HDI Risk Consulting

Cyber risks onboard ships

www.hdi.global

FACT SHEET

Prevent loss due to cyber risks.

Nowadays the information and operational technology onboard ships is very complex. Ships contain many system networks that are increasingly connected together. Think of bridge systems, propulsion and machinery systems, power control systems as well as systems like passenger serving systems, communication systems and such. A significant risk of these systems is the exposure to malicious cyber attacks. This leaflet gives a view on vulnerabilities and threats concerning cyber attacks of ships.

Cyber criminals

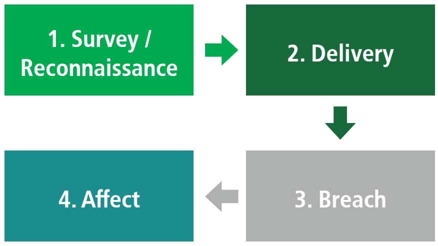
Cyber criminals can be divided into four groups with their own motivations and own objectives:

Group	Motivation	Objective
Activists	Reputational damage, disruption of operations	Destruction of data, publication of sensitive data, media attention
Opportunists	The challenge	Getting through cyber security defenses, financial gain
Criminals	Financial gain, commercial espionage, industrial espionage	Selling stolen data, ransoming data or system operability, arranging fraudulent transportation of cargo
States, state sponsored organizations, terrorists	Political gain, espionage	Gaining knowledge, disruption to economies and critical national infrastructure

There are two distinct types of attacks: untargeted and targeted. Untargeted attacks are attacks on ship's systems and data such as social engineering, phishing, scanning and ransomware. Targeted attacks are attacks on specific systems or data. Think of spear phishing, (D)DoS attacks or subverting the supply chain.

The anatomy of a cyber attack

The anatomy of a cyber attack criminals normally use is as follows:


1. Survey / Reconnaissance

2. Delivery

3. Breach

4. Affect

The first step is to gather information on how to penetrate the systems of a ship, company or seafarer by searching in social media, technical forums, publications etcetera. The second step is to deliver the malware by sending an infected e-mail or providing infected removable media or other kinds of methods. The third step is to gain access and take full control of the system or steal sensitive data from the system. The fourth step is to sell or destroy the sensitive data.

What are the risks?

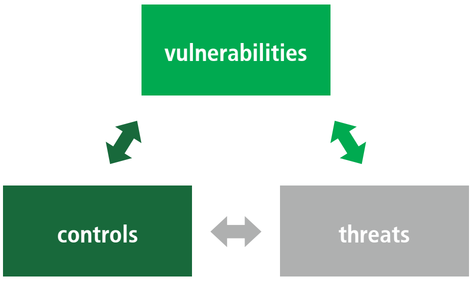
On ships, many systems are available that can be attacked by cyber criminals. For instance:

- cargo management systems;
- bridge systems;
- propulsion and machinery management;
- power control systems;
- access control systems;
- passenger servicing and management systems;
- passenger facing public networks;
- administrative and crew welfare systems;
- communication systems;
- core infrastructure systems.

Suppliers and contractors are a safety risk, because they have knowledge of ships' operations and often have full access to the systems of a ship. Technicians of third parties also pose a risk, because of their remote access to the ship's systems to read data for maintenance reasons.

Prevention

To prevent loss due to a cyber attack, the senior management must be aware of the different kinds of attacks. It is important to make a cyber risk assessment of all assets of a ship or company. Assets like software, hardware, infrastructure, crew members, etc., need to be identified as well as the vulnerabilities of these assets and the threats that can affect them.



Determine the likelihood of vulnerabilities being exploited by these threats and develop a protection plan and detection measures to mitigate the risks of the assets.

Contact

For questions and/or more information you can contact us via:
HDI Risk Consulting
T: +31 (0)10 – 40 36 328
hrc@nl.hdi.global
www.hrc-services.nl

Although we made every effort possible to ensure the accuracy of the information provided, no liability can be assumed for the currentness, correctness and completeness of the information. We neither intend, nor assume any obligation, to update or revise these statements in light of developments which differ from those anticipated.

Develop response plans to reduce the impact of threats to the safety and security of the ship (contingency plans). Respond to cyber security incidents by using the response plans. Assess the impact of the effectiveness of the response plan and reassess threats and vulnerabilities.

Cyber security awareness

Cyber security awareness is essential in order to reduce cyber risks onboard ships. Training, workshops and written procedures might help to make crew members more aware of the risks and possible consequences of cyber-attacks.

More information can be found at:
www.bimco.org
www.nist.gov/cyberframework

There are several other good sources. The DNV-GL as a European classification society does a lot in this respect.
https://www.dnvgl.de/services/cyber-secure-class-notation-124600

In addition, from 2021 ship owners and managers have to incorporate cyber risk management into their ISM systems. Otherwise they might be at risk having their ships detained. Hence, maritime cyber security awareness will finally be a "must have" rather than a "nice to have".
http://www.imo.org/en/OurWork/Security/GuidetoMaritimeSecurity/Pages/Cyber-security.aspx

Benefits of HDI Risk Consulting

- HDI Risk Consulting Professionals offer risk and safety related analysis to enable specific risk prevention action plans to be developed.
- Qualified international Risk Engineering network offers clients worldwide multi-discipline support in Risk Engineering.
- HDI Risk Consulting is a wholly owned subsidiary of HDI Global SE and thus part of the Talanx Group, one of the largest insurance groups in Germany and Europe.