Cyber security awareness in the maritime industry

There is no single solution to managing cyber risks. It is a collaboration involving people, processes and IT systems. Establishing awareness in all levels of an organisation is the important first step when implementing cyber security management.

Published 31 October 2016

Cyber breach is placed among the top operational risks by management consultants such as KPMG , EY and risk.net . A Plymouth University article shows that outdated systems can be a vulnerability for many vessel operators. Law firms are also warning against the rise in cyber-crime targeting the shipping industry. The accelerating rate of technological changes provides criminals with endless opportunities to gain access to unsecured systems. Increased connectivity to onshore facilities, more cloud computing, the use of connected networks instead of isolated computers, 'bringing your own device' (BYOD), use of social media and the Internet of Things – all contribute to the growing risk.

What types of cyber attacks could happen in the maritime industry?

There have been many examples of cyber security incidents in the maritime industry:

• diverting funds to fraudulent accounts using e-mail spoofing ;

• changing a vessel's direction by interfering with its GPS signal;

• causing a floating oil platform to tilt to one side, thus forcing it to temporarily shut down;

• infiltrating cyber systems in a port to locate specific containers loaded with illegal drugs to remove them from the port undetected;

• infiltrating a shipping company's computer systems to identify vessels with valuable cargoes and minimal onboard security, which led to the hijacking of at least one vessel.

What are the consequences of a maritime cyber attack?

In 2015, Lloyd's of London estimated that cyber attacks cost companies USD 400 billion every year . In addition to financial loss, the consequences are wide-ranging:

• physical loss of or damage to ships;

• physical injury to crew;

• loss of cargo;

• pollution;

• reputational damage;

• business interruption.

Cyber risk on the agenda

With increasing digitisation, we are seeing signs of a holistic approach from a broad spectrum of organisations:

• authorities have formed strategies and produced reports (US , EU);

• various organisations in the maritime industry have issued cyber security guidelines and recommendations (BIMCO_Guidelines%20on%20cyber%20security%20onboard%20ships_version%201-0.pdf , MSC.1-Circ.1526.pdf , DNVGL-RP-0496.pdf);

• the oil and gas sector have joined forces to combat cyber threats ;

• the UK's Department for Transportation and the Maritime Coastguard Agency have produced a Code of Practice on Cyber Security for Ports and Port Systems .

Where can you start?

The weakest link is the human factor: Most cyber attacks rely on human errors to succeed, and according to DNV GL, 97 per cent of attacks exploit human emotions to trick a user into revealing valuable information (social engineering). 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. This October, we marked the international cyber security month with various activities to raise awareness about the risks we face and how each individual can help prevent attacks.

We suggest that our Members, clients and business partners arrange similar international cyber security awareness activities to foster awareness within their organisations. More guidance and resources on how to get started are available on gard.no .

Questions or comments concerning this Gard Insight article can be e-mailed to the

irrespective of whether it is sourced from Gard AS, its shareholders, correspondents, or other contributors.

Gard Editorial Team