Sharing and reporting cyber incidents

Information sharing is critical in our collective defence against cyber crime and to strengthen cyber security within the maritime sector. Gard encourages Members to share information about events with the right authorities. This can contribute to and avert current or future cyber security threats. Together we can make a difference!

Published 15 August 2024

The information provided in this article is intended for general information only. While every effort has been made to ensure the accuracy of the information at the time of publication, no warranty or representation is made regarding its completeness or timeliness. The content in this article does not constitute professional advice, and any reliance on such information is strictly at your own risk. Gard AS, including its affiliated companies, agents and employees, shall not be held liable for any loss, expense, or damage of any kind whatsoever arising from reliance on the information provided, irrespective of whether it is sourced from Gard AS, its shareholders, correspondents, or other contributors.

The maritime industry has increasingly introduced internet-connected technologies and digital systems to improve commercial vessel and port facility operations such as those used for the movement of cargo and ship navigation. However, this digital interconnectedness has introduced cybersecurity risks, including the threat of ransomware attacks that can disrupt operations, unauthorized access to vessel controls and navigation systems, espionage in supply chain practices and behaviours, and theft of trade secrets.

When cyber incidents are reported quickly, the authorities can use the information to provide both assistance and issue warnings, to prevent others from falling victim to similar attacks. This information is also crucial to identify trends that can help us protect ourselves and the rest of the maritime sector.

Important items to share

Event data and time, location, type of activity and a detailed description of the event.

Types of activities you should share

• Unauthorized access of your system.
• Denial of Service (DOS) attacks lasting more than 12 hours.
• Malicious software in your systems, including type if known.
• Targeted and repeated scans against the company's IT services systems.
• Repeated attempts to gain unauthorized access to your system.
• Email, mobile or social media messages related to phishing.
• Navigation events related to SATCOM, AIS and GNSS interference

How should you share?

We encourage you to send an e-mail to the flag administration, coastal authorities, national police, port authority, class society and/or your cyber security service provider. Sharing information with your cyber security service provider does not replace statutory reporting requirements to authorities. Remember to include full contact information.

Reporting to the authorities

For example, the US Coast Guard (USCG) seeks to address maritime cyber espionage and cybersecurity risks by focusing on establishing minimum requirements for the reporting of cybersecurity incidents by the maritime shipping community. The USCG stresses that the mandate for reporting will be quite broad, and their expectations for reporting any such suspicious activity will become much higher going forward.

The new USCG requirements will only apply to US-flagged vessels, outer continental shelf facilities, and US facilities subject to the Maritime Transportation Security Act of 2002 regulations. Although not mandatory, any other vessel, harbour, port, or waterfront facility may also report activities that may result in a cyber security incident.

Ref. "NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-24" , issued in February 2024.

On an international level the **IMO** implemented Resolution MSC.428(98) in 2021, which requires vessel owners, operators, and managers to consider the overall cyber risks, and to implement cybersecurity across all levels of their management system, in line with International Safety Management (ISM) Code.

In combination with this resolution, the IMO also released Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3). This provides high-level recommendations for maritime cyber risk management that can be incorporated into existing risk management processes.

Since 2020, Gard has been a member of NORMA Cyber , a non-profit cyber security service company established by Norwegian shipowners and supported by the Norwegian Coastal Administration in their role as sectorial response function for cybersecurity within the Norwegian maritime sector.

NORMA Cyber welcomes all voluntary reporting of cyber incidents from Gard's Members and will act as an advisory body to Gard when needed during an incident and crisis management, as well as contribute to warnings and reports.

Gard encourages all members to share cyber incidents. Timely sharing of incidents enables vulnerability warnings to the broader maritime sector.

Read more on cyber security here: https://gard.no/insights/cyber-security/

The information provided in this article is intended for general information only. While every effort has been made to ensure the accuracy of the information at the time of publication, no warranty or representation is made regarding its completeness or timeliness. The content in this article does not constitute professional advice, and any reliance on such information is strictly at your own risk. Gard AS, including its affiliated companies, agents and employees, shall not be held liable for any loss, expense, or damage of any kind whatsoever arising from reliance on the information provided, irrespective of whether it is sourced from Gard AS, its shareholders, correspondents, or other contributors.