NETHERLANDS
MARITIME
TECHNOLOGY

Safety of data

The risks of cyber security in the maritime sector

Title:	Safety of data. The risks of cyber security in the maritime sector
Organization:	Netherlands Maritime Technology
Author:	S. de Vleeschhouwer
Project code:	MIIP018
Date of Publication:	April 2017

Contact information:

PO Box 23541
3001 KM Rotterdam
T +31 (0)88 41 51 032
E vleeschhouwer@maritimetechnology.nl

About Netherlands Maritime Technology
The Netherlands Maritime Technology (NMT) trade association is the first port of call for and primary representative of the Dutch maritime technology sector. NMT has 400+ members including shipyards, marine equipment suppliers and service providers, all united within a close and highly successful network.

The Dutch maritime technological sector is faced with increasing global competition and protectionism. NMT believes that the maritime sector should distinguish itself based on its knowledge, sustainability and innovation. Netherlands Maritime Technology strengthens this unique reputation by initiating activities and projects, stimulating cooperation and securing a level playing field.

Content

Summary

In this exploration, the issue of cyber security for the maritime sector is discussed with a focus on the shipping sector (liner, bulk and specialized shipping).

This exploration:

- Informs shipyards, suppliers and ship-owners about the motivations / reasons for cyber incidents;
- Creates awareness within the sector regarding the risks, roles and responsibilities and possible solutions;
- Informs organizations within the maritime sector on the specific guidelines for cyber security in the maritime domain. This report doesn't include new guidelines, it refers to the existing guidelines and the commonalities.

ICT could help shipping companies to reduce costs by using their assets more efficiently and manage the performance of a whole fleet, instead of single ships. In doing so, ships are more often equipped with systems that can be monitored from shore and sensors that generate data, which are available online and in real-time. With the perspective of unmanned and autonomous vessels, continuous connectivity is essential, to open a pathway for cyber incidents.

Cyber security is a real issue and of genuine concern for companies operating in the maritime domain. Cyber threats are real for today's ships, whether they are connected to the internet or not. Malware can be injected through a variety of paths, this includes: USB drives, through infected components (new build and retrofit), or through (wireless) network connections. Cyber threats could impact the entire organization and all operations. Although most ship-owners look to balance their budget to stay in business, the risks of cyber threat are not just an IT issue. It should be considered as a serious threat for the continuity of operations within the maritime sector.

To protect networks, computers, programs and data from being accessed without authorization, attacked or damaged, maritime companies should have technologies, processes and practices in place. This is what we refer to as cyber security. As a result of writing this report, we can conclude the following on preventing cyber security:

- The expectation is an increasing relevance on this subject over the coming years. A cyber incident will occur. It's more the question of when rather than if. Being a hundred percent secure is unfeasible and undesirable, because it limits flexibility and innovation. Processes and measures should be in place to prevent damage and it's important to stay agile as well as resilient.
- The processes and measures in place should include the entire supply chain. The shipping company should make arrangements with its suppliers regarding cyber security of the products and services they use.
- Know what you want to protect: Identify the 'crown jewels'. Awareness within the organization should be priority number one.
- In all guidelines and reports on how to become cyber resilient 'transparency' on cyber security is encouraged: Being open about incidents, cyber breaches and share cases with companies within the same industry and/or the supply chain is important.
- The question 'who is accountable for what?' is an interesting one, and unanswered by most people. Within the guidelines, reports and discussions the issue on responsibility and accountability of parties within the supply chain, is barely discussed. Where best practices are shared on the technical aspects of cyber incidents, it could be sensible to share information on the divide of responsibility as well. Maritime insurance companies could play a role in this.

§ 1 Introduction

"*Today, around 90% of world trade is carried by the international shipping industry. Without shipping the import and export of goods on the scale necessary to sustain the modern world would not be possible.*", stated IMO Secretary-General Koji Sekimizu on the IMO World Maritime Day in 2016.
With more than 50.000 merchant ships trading internationally, shipping is essential for world trade. Shipping is considered to be isolated, due to the physical distance between ships and shore, but the maritime sector plays a vital part in global transport.

Although the sector faces rough market situations today, shipping companies, shipyards and suppliers are constantly improving the performance of their products in a more safe, sustainable and efficient way. As Dr. Martin Stopford (Clarkson Research) mentioned in his articles on smart shipping, every aspect of sea transport could benefit from the new generation of Information and Communications Technology. ICT could help shipping companies to reduce costs by using their assets more efficiently and manage the performance of a whole fleet, instead of single ships. In doing so, ships are more and more equipped with systems which can be monitored from shore and sensors which generate data, which is available online and in real-time.

There is no doubt that ICT has great benefits, but with the implementation of more and more technology grows the dependency on technology as well. This opens a pathway for others to make use of this dependency and interfere certain processes without permission of the cargo-owner, charterer, operator or ship-owner. Since many of the control and monitoring systems onboard were not originally designed to connect with the Internet, therefore especially the maritime industry is at risk. Interruption of operations, loss of information and impact on privacy are just a few of the risks of connectivity.

In this exploration, the issue of cyber security for the maritime sector is discussed, with a focus on the shipping sector. Although the original goal was to explore both shipping and shipbuilding, it became apparent that shipbuilding is not distinct from other industries, such as the automotive sector. The construction of ships, or the systems, is therefore not included in this exploration. The focus is on the actual shipping, smart and safe. How do companies in the maritime sector manage the security risks and what role does cyber security play in the development of new products and systems? What is the responsibility of the shipyard, the system suppliers and the satellite connection provider and when does it become the responsibility of shipping companies? The goals of this exploration are:

- To inform ship-owners and shipyards / suppliers about reasons cyber incidents occur.
- Raise awareness within the sector regarding the risks, roles, responsibilities and possible solutions.
- Promulgate which guidelines for data security and communications are available.

§ 2 Definition and reported incidents

In this paragraph, an overview is given to grasp the issue; different definitions of cyber security are discussed as well as motivations and reported incidents.

§ 2.1. The definition

In various publications regarding the issue of cyber security different definitions are being used. For example:

- ABS definition of cyber security; "*The activity or process, ability or capability, or state whereby information and communication systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification or exploitation.*"

- The definition of cyber security of The North of England P&I Association; "*Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access*."

- According to an amendment for the IMO Maritime Safety Committee (96th session): "*Cyber security is defined as the range of information technology processes intended to protect data being transmitted over the Internet, and to combat the threat of the installation of malware programs.*"

- The definition of BIMCO and adopted by DNV GL in their recommended practice; *"Practices, tools and concepts that protect: a) the operational technology (OT) against the unintended consequences of a cyber incident, b) information and communications systems and the information contained therein from damage, unauthorised use or modification, or exploitation; and/or, c) against interception of information when communicating and using the internet."*

It is remarkable that only the fourth definition touches OT, while the other definitions mainly refer to cyber security as a form of information security. Information security has three aspects: confidentiality, integrity and availability. Cyber security protects operation and technology used for industrial control systems connected to physical assets, such as propulsion machinery. In this report, we focus on the broad definition of cybersecurity, which includes both IT and OT.

§ 2.2. Cyber incidents

Cyber incidents make newspaper headlines every day. In exploring this subject, it is essential to get a perspective on the severity of the issue. Is cybersecurity a true problem for the maritime sector or is it a misused buzzword by commercial parties to commercialize fear of cyber incidents? Desk research showed the following examples of known incidents in the maritime sector, in the last five years:

- Between 2011 and 2013 the Port of Antwerp was subject to cyber criminals to smuggle drugs. They installed physical devices, such as key loggers, and sent malware attached to emails, to infiltrate the computerized cargo tracking system of different companies within the port. In this way, they could identify the shipping containers in which the drugs were hidden. When these containers were located, they dispatched their own drivers to retrieve their containers and covered their tracks afterwards (HLN.be, 2013).

- In the summer of 2013 a 'friendly' experiment was performed by researchers from the department of Aerospace Engineering and Engineering Mechanics at the University of Texas at Austin. They created false civil GPS signals to gain control of the GPS receivers of a superyacht. This technique, called spoofing, did not trigger alarms on the ship's navigation equipment and allowed the research team to change the course of the vessel (The University of Texas in Austin, 2013).

Fig 1. A GPS spoofing-detection system above the bridge of the supervacht. Photo: Mark L. Psiaki

- In 2014, the Danish Maritime Authorities discovered they had been attacked in 2012. The attack was carried out through the transmission of a PDF document with an embedded virus. Consequently, this was spread throughout the networks of the organizations as well as other Danish government institutions (Seafocus, 2016).
- Off the coast of Africa an oil rig was tilted to one side. This action, caused by hackers, shut the production down for a week. Another incident occurred to an oil rig on its way from South Korea to Brazil. In this case malware had taken the rig's system offline, none of the workers knew the ins and outs of the computer system they were using to operate the rig, which contributed to a delayed response (CSIS, 2016).
- The company Verizon mentions a maritime case in their report 'Data breach digest. Scenarios from the field'. In this case, they were contacted by a shipping company who noticed a change in the way pirates operated. These pirates attacked specific vessels and, once on board, they headed for certain cargo containers and then departed the vessel without further incident. After investigation, it became apparent that hackers could access the CMS of the shipping companies, which led them to get insight in the shipping inventories and bills of lading for future shipments (Verizon, 2016).
- Personal data of over 134.000 US navy personnel was retrieved by computer hackers. They were able to do so via an access point of the company Hewlett Packard, who are responsible for the automation of the US navy.
- The company Fox-IT presented recent 'maritime' cases during Digital Ship Maritime Cyber Resilience Forum Rotterdam (2017). Hacking is a business model to some and can generate a serious income. One of the methods used by cyber criminals is CEO fraud. In the case presented, a hacker infiltrated in the company's systems and got familiar with the use of language and correspondence between a CEO and financial colleagues. Then he took over the email correspondence and requested the finance employee to transfer an amount of €450k. The finance employee asked some questions by mail, which were answered by, what he believed was the CEO. Luckily, the financial employee met his CEO the next day in office and asked him about the transfer. They found out just in time and could prevent the transfer from taking place.

During interviews with different parties within the maritime sector, just a few mentioned cases of cyber incidents within their own organizations. A Dutch ship-owner explained that cyber security was brought to their attention when they noticed irregularities within the ICT infrastructure of the office. It then became apparent to them that this could impact the ship operations as well. In 2016, a survey was conducted by IHS Fairplay in association with BIMCO. 21% of the 300 respondents confirmed that their company's computer systems had been violated. Of those respondents 67% experienced IT downtime, 48% lost corporate data and 21% endured some form of financial loss (Good, 2016). 50% of the respondents, who experienced an attack, suffered a loss between $5.000 and $50.000.

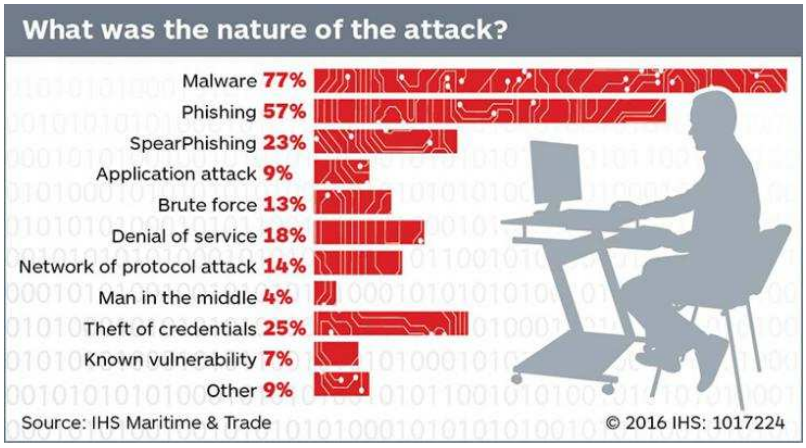


Fig 2. Overview type of attacks, survey IHS Fairplay & BIMCO 2016

When information and communication systems are damaged and information is used, modified or exploited without authorization it has a negative economic result for companies in all industries, maritime included. The IBM X-Force® Research 2016 Cyber Security Intelligence Index showed that the transportation industry was fifth, in a list of most targeted industries in 2015 (healthcare being first). During the Digital Ship Maritime Cyber Resilience Forum Rotterdam (2017), the firm Hudson Analytics, gave a presentation on the maritime cyber risk. They argued that the maritime sector could be a target for cyber threats, because: stakeholders exchange lots of information across different organizations, substantial amounts of money are involved in transactions, stakeholders each have their own process systems and most people working in the maritime sector speak a non-native language. Broker Willis Towers Watson stated that the prolonged economic struggles of most shipping lines have made the maritime sector more sensitive to risk than other modes of transport. Due to the decreased revenue of the last years and the investments needed to adjust ships to comply with new regulations, the financial capacity to invest in cybersecurity measures is limited.

Although irregularities within the ICT infrastructure are not always known and many incidents stay unreported, the above cases and survey results prove that cybersecurity should matter to the shipping sector. Although there are no concrete numbers available on the impact of cyber incidents, the examples above and study shows that the maritime sector is at risk. Cybersecurity, thus, is a real issue and of genuine concern for companies operating in the maritime domain.

§ 2.3. Causes

The cause of cyber incidents can be quite different, since there is a wide spread of cyber threats.
Aon Global Risk Consulting mentions three main categories for cyber incidents; technical failure, human failure (unintentional acts) and deliberate attacks (such as criminality) (ABN AMRO et al., 2016). In the recommend practice of DNV GL (DNV GL AS, 2016) there is also a distinction made between unintentional threats and intended/targeted threats. In most cases, cyber systems and data are compromised unknowingly, for example by unsuspecting users or undetected weaknesses in software.

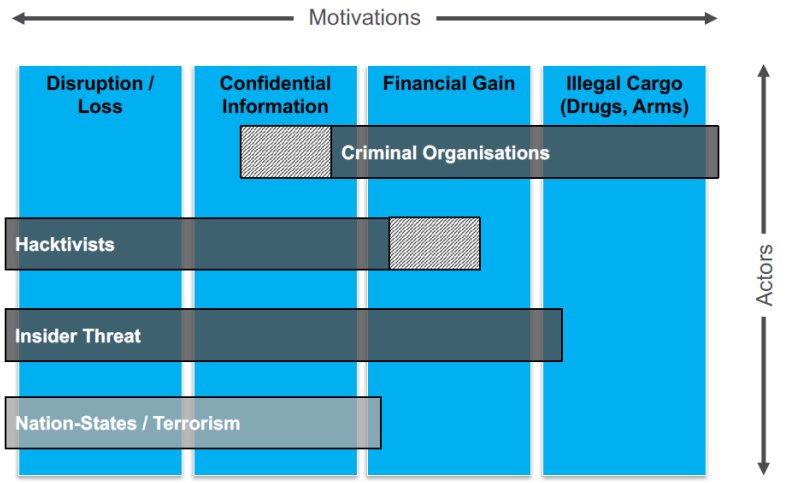


Fig 3. Motivations for cyber-attacks (Marlink, 2017)

The actors behind deliberate attacks differ. As shown in paragraph 2.2., most examples you will read in the newspaper involve criminal organizations. In the case of Port of Antwerp, the actors were 'criminal organizations' with the motivation to transport illegal cargo.

In figure 3 an overview is given of types of actors behind intended threats (Marlink, 2017). Deloitte describes four threat profiles, in which they make a distinction between fast and slow attackers. Fast attackers are more opportunistic and apply the same method for multiple targets, that are vulnerable for attacks. The table beneath shows the four threat profiles in relation to the main targets, which are explained in paragraph 3.1.

Table 1: Threat profiles (Deloitte, 2016)

Threat profile	**Sophistication**	**Abuse rate**	**Main targets**
Espionage	High	Low	Strategic Information, Intellectual Property
Advanced Crime	High	Low	Liquidity Integrity, Strategic Information
Mass Crime	Low	High	Liquidity Integrity, Privacy-related Information
Disturbance	Low	High	Operational Continuity

§ 3 Cybersecurity, the drivers

In this paragraph, the drivers on cybersecurity are discussed. It explains why cybersecurity matters to companies within the maritime sector.

§ 3.1. Risks

Risk is defined in ISO/IEC Guide 73 as a "*combination of the probability of an event and its consequence*". The definition of cyber risks according to The North of England P&I Association is; "*Means any risk of accidents, incidents, financial loss, business disruption, or damage to the reputation of an organization through failure of its electronic systems or by the persons using those systems.*"

Amongst the risks at stake are interruption of operations, loss of information, damage to a companies' reputation and impact on privacy. Furthermore, a company could be in breach with the law or act against contract conditions (for example leaking confidential information). Moreover, in large companies, board members have fiduciary duties. They require them to balance their targets for profitability with managing corporate risks, such as cyber threats. When a cyber-incident leads to leak of information, shareholders could question the fiduciary responsibility.

A recent study from Deloitte on cyber values at risks, comprehends a list of seven information assets that could be at risk and lead to impact on economic value (Deloitte, 2016). These information assets are described in the table underneath. In this study fourteen sectors were examined. Operational continuity and privacy-related information are the information assets which are most important to the Oil, Gas & Chemicals sector and Transportation sector.

Table 2: Information assets (Deloitte, 2016)

	Information asset	***Threat description***	***Main value impact***
1	Operational continuity	Availability of ICT systems related to operations, including income	Income
2	Control Integrity	Control over non-cash assets or customer products (unwittingly) lost	Assets
3	Intellectual Property	Competitive advantage from investment into IP (partially) lost	Equity
4	Strategic Information	Loss of company confidential information may lead to (M&A) opportunity loss and impair growth	Growth
5	Third Party Information	Leakage of confidential information on third parties may lead to loss of clients	Market share
6	Privacy-related Information	Confidential information on persons (including employees) may lead to loss of customers and talent	Market share
7	Liquidity Integrity	Financial transactions that are initiated or altered by cyber fraudsters may lead to direct financial losses	Liquidity

1) Operational continuity

Availability of ICT systems related to operations is essential for the shipping industry. Costs involved with downtime due to systems failing to function are high. Cyber-attacks cost UK oil and gas companies around 400 million pounds a year. It was estimated that the cost of cyber-attacks against oil and gas infrastructure will cost energy companies almost 1.9 billion dollars by 2018 (Wagstaff, 2014).

The Deloitte study on cybersecurity estimated that in the Oil, Gas & Chemicals sector the information asset 'operational continuity' leads to approximately 71% of the risk. In the Transportation sector

'operational continuity' is the information asset with the highest risk involved as well (Deloitte, 2016). In the IHS Fairplay / BIMCO survey of 2016, 27% of the respondents who were attacked, experienced system downtime or server disruption.
The inability of continuing the operations has a direct impact on the revenue of a company. Furthermore, companies unable to perform the reputation of responsible and reliable business partner are also at risk.

2) Privacy related information
This category refers to information on for example crew and/or passengers, which is commercially sensitive or confidential. It strongly relates to the category on third party information, for example data on cargo and passengers, which can be commercially sensitive and/or confidential.

The privacy issue is also important with regard to the EU General Data Protection Regulation. The EU/EEE regulation 2016/679 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) was approved in April of 2016 and will be enforced in May 2018[1]. Due to this regulation both public and private organizations are compelled to take actions to protect data and herewith the privacy of their employees as well as their customers. Larger organizations must appoint a security officer and incidents should be reported within 72 hours. This is relevant for the cruise, ferry and yachts market in particular.

§ 3.2. Regulations and standards

Although there are frameworks and guidelines on cybersecurity (further discussed in paragraph 5), there are not many regulations (yet) for cybersecurity. This seems odd: if maritime systems, essential for navigation and safety, are compromised then the ship itself forms a potential hazard, especially when this occurs in busy waterways. As the GPS spoofing example illustrates, it is possible to have a correct display of chart information, while in the meantime the course of a vessel is being changed.

In current regulations, the focus is on physical security and not so much on cybersecurity. However, in both the International Safety Management (ISM) code as well as the International Ship and Port Facility Security (ISPS) code, reference is made to manage information system security on board ships. BIMCO mentions that company plans and procedures for cyber risk management should be complementary to existing security and safety risk management requirements contained in the ISM Code and ISPS Code.

Table 3: Cybersecurity in relation to ISM & ISPS

Measure	Reference	
1	Do an assessment of the ship's information security systems (ISS including Information technology (IT) and operational technology (OT)).	ISPS Code - B8.3
2	Apply the physical protection measures for the ship's information systems (priority is given to the restricted areas of the ship).	ISPS Code - A9.4.2
3	Draft a company information systems policy for the ship.	ISM Code, chapter 1
4	Train the crew on the ship's information systems.	ISM Code, chapter 6
5	Apply best practices in management of information systems on board the ship.	ISM Code, chapter 7
6	Apply checking on interchanges by the information systems on board the ship.	ISM Code, chapter 7

[1] The Dutch law already effectuated the Algemene Verordening Gegevensbescherming 2016/679 (AVG) which is similar to the EU/EEE regulation.

7	Implement an operational continuity plan for after an incident.	ISM Code, chapter 8
8	Manage the ship's information systems incidents.	ISM Code, chapter 9
9	Implement checking of activity of the ship's information systems.	ISM Code, chapter 12

Apart from the references in the ISPS code and the ISM code, some regulators are more specific. The U.S. Coastguard, for example, has published their Cyber Security Strategy in 2015. This leads to a set of cyber hygiene requirements for vessels in US waters. In December 2016, the U.S. Coast Guard published a CG-5P Policy Letter 08-16. This letter, for vessels and facilities that are regulated by the Maritime Transportation Security Act, clarifies what type of cybersecurity events constitute in suspicious activity such as a breach of security that must be reported to the National Response Center. There are no ISO/IEC standards for cybersecurity on board yet. However, for security of information assets, the ISO/IEC 27000 family of standards could be helpful. ISO/IEC 27001 provides requirements for an information security management system (ISMS). An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process. Furthermore, the IEC-62443 offers a series of standards that define procedures for implementing electronically secure industrial process measurement and control systems. This guidance applies to end-users, system integrators, security practitioners and control systems manufacturers.

§ 3.3. Insurability

Most insurance policies that cover ships, shipyards and cargo-handling facilities include a Cyber Attack Exclusion Clause (CL 380) 10/11/2003. This clause excludes any loss, damage or liability caused either directly or indirectly by the use of a computer and its associated systems and software "as a means of inflicting harm". Standard marine insurance policies refer to tangible property being damaged, but it is unclear whether damaged software and computer systems would be considered as such. In a report on cybersecurity of Marsh & McLennan Companies (2014) they refer to the coverage gap: *"Insurers were unable to gauge the probability of a loss which, in turn, meant they were unable to put a price on the exposure. Consequently, insurers (and their reinsurers) began excluding losses as a result of a cyber-attack from their policies"*.

Specific cyber insurance policies are offered to fill this gap and could cover potential losses that might arise because of a cyber-incident. Furthermore, these insurance policies could cover additional costs, such as legal expenses and crisis management costs. According to the global law firm Norton Rose Fullbright (2016) the cyber insurance market is growing in several regions, not least in Europe. The Dutch Association of Insurers mentions that cyber insurances are today considered as a niche market, since they are primarily existing of subsidiaries of foreign insurers (from a Dutch perspective).

For cyber risks the more accepted methods for risks assessment are hard to apply, since risks are mostly assessed on past information and data. Cyber risks are relatively new and when issues occur they are not always known and/or reported. On a research and survey on cyber security FutureNautics (2016) state: *"… insurers are struggling to quantify the potential impact of cyber breaches on their clients and develop the policies necessary to protect shipping and marine companies, whilst lenders are waking up to what could be huge risks in their portfolios."*

This struggle to quantify the potential impact translates to the price of cybersecurity insurances. Insurance policies are relatively low priced, but the expectation of these prices will rise when insurance companies get better insights on the actual risks and costs. Currently, insurers are aiming to get a larger customer base, so they can create more accurate risks assessments. The BIMCO Association expects to see cyber clauses in shipping contracts, which might increase the demand for cyber insurance policies as well.

The question ‘who is accountable for what?’ is an interesting one, and unanswered by most people. Where best practices are shared on the technical aspects of cyber incidents, it could be sensible to share information on the distribution of responsibility as well. Maritime insurance companies could play an important role in this.

§ 4 Challenges within the maritime domain

As mentioned in the introduction, ICT could help shipping companies to reduce costs. Today many onboard systems are being monitored from shore, using onboard sensors and data transmission via satellite. Remote monitoring enables both fleet management and suppliers to retrieve information on the status of the systems 24/7 through online portals. Satellite connection providers form the connectivity link. Equipment suppliers use the transferred data to monitor performance of their products and for product improvement. With advanced technology, it is also possible for suppliers to use this data in providing fleet managers with advice on the condition of the systems and predict failures of systems.

The above describes the situation as it is today. However, the predictions of companies such as Rolls-Royce and Wärtsilä are clear; within the next ten years onboard systems will be managed from an onshore control center, where operators manage several vessels, access systems and intervene when necessary. Moreover, more systems are equipped with an IP number to make Internet connection possible (Internet of Things). This also requires continuous connectivity for onboard systems.

From control onboard, to remote control, to interactive remote control, to autonomous shipping. Every growth strategy requires sharing information and trusting people, it is inevitable that this leads to cyber risks. Within the maritime domain, there are a few specific challenges.

§ 4.1. Number of parties involved and lack of uniformity

As stated in paragraph 2.2. there are many parties involved in the logistic supply chain. Lots of information is exchanged between different organizations, such as cargo owners, terminal operators, ship managers, vendors / charters, ship owners, system integrators (shipyards) and equipment suppliers (see figure 4).

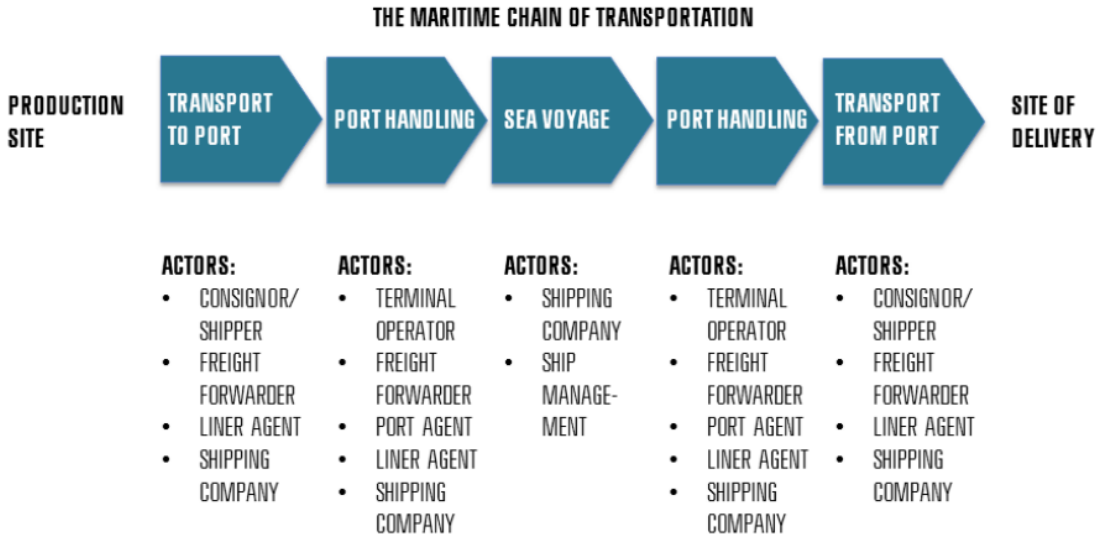


Fig 4. The maritime chain of transportation (Roslyng Olesen, 2015)

The above chain illustrates a simplified situation for the transportation market (liner, bulk and specialized shipping). In market segments where ships are needed for operations, such as dredging, the above situation is less complicated, but there are still many partners involved.

The beneath figure, for example, shows a common communication infrastructure for connected ships.

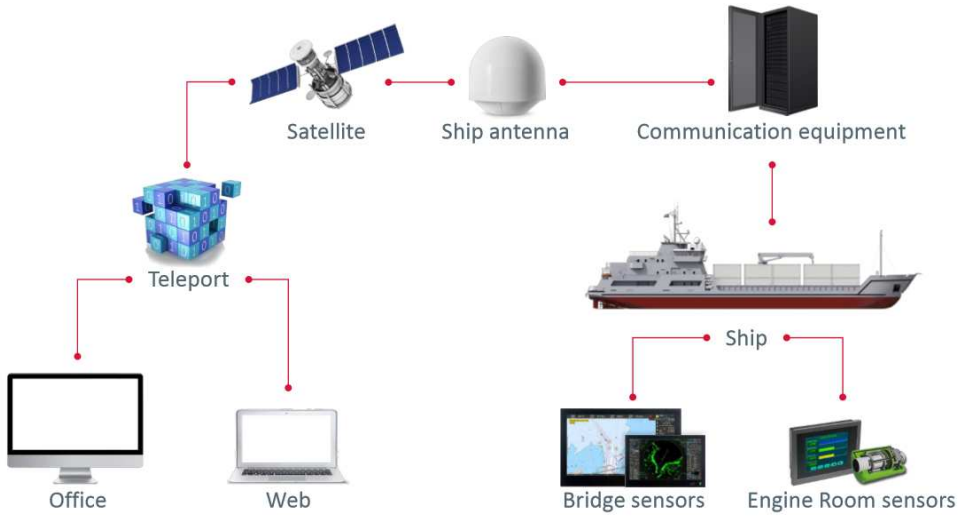


Fig 5. The connected ship (Transas, 2016)

The shipping industry consists of 50.000 merchant ships incorporating different systems and configurations. Many ships and offshore units make use of outdated platforms and operating systems with a patchwork of hardware and software. Furthermore, many onboard networks are intertwined. Most operating systems onboard run on Microsoft, but the applications are very diverse. There is no uniform standard for software used onboard.

This works in two ways; it makes the sector more resilient, but it may also slow the adoption of innovative technology. As director Tore Morten Olsen, director of Marlink, stated in an article in Digital Ship; "*It could even be viewed that the threat of cyber-crime is slowing adoption of contemporary technologies that could make shipping safer and more effective as a whole. For instance, the slow uptake over-the-air ECDIS updates may be linked to a reluctance to connect such sensitive systems to the Internet" (Olsen, 2016)*.

The complexity of the IT infrastructure could potentially lead to a lack of accountability. To reduce the risk of cybersecurity it is important for parties within the chain to be aware of their specific role to define the responsibilities. This is further discussed in paragraph 5.

§ 4.2. Integration challenges of IT & OT

To manage the fleet as a whole, shipping companies should deal with integration challenges between Information Technology (IT) and Operation Technology (OT).

IT systems process, store and transmit digital data. OT is used to manage and control industrial processes in a safe and efficient manner. A category of OT technology is referred to as Industrial Control Systems (ICS). These are systems used to monitor and control industrial processes, including the supervisory control, data acquisition and distributed control systems. Many OT systems were originally built as stand-alone systems with a single purpose, which had to be operated by manual or specific electronic controls. Security for the OT department thus meant physical security and cyber risks were low. The OT and IT department were managed as separate departments.

This situation has changed, due to the availability of innovative technologies, the desire of fleet managers to optimize the performance of their fleet and to manage their resources proactively. The ‘air-gap’ between ship and shore is diminishing. The expectation is that this will no longer exist in the future.
Currently many operational systems generate data which is send to shore, for the sole purpose of monitoring. When this connection changes from access to monitor in access to intervene, it becomes even more challenging. This will require ‘opening up’ of OT systems and connecting them with the Internet. Open and interconnected systems that provide benefits also introduce cybersecurity risk to the processes.

§ 5 Frameworks and guidelines on how to manage cyber risks

In various publications, such as a report on cybersecurity for logistic service providers (ABN AMRO et al., 2016), it is mentioned that companies should accept the impossibility to exclude digital incidents. They will occur, but the way they are managed could considerably reduce the damage.

Several frameworks and guidelines were published to give companies in the maritime domain insights on cybersecurity and to support ship owners in the management of cyber risks. The most well-known are;

- BIMCO Guidelines. The guidelines published in 2016 will be updated with paragraphs on 'insurance', 'ship-port interface' and a part on BYOD (bring your own device).
- ABS Guidelines
- Interim Guidelines on Maritime Cyber Risk Management: IMO-MSC 1/CIRC 1526 June 1st, 2016
- The Cyber Security Framework of the National Institute of Standards and Technology, U.S. Department of Commerce (NIST)
- DNVGL-RP-0496, Recommended practice; Cyber security resilience management for ships and mobile offshore units in operation.

Although the above guidelines have some general rules (which are relevant for every sector), they consider the challenges within the maritime domain. They differ from target audience and level of detail, but have the following steps in common:

1. Identify what's at risk and gather information on possible threats and vulnerabilities within the organization

It helps to use a holistic approach in which cybersecurity is a) part of business operations and b) part of the safety and security culture and responsibility of the board of directors and organizational commitment. Any procedures or measures taken to reduce cyber risks might grasp into other procedures within the organization.

Each organization should develop a form of organizational understanding of the stakes involved and the cyber threats that could impact the organization. By knowing the crown jewels of the company, measures can be taken to protect them. Risk management starts with an assessment of the risks to weigh off the effects of the risks versus the costs involved. A risk assessment is intended to identify those factors that must be considered for risk reduction, mitigation, transfer or acceptance. In the risk assessment, vulnerabilities should be identified, such as web browsers, USB ports, wireless routers, entertainment systems, printers, systems with Wi-Fi connectivity, et cetera.

Not only direct risks matter, but the indirect risks are important as well. Indirect risks are first and foremost the concern of parties within your supply chain, such as suppliers and customers. Their quality of risk management directly influences your organization. Vulnerability of their network may impact your network. As described in paragraph 4.1. the complexity of the IT infrastructure could potentially lead to a lack of accountability. To overcome this gap, the BIMCO guidelines offers tips for third party risk assessments, and concrete working arrangements are discussed in the Recommended Practice of DNV GL (DNV GL AS, 2016). The phases include:

- Identifying the main producers of critical shipboard IT and OT equipment;
- Reviewing detailed documentation of critical OT and IT systems, and their interfaces;
- Identifying cyber security points-of-contact at each of the producers and establish working relationships with them;

- Reviewing detailed documentation on the ship's maintenance and support of its IT and OT systems;
- Establishing contractual requirements and obligations that the ship-owner/ship operator may have for maintenance and support of shipboard networks and equipment.

2. Prevent and protect your organization from cyber incidents

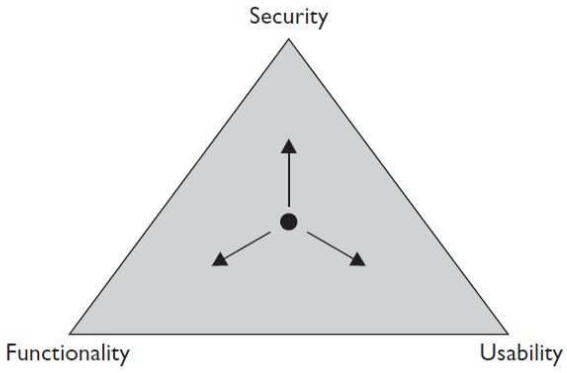
Once you know the possible threats, the vulnerabilities within the organization and the risks you face, it is possible to develop protection and detection measures, to prevent cyber incidents take place.

In virtually all guidelines the advice is given to segregate the networks. The advice to split the networks for safety and critical systems from other networks is not only sensible for a cybersecurity perspective, it also gives insights in the usage of bandwidth which helps ship-owners / managers to control their investments and expenditures on ICT.

The NCC Group, a cybersecurity and risk mitigation company, proposes to segregate the network in different groups related to the importance of their functionality:

1) Maritime systems for navigation and safety, such as ECDIS (Electronic Chart Display and Information System), AIS (Automatic Identification System) and GMDSS (Global Maritime Distress and Safety System.
2) Operational technology network, necessary for a vessels' performance. This includes functions such as engine management and performance, drilling system control, ballast system control, ballast system control, propulsion plant control and fuel and cargo handling.
3) The third network is related to the IT systems, for the back office, needed for fleet and inventory management, contact with the back office via email, et cetera.
4) This network relates to crew welfare and covers crew internet access and multimedia solutions. This network is hard to control, since most crew members bring their own devices on board.

Apart from network segregation other advices are related to: access and user management, configuration management (of both hardware and software), protective software (firewall, antivirus), secure satellite and radio connection. Updates for hardware and software are necessary for maintaining a cyber secure situation. It is recommended for both ship-owners and suppliers to consider not only the initial costs for products and systems, but to view it from a lifecycle perspective.



To answer the question if your organization has done enough it might be helpful to think of the level of security as a dot, positioned within a triangle, between the corners 'security', 'functionality' and 'usability'.

If the organization aims to be fully secure, then it might have to give up a certain degree of functionality and usability. The most cyber secure organizations are those that are transparent, they understand the meaning of agility & resilience and are familiar with trial and error.

3. Monitor and detect anomalies and incidents within your systems

In the NIST Framework three subcategories are determined for the action 'detect', which are: anomalies and incidents, security monitoring and detection processes.
The DNV GL guidelines add another subcategory, namely testing both components and systems. By testing it is possible to verify if the mitigation actions (as described above) are in place. The testing could be performed by a third party. A well-known method is penetration testing. With pen-testing an authorised third party tests the weaknesses of a computer system to gain access. This can be performed upfront, to identify initial weaknesses, but also when measures and procedures are in place.

Identification of the occurrence of a cyber incident is essential, to prevent hackers from entering your systems unknown. When inside, they could wonder around and get insights in all processes and systems. This was the case for the Port of Antwerp (see paragraph 2.2). It might be helpful to keep track of usage patterns: if a specific device has started consuming more bandwidth then normal, then it could have been compromised by criminals. User access can be set based on specific time slots according to shift patterns.

Some organisations choose to invest heavily in logging and security analytics, especially for the IT systems, and less in protection. Furthermore, the prevention of abuse (for example encryption), should be considered.

4. Respond and recover to reduce the impact and prevent more damage from being done by being transparent

When a cyber incident has occurred, and detected, it is important to have a response and recovery plan. This supports an organization to take action regarding a detected cyber security event and to restore damages done. This is not just a technical matter (of back-up systems), it is just like every other safety incident just as important to invest in crisis management, legal support and communication. Personnel should know their roles and responsibilities, suppliers should be involved and clients / customers should be informed about the incidents and any consequences.

Veiligheid oefening in de haven. Het havengebied is voor kwaadwillenden een tot de tand toe gevulde snoeppot

VEILIGHEID

Offensief haven om hackers buiten de deur te houden

De afhankelijkheid van IT neemt toe en dus ook de risico's. Het Havenbedrijf wil nu een centrale aanpak. Digitale zwaktes moeten bespreekbaar worden.

Door **Maurice Geluk**

ROTTERDAM. Terwijl de haven in hoog tempo digitaliseert, beschermen tal van bedrijven hun IT-systemen onvoldoende. Dit leidt tot risico's op het gebied van cybersecurity. Het Havenbedrijf Rotterdam (HbR) stuurt aan op een inhaalslag, een expert pleit voor een centrale aanpak.

Het 42 kilometer lange havengebied is voor kwaadwillenden een tot de rand toe gevulde snoeppot. Circa 700 bedrijven zijn er actief, waarvan vele aan de lopende band innoveren. Jaarlijks passeren ruim 12 miljoen containers (TEU's, 30.000 zeeschepen varen in en uit.

Informatie over de locatie van een partij cocaïne is voor criminelen goud waard, toont de recente rechtszaak tegen de corrupte douanier Gerrit G.. Datatikkie geldt voor inlogcodes, bankgegevens of de heimelijke details rondom een grote overname. Het maakt bedrijven, vooral medewerkers, kwetsbaar.

Ondat bedrijven almaar afhankelijker worden van IT, heeft het HbR digitalisering recent tot speerpunt gemaakt.

Neem de in 2015 gestarte en volledig geautomatiseerde containerterminal van APM Terminals op de Tweede Maasvlakte. Volgens risicomanager Stefan Huyvenaers sheeft het voorkomen van „downtime bij het vlaggenschip" van deze Maersk Group-dochter topprioriteit. „Vertraging levert ons en onze klanten significante schade op." Er zijn kwaadwillenden die graag willen weten waar een container is en die hoe ze die te pakken kunnen krijgen omdat er bijvoorbeeld drugs of een andere kostbare lading in zit. Of juist een terminal voor de lol willen platleggen. Omdat ze steeds professioneler te werk gaan, moet de digitale beveiliging omhoog.

Digitale beveiliging is ieders eigen verantwoordelijkheid. Van multinational tot ondernemertje. Ronald Prins, oprichter van cybersecuritybedrijf Fox-IT vindt dat het afgelopen moet zijn met deze „ontheid-bij-heid". Bij haat kan ook elk voorbeeld. Daarvan is bekend dat het overal digitaal ontdoend. We slecht beveiligd is, maakt geen schijn van kans. Ook neemt bij gevallen van digitale spionage in de haven waarbij gevoelige bedrijfsinformatie werd gestolen.

De zogenoemde *port cyber resilience officer*, afgelopen zomer benoemd, moet partijen zoden tot elkaar brengen. De aandacht gaat met name uit naar het verhogen van bewustwording rondom cyberdreigingen, zoals phishing en ceo-fraude (emails ongeautoriseerd afkomstig van de directeur). Probleem is dat de bereidheid om digitale zwaktes te bespreken, laag is vanwege de concurrentiegevoeligheid.

Prins, van Fox-IT, signaleert dat de „grote jongens" goed doorhebben dat het beschermen van hun primaire bedrijfsprocessen cruciaal is. „Maar bij kleine bedrijven is digitale beveiliging een sluitpost." De oud-hacker ziet een oplossing in het oprichten van een centrale meldkamer. „Samenwerking op de werkvloer is noodzakelijk. Je wil van elkaar weten wat er op dit vlak gebeurt."

Professioneel
Hackers 'rammelen dagelijks aan poort'

Het Havenbedrijf Rotterdam (HbR) ziet dat de professionaliteit van cyberaanvallen toeneemt. „Hackers verdiepen zich actief in bedrijven", aldus Martijn van Schaick, expert digitale beveiliging bij de havenincidentenbestrijder. Bij het HbR zelf wordt dagelijks aan „de poort gerammeld". Grote incidenten hebben zich bij dijn weten niet voorgedaan. Overzicht ontbreekt echter.

Om bedrijven waar het geld voor dure, externe beveiligingsexperts ontbreekt op weg te helpen, bekijkt het HbR de mogelijkheden voor een collectieve regeling. Deelname moet zorgen voor een betaalbaar niveau van gezamenlijke beveiliging op de werkvloer tussen de verschillende havenspelers.

In all guidelines and reports on how to become cyber resilient 'transparency' on cybersecurity is encouraged: Open about incidents, cyber breaches and share cases with companies within the same industry and/or the supply chain. Although this is difficult in a supply chain (companies are not always eager to confess their weak spots to the clients) it could be beneficial for both. This is one of the motivations of the Port of Rotterdam to launch a Cyber Resilience Program. Port Cyber Resilience Officer René de Vries states in an interview on this topic: "*Preventing cyber criminality will be a focal point in the future. Off course we have our own systems in place, but we want to share our knowledge in this field with the eight hundred companies within our port.*" (Steenhoff, 2016). The project FERM (no abbreviation, but the Dutch word for firm/steady) is also part of the program and provides companies within the port with information and practical tools on cyber security.

5. Make sure your employees are educated and continuous aware

In most guidelines education and awareness is seen as an important part of prevention and protection, but education and awareness are important in all phases. According to the 2015 Crew Connectivity Survey 2015 (Adamson, 2015) of over 3,000 crew members, only 12% had received any form of cyber security training; only 43% of the crew were aware of any cyber-safe policy or cyber hygiene guidelines provided by their company for personal web-browsing or the use of removable media (USB memory sticks etc.). During the Digital Ship Maritime Cyber Resilience Forum Rotterdam (2017) a Dutch ship-owner mentioned: "*All the recent incidents in our company could have been prevented from single users being more alert. Safety is everybody's responsibility.*"

Employees should be aware of the risks of cyber security, but more importantly they should be aware of their digital behavior in relation to cyber security. It's not just an issue for crew on board, but also for office personnel and third parties logging into the systems. Furthermore, several maritime educational institutes argue that simulation of cyber incidents should be part of the curriculum of students, so that it becomes part of their education and basic skills.

Appendix I – Sources

ABN AMRO, TLN, & Aon Risk Solutions. (2016, November). *Cybersecurity voor logistiek dienstverleners.* Retrieved from https://insights.abnamro.nl/2016/11/cybersecurity-voor-logistiek-dienstverleners/

ABS. (2016). *Guidance notes on the application of cybersecurity principles to marine and offshore operations*. Retrieved from http://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/221_Guidance_Notes_Cyber_Safety_Principles_Maritime_Operations/Cyber_Security_v1_GN_e.pdf

Adamson, R. (2015, September). *Evolution of maritime data* [PowerPoint slides FutureNautics – Digital Ship CIO Forum Rotterdam]

BIMCO. (2016). *The Guidelines on Cyber Security onboard ships*. Retrieved from www.bimco.org/News/Press-releases/20160104_Cyber_security_guidelines

CSIS. (2015, July 22). *Coast Guard Commandant Addresses Cybersecurity Vulnerabilities on Offshore Oil Rigs.* Retrieved from www.csis-tech.org/blog/2015/6/22/coastguard-commandant-addresses-cybersecurity-vulnerabilities-in-offshore-oil-rigs

Decool, P. (2017, January). *The reality of shipping's cyber challenge* [PowerPoint slides Marlink - Digital Ship Maritime Cyber Resilience Forum Rotterdam]

Deloitte. (2016). *Cyber Value at Risk in the Netherlands*. Retrieved from www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-cyber-value-at-risk.pdf

DNV GL AS. (2016). *Recommend practice: Cyber security resilience management for ships and mobile offshore units in operation* (DNVGL-RP-0496). Retrieved from www.dnvgl.com/news/dnv-gl-launches-recommended-practice-to-enhance-the-cyber-security-of-maritime-assets-74585

Good, N. (2016, September 19). *IHS Fairplay Maritime Cyber-security Survey – the results.* Retrieved from http://fairplay.ihs.com/article/4275151/ihs-fairplay-maritime-cyber-security-survey-the-results

HLN.be. (2013, June 17). *Recordvangst heroïne in haven van Antwerpen*. HLN.be. Retrieved from www.hln.be/hln/nl/957/Binnenland/article/detail/1653473/2013/06/17/Recordvangst-heroine-in-haven-van-Antwerpen.dhtml

IMO (2016). *Interim Guidelines on Maritime Cyber Risk Management: IMO-MSC 1/CIRC 1526 June 1st 2016.* Retrieved from www.safety4sea.com/wp-content/uploads/2016/06/IMO-MSC1-Circ1526-Interim-Guidelines-on-Maritime-Cyber-Risk-Management-2016_06.pdf

Marsh & McLennan Companies. (2014). *The risk of cyber-attack to the maritime sector.* Retrieved from https://uk.marsh.com/Portals/18/Documents/The%20Risk%20of%20Cyber-Attack%20to%20the%20Maritime%20Sector.pdf

Olsen, T. M. (2016, September). *Cyber security - a practical approach*. Digital Ship, 2016(117), 24-25.

Popular Mechanics. (2016, March 2). *Sea Pirates Hacked a Shipping Company To Figure Out Which Vessels to Plunder.* Retrieved from www.popularmechanics.com/technology/infrastructure/a19719/sea-pirates-hacked-a-shipping-firm/-oil-rigs

Roslyng Olesen, T. (2015, December). *Value creation in the maritime chain of transportation* (The role of carriers, ports and third parties in liner and bulk shipping). Retrieved from

http://openarchive.cbs.dk/bitstream/handle/10398/9252/Mapping_Report_C_Value_Creation_2nd_Edition.pdf?sequence=3

SeaFocus. (2016, January 7). *Maritime Cyber RiskPlunder.* Retrieved from www.seafocus.fi/maritime-cyber-risk

The North of England P&I Association. (2016, June). *Loss prevention briefing: Cyber risks in shipping.* Retrieved from www.safety4sea.com/wp-content/uploads/2016/06/North-Club-LP-Briefing-Ships-Cyber-Risks-in-Shipping-2016_06.pdf

The University of Texas at Austin. (2013, July 29). *UT Austin Researchers Spoof Superyacht at Sea*. Retrieved from www.engr.utexas.edu/features/superyacht-gps-spoofing

U.S. Coast Guard. (2016). *Maritime Bulk Liquids Transfer Cybersecurity Framework Profile*. Retrieved from www.uscg.mil/hq/cg5/cg544/docs/Maritime_BLT_CSF.pdf

Verbond van Verzekeraars. (2016, September 29). Meer bewustwording nodig rond cybercrime. Retrieved from www.verzekeraars.nl/actueel/nieuwsberichten/Paginas/%E2%80%98Meer-bewustwording-nodig-rond-cybercrime%E2%80%99.aspx

Verizon. (2016). *Data breach digest. Scenarios from the field.* Retrieved from www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf

Wagstaff, J. (2014, April 23). *All at sea: global shipping fleet exposed to hacking threat.* Retrieved from www.reuters.com/article/us-cybersecurity-shipping-idUSBREA3M20820140423