HDI Risk Consulting

Information leaflet Cyber risks onboard ships

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 etcetera. But also 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

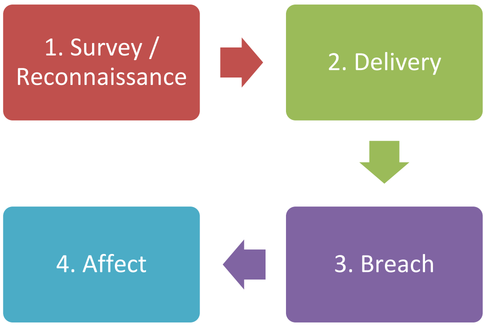
Cyber criminals can be divided in four groups with their own motivations and own objectives:

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 like 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 how to penetrate into 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 to the system to take full control of the system or steal sensitive data from the system or something else. The fourth step is to sell or destroy the sensitive data.

What are the risks?

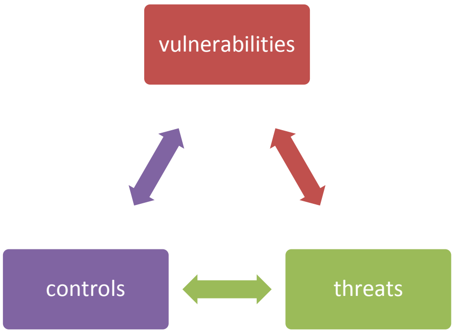
Onboard ships, many systems are available that can be attacked by cyber criminals. For instance:

- ✓ 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.

Also, suppliers and contactors 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 be able to prevent loss due to a cyber attack, the senior management must be aware of the different kinds of these 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, etcetera. Identify the vulnerabilities of these assets and identify 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. Develop response plans to reduce the impact of threats that are realized on 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 to reduce cyber risks onboard ships. Training, workshops and written procedures for example 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

How we work

HRC stands for a high level of knowledge. By means of training, study, the attendance of workshops, regular visits to trade fairs as well as the consulting of dedicated press, the risk engineers and technical advisors keep their knowledge level high and stay abreast of the latest developments in the market. HRC works together with insurance brokers and clients in order to achieve a corporate culture in which risk awareness will be one of the principal elements. By working on a safety culture from within the organization a general awareness will develop, whereby risks will be recognized and addressed. Organizational and technical recommendations will be implemented where possible in order to control the risks. The business continuity of our clients will always be a central element.

Contact

For questions and/or more information you can contact:

HDI Risk Consulting
T: +31 (0)10-40 36 328
hrc@nl.hdi.global
www.hrc-services.nl

HDI Risk Consulting (HRC) consists of about 180 experienced and competent risk engineers worldwide, working for various national and international clients. HRC performs risk analyses and advisory assignments for (the customer of) the parent company, HDI Global, but also by appointment for various insurance brokers and / or companies

Especially within the disciplines Fire, Transport, Security, Motor vehicles, Technical Insurance and Cyber security HRC can play a significant role.

HDI Global is member of the Talanx Group.