confidentiality is defined in ISO/IEC 27000:2017 clause 2.12 as "property that information is not made available or disclosed to unauthorized individuals, entities, or processes".

This section sets out the elements which Vendors are encouraged to consider in order to ensure that customer's data and information related to cyber security and cyber security events remain confidential.

[5] https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management
[6] https://www.ncsc.gov.uk/collection/supply-chain-security

3.2 The '3Ps' of confidentiality

To achieve and maintain confidentiality, Vendors should address the '3Ps': People, Processes and Products:

- **People** should be provided with adequate, appropriate and relevant training on why and how to maintain confidentiality and which information it is necessary to keep confidential;
- **Processes** should be in place in the company to define which information is to be handled on which level of confidentiality; and
- **Products** should be able to support the level of confidentiality that is needed. e.g. ensuring that products do not leak information to third parties or contain undocumented backdoors, allowing unauthenticated access.

3.3 Conclusions and recommendations

Organisations adhering to the Code are encouraged to ensure that staff training, and company processes are in place, and products are fit for purpose to ensure the confidentiality of customers' information and data.

4. QUALITY AS THE FOUNDATION FOR CYBER RISK MANAGEMENT

4.1 Purpose

A Quality Management System (QMS) can be considered an essential foundation for cyber risk management as it creates a quality framework within which cyber risk management can be identified as an objective in the design, development and delivery of products and services.

4.2 Definition of a QMS

One example of a QMS is ISO 9001:2015[7], an international standard specifying requirements for QMS, and the most prominent approach to QMS.

A QMS is defined in ISO 9001:2015 as follows:

- A QMS comprises activities by which the organization identifies its objectives and determines the processes and resources required to achieve desired results;
- The QMS manages the interacting processes and resources required to provide value and realize results for relevant interested parties;
- The QMS enables top management to optimize the use of resources considering the long- and short term consequences of their decision; and

[7] Available at: https://www.iso.org/standard/45481.html

- A QMS provides the means to identify actions to address intended and unintended consequences in providing products and services.

4.3 Conclusions and recommendations

Organisations adhering to the Code are encouraged to use a QMS which is compliant with the principles set out in section 2.4.2.

5. SOFTWARE UPDATES AND VULNERABILITY HANDLING

5.1 Purpose

This section considers the ongoing cyber risk management handling of equipment which has already been installed and is in operation on a vessel. It sets out approaches to product and system maintenance in the maritime environment. It also looks at what is required to ensure that Vendors are made aware of vulnerabilities in their products.

5.2 Product and system maintenance

The software maintenance activities recommended for Vendors are set out in the CIRM / BIMCO Industry Standard on Software Maintenance of Shipboard Equipment support cyber security[8].

The marine environment creates specific challenges for maintenance of shipboard equipment. The following should be considered in mitigation of these challenges:

- Preferably alternative routes for ship/shore data connections should be available, e.g. dual or redundant satellite communications systems, to mitigate the risk of slow or unstable connectivity;
- Users should be able to set a schedule or a specific time for updates to be applied, as automatic updating may be inappropriate; and
- If applicable, due care must be taken to ensure that continuous or automatic virus screening and removal does not result in reduction of performance, equipment malfunction or loss of type approval.

5.3 Responsible Disclosure

The International Standard ISO/IEC 29147: 'Information technology - Security techniques - Vulnerability disclosure' provides guidelines for Vendors to be included in their business processes when receiving information about potential vulnerabilities and distributing vulnerability resolution information.

[8] Available at: http://cirm.org/publications/industry_standards/Industry%20Standard%20on%20Software%20Maintenance%20of%20Shipboard%20Equipment%20v1-0.pdf

5.3.1 Responsible Disclosure of Vulnerabilities to the Vendor

Across the technology industry, best practice has been established that Vendors implement a clearly defined process which allows researchers, testers, and customers to report potential vulnerabilities in their products. Doing this has very clear advantages for an organisation. Security researchers and third-party testing organisations will have policies that require them to disclose vulnerabilities to Vendors in a responsible manner. If, however, contact attempts go unanswered, there is an ambiguous response, or the Vendor refuses to engage, then it may be appropriate for vulnerability information to be released in the public interest, such that customers are able to put in place their own workarounds or mitigations.

5.3.2 Responsible Disclosure of Vulnerabilities to Customers

Where a security vulnerability is identified in a product which could present a threat to a customer's systems or data, a Vendor has a responsibility to inform the customer how to mitigate the threat within a reasonable period, e.g. by giving instructions on how to protect the equipment or providing a security update. Where a vulnerability is already exploited in the field then the priority is to inform to customer; where the vulnerability has not been exploited then there is an argument for taking the time to create and deploy a fix before releasing any details.

Regardless of the exact circumstances of the situation, it remains a responsibility of any Vendor to ensure that they release information relating to security vulnerabilities to their customers when it could impact the customer's own cyber risk assessment. This does not necessarily require technical details or detailed reproduction steps; it is possible to provide customers with enough information to assess risk without giving details on how to exploit the vulnerability.

5.4 Conclusions and recommendations

Products require ongoing protection after deployment to ensure that they are protected from emerging threats. Cyber risk protection for ship systems must be tailored around the maritime environment. Not all land-based solutions or concepts are easily applied to the maritime environment without modification.
Organisations adhering to the Code are encouraged to:

- establish a cyber security point-of-contact for shipowners, operators, security researchers and incident investigators to communicate on cyber matters and to facilitate the reporting of potential vulnerabilities[9];
- publish a responsible disclosure policy which includes response times that a researcher should expect from the company's security team; and
- consider allowing cyber vulnerabilities in products or services to be reported via their public website.

[9] This corresponds to 'Phase 4: Producer debrief' of the risk assessment process given in section 4.3 of The Guidelines on Cyber Security Onboard Ships v3.0 (BIMCO et al.)

6. CONTINUOUS DEVELOPMENT

6.1 Purpose

Experience has shown that the landscape of cyber risk does not stay still. Vendors are encouraged to make constant efforts to stay up to date with emerging threats, vulnerabilities and other developments related to cyber risk management.

6.2 Conclusions and recommendations

Organisations adhering to the Code are encouraged to:

- Maintain and develop their skills, knowledge and experience in the cyber domain;
- Actively participate in the work of the CIRM Cyber Risk Working Group, which maintains the Code and this Guidance; and
- Participate in the work of external organisations to develop policy and instruments related to maritime cyber security.

APPENDIX I: REFERENCES

- A Taxonomy of Operational Cyber Security Risks, Software Engineering Institutes.
- DNVGL-CP-0231: 'Cyber security capabilities of control system components', DNV-GL.
- DNVGL-RP-0496: 'Recommended practice - Cyber security resilience management for ships and mobile offshore units in operation', DNV-GL.
- ENISA ISMS Framework, The European Union Agency for Cybersecurity
- Essential Eight Maturity Model, Australian Cyber Security Centre.
- IEC 61162-460: 'Maritime navigation and radiocommunication equipment and systems — Digital interfaces Part 460: Multiple talkers and multiple listeners — Ethernet interconnection — Safety and security', International Electrotechnical Commission.
- IEC 62443-4-2: 'Technical security requirements for Industrial Automation and Control Systems (IACS) components', International Electrotechnical Commission.
- IMO MSC.1/Circ.1575: 'Guidelines for shipborne position, navigation and timing (PNT) data processing', International Maritime Organisation.
- IMO MSC-FAL/Circ.3: 'Guidelines on Maritime Cyber Risk Management', International Maritime Organisation.
- IMO Resolution MSC.428(98): 'Maritime Cyber Risk Management in Safety Management Systems', International Maritime Organisation.
- Industry Standard on Software Maintenance of Shipboard Equipment (Version 1.0), CIRM/BIMCO Joint Working Group.
- ISO 9001:2015: Quality management systems — Fundamentals and vocabulary, International Organization for Standardization.
- ISO/IEC 29147: 'Information technology - Security techniques - Vulnerability disclosure', International Organization for Standardization.
- The Guidelines on Cyber Security Onboard Ships (v3.0), BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL.
- The NIST Cybersecurity framework, National Institute of Standards and Technology.
- The NIST Glossary of Key Information Security Terms, National Institute of Standards and Technology.

APPENDIX II: USEFUL LINKS

- maritimecyberalliance.com offers an anonymous cyber incident reporting system for the rapid sharing of information on cyber incidents against ship owners, ship equipment and services, ports and the wider maritime supply chain.
- http://www.cyberessentials.ncsc.gov.uk/advice/ gives five cyber security technical controls that should be put in place immediately in any organisation.