
gard
Cyber security
Managing the threat

Cyber security
Managing the threat

Contents

Disclaimer
The information contained in this publication is correct as of July 2017. Whilst we have taken every care to ensure the accuracy and quality of the information provided, Gard can accept no responsibility in respect of any loss or damage of any kind whatsoever which may arise from reliance on information contained in this publication regardless of whether such information originates from Gard, its shareholders, correspondents or other contributors.

© Gard, July 2017

Across the global maritime community, ports, vessels and facilities are increasingly connected to and dependent on cyber systems. Failure to anticipate and prepare for a cyber incident may have significant consequences.

Maritime industry operations and management rely on cyber systems. Global Positioning Systems (GPS), automated equipment, physical security sensors, electronic certificates, cargo tracking, electronic navigation, Automatic Identification Systems (AIS), record-keeping and pre-arrival processing are just some of the equipment and activities that depend on reliable and secure cyber systems. This reliance on computers and computer networks, particularly those connected to the internet, creates a potential vulnerability to cyber attacks as a result of poor cyber security practices.

There are many examples of cyber security incidents related to the maritime industry:

- Researchers from the University of Texas in the US demonstrated in July 2013 that it is possible to change a vessel's direction by interfering with its GPS signal to cause the on-board navigation systems to falsely interpret a vessel's position and heading.
- A hacker caused a floating oil-platform located off the coast of Africa to tilt to one side, thus forcing it to temporarily shut down.
- Hackers accessed cyber systems in a port to locate specific containers loaded with illegal drugs and remove them from the port undetected.
- Somali pirates employed hackers to access a shipping company's cyber systems to identify vessels passing through the Gulf of Aden loaded with valuable cargoes and minimal on-board security, which led to the hijacking of at least one vessel.
- In the Norwegian energy and oil and gas sector, more than 50 cyber security incidents were detected in 2015.
- Ten years ago, the antivirus company McAfee registered 25 new threats a day - now they register half a million threats daily.
- An increasing number of objects are connected to the Internet and may be hacked.

The consequences of a cyber attack could be wide-ranging. For example, ship collisions could result from hacking of e-navigation and other systems which could lead to:

- physical loss of or damage to ships,
- physical injury to crew,
- loss of cargo,
- pollution, and
- business interruption – including disruption to the port's activities which could lead to considerable business interruption losses.

Cyber risks are therefore of increasing concern and should be considered a part of the overall operational risk picture and addressed in a systematic way.

IMO makes cyber risk management onboard ships mandatory as of 1 January 2021

The Maritime Safety Committee (MSC) adopted Resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems in June 2017. The resolution states that an approved safety management system should take cyber risk management into account in accordance with the objectives and requirements of the ISM Code. Based on the recommendations in MSC-FAL.1/Circ3, *Guidelines on maritime cyber risk management,* the resolution confirms that existing risk management practices should be used to address the operational risks arising from the increased dependence on cyber enabled systems.

The guidelines set out the following actions that can be taken to support effective cyber risk management:

1 *Identify*: Define the roles responsible for cyber risk management and identify the systems, assets, data and capabilities that, if disrupted, pose risks to ship operations.
2 *Protect*: Implement risk control processes and measures, together with contingency planning to protect against a cyber incident and to ensure continuity of shipping operations.
3 *Detect*: Develop and implement processes and defences necessary to detect a cyber incident in a timely manner.
4 *Respond*: Develop and implement activities and plans to provide resilience and to restore the systems necessary for shipping operations or services which have been halted due to a cyber incident.
5 *Recover*: Identify how to back-up and restore the cyber systems necessary for shipping operations which have been affected by a cyber incident.

IMO Resolution MSC.428(98) encourages IMO member states to ensure cyber risks are addressed in safety management systems no later than the first annual verification of a company's Document of Compliance after **1 January 2021**.

Gard's experience

Some Gard Members and clients have been victims of cyber crime where hackers have accessed the e-mail accounts of their service providers and sent emails purporting to be from our Members requesting fees and payments be sent to different bank accounts than usual. This diversion of funds led to one ship being detained because the agents had not received funds for port clearance. This type of phishing scams have been going on since 2013 (read more in chinalawblog.com).

© Gard, July 2017

Viewing cyber security as simply an Information Technology (IT) issue is similar to considering the safe operation of a vessel as simply a main engine issue. Addressing cyber security should start with the senior management of a company rather than being delegated to the Vessel Security Officer or head of the IT department.

Any company can be vulnerable to cyber risks. At Gard we strive to protect the interests of our Members and clients in the best possible way. We are developing an internal Information Security Management System to protect the confidentiality, integrity and accessibility of our organisation's information through measures relating to people, processes and IT systems.

Where should you start to improve your cyber security?

Take a holistic approach involving:

1. *People – focus on knowledge, behaviour and mind-set*
   - Raise awareness, provide training and communicate the risks at all levels of the organisation.
2. *Processes – focus on policies, procedures and risk assessments*
   - Align cyber risks with existing security and safety risk management requirements contained in the ISPS and ISM Codes as included in company policies.
   - Include requirements relating to training, operations and maintenance of critical cyber systems in relevant documentation on-board.
3. *IT systems – focus on firewalls, antivirus and encryption*
   - Ensure there is adequate protection at all levels of the company - from senior management ashore to the crew on-board - so that it becomes an inherent part of the safety and security culture on-board each vessel.

Definitions

Cyber security, also known as **computer security** or **IT security**, is the protection of information systems from theft of or damage to:

- the hardware
- the software
- the information contained in the systems and disruption or misdirection of the services they provide.

Information security, also known as **InfoSec**, is the practice of protecting information from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Reference is also made to the IMO Multilingual Glossary on Cyberterms published in May 2016.

Gard Updates

Cyber security awareness in the maritime industry
Gard Alert: Managing cyber risks at sea
Frequently asked questions: Paperless trading (electronic bills of lading)
Cyber security posters

Other resources

BIMCO

BIMCO, together with other leading shipping organisations, launched a set of guidelines in January 2016 to help the global shipping industry prevent major safety, environmental and commercial issues that could result from a cyber incident on-board a ship. The second version of the guidelines was released in July 2017 and includes new information on how to segregate networks, manage ship-to-shore interfaces and handle cyber security during port calls. The 2017 version also has a chapter on the insurance cover. The guidelines have been aligned with the recommendations given in the IMO Guidelines on Cyber Risk Management. See also this useful poster which can help prevent the most common cyber incidents.

US Coast Guard

The US Coast Guard published its Cyber Strategy in July 2015 in response to what it perceives is one of the greatest threats to US economic and national security interests. The Coast Guard's cyber security website provides access to the strategy document and other cyber-related information, e.g. their Cyber Maritime Bulletins, and can be viewed by using this link: http://homeport.uscg.mil and the following path: Missions > Cybersecurity.
The US Coast Guard published a draft copy of its planned Navigation and Vessel Inspection Circular (NVIC) entitled Guidelines for Addressing Cyber Risks at MTSA Regulated Facilities on 12 July 2017. The draft NVIC provides guidance on how to develop and implement measures and activities for effective self-governance of cyber vulnerabilities, that shipowners and operators may find useful.
https://www.gov.uk/government/publications/ship-security-cyber-security-code-of-practice.

UK DfT

The UK Department of Transport (DfT) published its Code of Practice: Cyber Security for Ships on 13 September 2017, providing a management framework that can be used to reduce the risk of cyber incidents that could affect the safety or security of a ship, its crew, passengers or cargo. The Code of Practice is intended to be used as an integral part of a company's or ship's overall risk management system and subsequent business planning and provides actionable advice on:

- developing a cyber security assessment and plan to manage risk
- handling security breaches and incidents
- highlighting national and international standards used
- the relationship to existing regulation

Although the Code of Practice refers to Maritime Security Regulations in the UK, its provisions are complementary to those of the SOLAS Convention, the ISM Code and the ISPS Code and it is therefore considered as a useful guidance document for all nationalities of ships. A copy of the UK's Cyber Security Code of Practice for Ships can be downloaded via GOV.UK at: https://www.gov.uk/government/publications/ship-security-cyber-security-code-of-practice.

An article published by Reed Smith (available here) provides a breakdown of the Code and shed some light on the cyber security vulnerabilities unique to the shipping industry.

IACS/Classification Societies

IACS Council Focuses On Next Generation Safety Systems: Establishes Cyber Systems Panel
New IACS Chairman to focus on goal-based standards, cyber system safety and quality
ABS Expands Comprehensive Industry-First Cyber System Guidance
DNV GL recommended practice: Cyber security resilience management for ships and mobile offshore units in operation
DNV GL addresses cybersecurity risks
DNV GL: top 10 cyber security vulnerabilities
Lloyd's Register issues technical guidance for ship design in a digital age
Lloyd's Register warns of the risks associated with marine information technology

Insurance market

Joint Hull Cyber Risk Information Paper
JHC Cyber Risk Assessment Guidance
Swiss Re on cyber risks
Willis: Cyber: A Risk Like No Other
Marsh UK on cyber risks
KPMG on cyber risks in shipping

General

Maritime Executive: Maritime Industry "Next Playground for Hackers"
The International Maritime HE Bulletin: Operational cyber risk management (page 6)
Blank Rome Maritime: Cyber Security Articles
SAFETY4SEA: Cyber Security at Sea
Navigator Issue 12: Cyber security – Cyber hygiene and the use of ICT on board
Be cyber aware at sea: A global maritime & offshore industry initiative

© Gard, July 2017

Contact details for our offices around the world

Lingard Limited
Trott & Duncan Building
17A Brunswick Street
Hamilton HM 10
Bermuda

Tel +1 441 292 6766
Email companymail@lingard.bm

Gard AS
P.O. Box 789 Stoa
NO-4809 Arendal
Norway

Tel +47 37 01 91 00
Email companymail@gard.no

Gard AS
Skipsbyggerhallen
Solheimsgaten 11
NO-5058 Bergen
Norway

Tel +47 37 01 91 00
Email companymail@gard.no

Gard AS
Dronning Eufemias gate 6
NO-0191 Oslo
Norway

Tel +47 37 01 91 00
Email companymail@gard.no

Oy Gard (Baltic) Ab
Bulevardi 46
FIN-00120 Helsinki
Finland

Tel +358 30 600 3400
Email gardbaltic@gard.no

Gard (Greece) Ltd
2, A. Papanastasiou Avenue
185 34 Kastella, Piraeus
Greece

Tel + 30 210 413 8752
Email gard.greece@gard.no

Gard (HK) Ltd
Room 3003, 30F
The Centrium, 60 Wyndham Street
Central
Hong Kong

Tel +852 2901 8688
Email gardhk@gard.no

Gard (Japan) K.K.
Shiodome City Center 8F
1-5-2 Higashi Shinbashi
Minato-ku, Tokyo 105-7108
Japan

Tel +81 3 5537 7266
Email gardjapan@gard.no

Gard (Japan) K.K.
Vogue 406,
3-9-36 Higashimura, Imabari-City,
Ehime 799-1506,
Japan

Tel +81 898 35 3901
Email gardjapan@gard.no

Gard (North America) Inc.
40 Fulton Street
New York, NY 10038
USA

Tel +1 212 425 5100
Email gardna@gard.no

Gard (Singapore) Pte. Ltd.
72 Anson Rd
#13-02 Anson House
Singapore 079911
Singapore

Tel +65 3109 1800
Email gardsingapore@gard.no

Gard (UK) Limited
85 Gracechurch Street
London EC3V 0AA
United Kingdom

Tel +44 (0)20 7444 7200
Email garduk@gard.no

Gard Marine & Energy- Escritório de Representação no Brasil Ltda
Rua Lauro Muller 116 – suite 2402
Botafogo, 22290-160,
Rio de Janeiro, RJ,
Brazil

Tel +55 (21) 3037 9764
Email gardbrasil@gard.no

Emergency Telephone Number
+47 90 52 41 00

www.gard.no

© Gard, July 2017