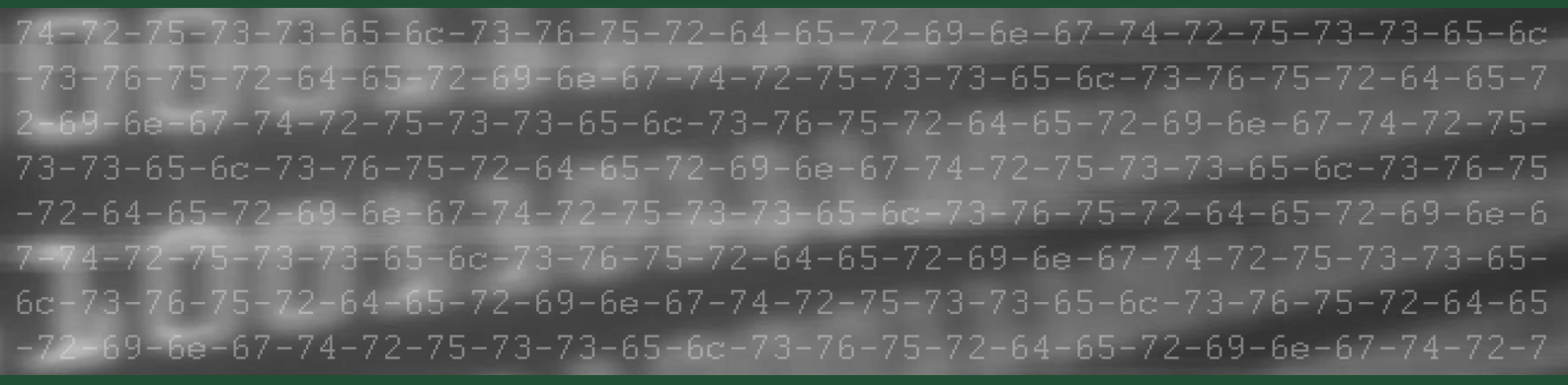
CENTRE FOR
CYBER SECURITY

Threat Assessment

The cyber threat against the maritime sector



Threat Assessment Branch under the Centre for Cyber Security

March 2017

CENTRE FOR CYBER SECURITY

Threat Assessment: The cyber threat against the maritime sector

This threat assessment covers the cyber threat to the maritime sector in Denmark. The general cyber threat against the maritime sector is directed against the commercial business of the sector.

Key Assessment

- The general cyber threat against the maritime sector is directed against the commercial business of the maritime sector. The cyber threat generally does not pose a direct threat to the physical security of maritime operations.
- The threat from cyber criminals is **VERY HIGH**. Sector specific threats include cyber-enabled smuggling and theft, whereas non-sector specific threats include ransomware and cyber-enabled fraud.
- The threat of cyber espionage against the maritime sector is **VERY HIGH**. Several states systematically use cyber espionage as a means to achieve industrial and business advantages and promote political and economic interests.
- The threat of destructive cyberattacks against the maritime sector is **LOW**. Maritime lines of communication, including vessels and ports, may be targets for destructive cyberattacks during times of conflict.
- The threat of cyber activism against the maritime sector is **LOW**. The shipping industry does not enjoy a high degree of attention from cyber activists, and as such is not a high-profile target.
- The threat of cyber terrorism against the maritime sector is **LOW**. Terrorist groups have only shown a limited interest in the maritime sector. Also, terrorists lack the capabilities to launch spectacular cyberattacks at the maritime sector.

Analysis

This threat assessment gives an overview of the cyber threat against the maritime sector in Denmark. In this assessment, the Danish Defence Intelligence Service's Centre for Cyber Security (CFCS) defines the maritime sector relatively broadly as shipping companies, vessels, port infrastructures and other maritime suppliers. In the assessment the CFCS view the cyber threat from a global perspective as Danish maritime companies have a large foreign operational and commercial presence.

In general, the maritime industry faces a range of cyber security challenges. The global nature of business relationships and the diversity and complexity of operational activities expose the maritime sector to a broad range of cyber security threats. The supply chain is not isolated but part of a wider supply chain, including companies and lines of transportation in other sectors. Threats and security challenges can therefore cross sector boundaries.

Maritime companies rely on numerous local partners across the globe, exposing back-end system linkages as well as critical information flows to local weaknesses in the cyber security infrastructure.

The maritime supply chain can be very complex and connected to other sectors. The shipment of a single container, bulk or tanker shipment can involve a multitude of cargo owners, shipping lines, ports, land transportation companies, customs authorities and financial institutions. A successful penetration of cargo-related systems in just one of these entities can compromise both information integrity and operational aspects in any of the other entities involved.

Maritime back-end systems set very few industrial standards; consequently, industrial IT landscapes is often custom-built with limited systematic testing of cyber security issues.

Shipping lines with a high degree of complexity and/or individual cargo pieces, notably container lines, have reached a stage of electronic commerce where business operations cannot be handled manually for any extended period of time. Thus, these shipping lines have an added vulnerability in case of extended deliberate or accidental system outage.

The rapid development in maritime broadband satellite coverage combined with the introduction of highly sophisticated equipment such as computer controlled engine systems has changed the structural risks to maritime vessels. Ships are no longer protected by an air-gap from external systems. Today, an estimated 30,000 vessels globally have equipment providing them with constant internet access, which is an increase from only 6,000 in 2008. Even if networks on board are separated between systems for ship operation, crew welfare and remote access to suppliers, separations can over time be compromised by ad hoc interventions by the crew or suppliers, for instance in connection to maintenance. The separations can also be compromised by manual transfer of data. A further complexity is that shipping lines operate a mix of vessels which they either own or charter for a short period of time. Additionally, vessels and other key systems can carry an analogue heritage, being built for analogue control, but later added digital solutions.

Ports are an integral node of both the maritime transportation chain and the land transport chain, and ports rely on information from both shipping lines and land-side logistics companies. As for the port infrastructure, key systems may be penetrated – the most well-known example being the penetration of Antwerp port which enabled the attackers to access the port's terminal operating system.

Maritime suppliers, such as maintenance companies, cover a wide range of maritime interests. Given their position in the maritime supply chain, threats to maritime suppliers can affect customers within the maritime sector. Due to the often complex and transnational nature of maritime operations a mix of known and lesser known suppliers support these operations. Each of these suppliers poses a potential vulnerability to the supply chain.

These structural vulnerabilities and challenges may enable cyber threat actors to compromise the IT systems used in the maritime sector.

At a general level, the cyber threat against the maritime sector is directed against the commercial operations of the maritime sector. The cyber threat generally does not pose a direct threat to the physical security of maritime operations. There are some instances, however, where cyber operations against shipping companies and ports have enabled criminals to perform theft and smuggling of cargo.

The threat from cyber criminals

The threat from cyber criminals is **VERY HIGH**. The threat from cyber criminals against the maritime sector includes both non-sector specific threats such as ransomware and cyber-enabled fraud and sector-specific threats such as cyber-enabled smuggling and theft.

Smuggling and cargo theft are a well-known phenomenon in the maritime industry. However, cyberattacks have provided criminal groups with additional tools to facilitate illegal shipments of goods. Illustrative of this is the smuggling of drugs through the port of Antwerp, penetration of customs authorities in Australia as well as theft of shipping lines' credentials with the intent to commit fraud in connection with the sale of oil shipments.

Cyber criminals have provided reconnaissance information to pirates through hacking prior to piracy operations. Compromise and exploitation of vulnerable systems in shipping lines and ports provide criminals with detailed information regarding the exact location of specific goods, making them vulnerable to theft either in port, to/from the port or through targeted piracy operations. As an example, Indonesian pirates used hackers prior to a piracy operation in 2015 to gain critical information about cargo content and ship locations.

This facilitates either standard theft of identified goods or the manipulation of information resulting in the deliberate hand-over of cargo to the wrong destination. Given the many different hand-over points of information during the supply chain, criminals only need to find one or two vulnerable entities within the chain to be able to manipulate the shipment.

Such efforts to manipulate information also enable criminals to get illegal cargo loaded onto vessels for smuggling purposes. This approach could jeopardize the safety of the vessels if the shipment contains hazardous materials.

There are examples of thefts of digital certificates from maritime companies, which allow criminals to falsify ownership documents, thereby tricking a third party into payment for cargo which is not owned by the criminals or does not exist at all.

Even non-sector specific threats like ransomware may have a significant impact on maritime operations, if the ransomware attack is aimed at physical assets such as vessels and physical port infrastructure or other critical systems, for instance online booking systems that are vital to most shipping companies.

The cyber threat from states
The threat from cyber espionage against the maritime sector is **VERY HIGH**. The threat from destructive cyberattacks against the maritime sector is **LOW**.

Several states systematically use cyber espionage as a means to achieve industrial and business advantages and serve political and economic interests.

State-sponsored cyber espionage against the maritime sector may be in the form of industrial espionage aimed at promoting industrial and business advantages, targeting sensitive information about business activities as well as key technologies and assets. Therefore, cyber espionage is often directed against the business or central management of maritime companies.

Cyber espionage against the maritime sector could also be motivated by geopolitical interests as shipping lines, vessels and ports are important assets providing lines of transportation. Some sea lanes pass through areas of geopolitical significance and territorial disputes.

In 2014, the United States Transportation Command (US TRANSCOM) provided a report to the US Senate Oversight Committee on Armed Services wherein US TRANSCOM linked state-sponsored actors to twenty successful intrusions into logistics providers for the US TRANSCOM as well as spear-phishing campaigns targeting specifically commercial sealift companies. From 2011 to 2013, cyberattacks against various sectors in Japan, Taiwan and South Korea also targeted shipbuilding and maritime companies.

Several states are developing cyber capabilities to launch destructive cyberattacks against foreign countries. Maritime lines of transportation, including vessels and ports, are potentially targets of destructive cyberattacks during times of conflict. The threat, though low, is mainly relevant to maritime companies operating in areas of territorial disputes and conflict or supporting military operations.

In general, access to critical systems is necessary in order to carry out destructive cyberattacks. Targeted intrusions, including cyber espionage, against critical systems in the maritime sector may thus serve as a warning of the risk of becoming a victim of destructive cyberattacks.

The threat from cyber activism
The threat from cyber activism against the maritime sector is **LOW**. However, the threat can rise suddenly if cyber activist get a negative focus on the sector. Cyber activism focuses on specific themes and subjects and typically seeks media attention for specific causes through high-visibility cyberattacks. Cyber hacktivists typically target companies and individuals that they regard as opponents of their cause.

The maritime sector does not generally suffer a high degree of attention from activists, and as such, is not a high-profile target.

However, cyber activism is agenda driven and any negative focus from activists on maritime companies may lead to a more significant and sudden threat from cyber activists, for example in relation to high-profile incidents or events such as environmental disasters, including oil spills, transportation of controversial cargo or support to military operations.

The threat from cyber terrorism
The threat from cyber terrorism against the maritime sector is **LOW**.

Terrorist groups have only shown a limited interest in the maritime sector, including a limited number of traditional, kinetic terrorist attacks against ports and ships.

The primary aim of terrorists is the creation of fear, using the destruction of physical property or lives as a tool to this end. In general, terrorists do not have the capabilities to launch such successful cyberattacks.

Attempts to create a spectacular, catastrophic incident on board a ship through remote cyber manipulation of critical systems would be hampered by numerous redundant safety systems. Hence, from a cyber security perspective, such a scenario is assessed unlikely.

The most realistic threat from terrorists is the use of cyberattacks to facilitate the illicit shipment of materials involved in an attack and as such, this threat is similar to the one posed by cyber-enabled smuggling conducted by criminals.

Recommendations
CFCS recommends that the strategic management of cyber security in the maritime sector is anchored at top management level and not within the IT department.

CFCS recommends that top management in land-based parts of the maritime organizations recognize and act on the basis of the described threat scenarios in this threat assessment. These scenarios should have a specific focus in the organizations' assessment of relevant information security risks in order to establish an appropriate and robust cyber defense on a daily basis and in incident management. The risk assessment should involve the individual organization’s acknowledged vulnerabilities. The prerequisite for this is the establishment of an overview of business processes, IT infrastructure, IT processes and possible supply chain threats.

CFCS recommends that security in general is managed based on a generally approved standard such as ISO/IEC 27001. Within specific guidance for management and control of security in the maritime sector, including on board ships, there are a number of standards provided by organizations such as the International Maritime Organization (IMO) and the international shipping association BIMCO, which could also be relevant to the specific organization.

General recommendations
On a general level CFCS recommends that the organization assesses the implementation of specific security measures and controls on the basis of the organization's business context and risk appetite.

The main recommendations include the following:
- Provide a detailed information security risk assessment focusing on cyber threats
- Adjust business processes to mitigate cyber and information security threats

- Conduct information security awareness training for both land-based and sea-based employees in general and regularly with a focus on cyber threats
- Security patching of applications and operating systems
- Application white listning
- Implement strict policies to minimize the number of entities with access to critical systems as well as the number of users with privileged access rights
- Restrict users access to information based upon the need-to-know principle
- Segmentation, if possible, of the location of critical business data
- Establish back-up routine procedures to allow complete restoration from removal of IT infrastructure in the company/vessel/port and test the routine procedures
- Test of backup media and restoration procedures
- Virus-protection - with continuous and rapid update - on all systems
- Perform audits on board vessels to enforce system segregation
- Conduct relevant penetration tests on land-based and seaborne entities as well as on critical industrial control systems
- Be especially vigilant when introducing online access to automated equipment
- Scanning of incoming e-mails in order to avoid spam and malware
- Restricting users' access to write on shared IT drives to the functionally necessary.

Specific onboard considerations

Apart from the technical and procedural cyber security controls that needs to be considered by all organizations, there are a number of aspects particularly interesting in an offshore operation.

The fact that data transfer between ship and ashore are based on satellite and radio communication creates a need for special security considerations. The update of operating systems, application, anti-malware etc. is not as effortless and low-cost as ashore, therefore procedures should be established to ensure timely distribution of updates to ships and to ensure that all relevant onboard equipment are updated.

There are many systems, types of equipment and technologies that could be vulnerable to cyber-attacks onboard ships. These may include bridge systems, ship access control systems, power control systems, crew and passenger wi-fi, administrative systems, and many more. For this reason special care and considerations should be taken when designing and implementing the segmentation for systems and networks. Furthermore, extra care should be taken in protecting the boundaries for these components.

In the event of a cyber-attack on a ship offshore the required capabilities are not necessarily at hand onboard. In such an event, external expert assistance should be available to ensure an effective response and contingency plans for dealing with an incident.

Contingency plans should also be developed for the event of a complete loss of data communication and other communication. The contingency plan should contain a strategy for

graceful shutdown of all non-essential systems and a prioritization of the systems that must remain in operation. Contingency plans must always be tested through training exercises.

Below is the scale of probability the DDIS applies