MARITIME CYBER-RISKS

10/15/2014

Virtual pirates at large on the cyber seas

The maritime industry is shown to be vulnerable to a wide array of cyber risks, and multiple examples of actual breaches have been seen. However, cyber defenses do not appear to have been developed adequately addressing the threats being faced.

Maritime Cyber-Risks

Table of Contents

Issued by :

CyberKeel , Copenhagen, Denmark

For contact details see: www.cyberkeel.com

With technical support intelligence provided by ClearSky (www.clearskysec.com)

Introduction

When the term "cyber risk" is mentioned, this typically invokes one of three different mental associations with most people. Either it signals that this is a highly technical area on which they have little or no influence, or that this is the realm of writers of action movies featuring geeky characters or finally that this is something which only happen to someone else. This behavior is replicated for the majority of business industries, including the maritime sector.

At CyberKeel, our focus is specifically on the maritime sector and with this whitepaper we will address the current status of cyber risks and cyber security in the industry – and it is clear that the risks are significant.

The three typical reactions mentioned all lead towards the same behavior. Most people get to the conclusion that cyber security is the responsibility of the IT department, and apart from that there is nothing they can really do. Unfortunately this has a direct, and negative, impact.

Certainly some aspects of cyber security requires technical knowledge and skill, but need to be seen in the context of several other aspects which tend to be non-technical in nature.

First of all, management need to be involved in making decisions pertaining to the level of security a company wants, as very often increased levels of cyber security comes at the price of having to modify business processes in such a way that daily business operations might be impacted. It is then a clear strategic risk decision which has to be made, and not a specific IT decision.

Secondly, the most vulnerable attack point related to cyber security is people. Hacking into company systems using only your computer from afar, whilst possible, is often quite difficult if the company has good cyber defense systems. However, getting employees to do things online, which they should not do, or attacking the employees smartphones while they are at conferences, or getting physical access to an office and installing your own devices into employee computers, is much easier. Hence a defense strategy pertaining to cyber security can only be effective is it includes careful consideration as to how you want your people to behave, as well as how you actually get them to comply with any rules you establish.

The maritime industry is of paramount importance to almost all countries globally. Cyber attacks within this sector does therefore not only have ramifications for the companies involved, but also have national security implications as well as the ability to impact the finances of entire nations. Our aim with this whitepaper is to illuminate the current status in the industry, in order for the industry to use this as a starting point for increasing cyber defenses.

CyberKeel – www.cyberkeel.com

The current state of affairs in the maritime sector

Having approached multiple stakeholders and senior decision makers in the commercial maritime sector over the past 6 months, we have seen a pattern emerge. Although we do find some who are quite aware of cyber security issues, the general pattern we see amongst senior decision makers tend to revolve around one, or more, of the following approaches:

- Cyber security is a technical matter largely delegated to the IT manager or the CIO, and is not something materially involving the CEO, CCO, COO, CFO or the HR manager
- A general unawareness of the actual incidents which have taken place in the maritime sector, or sectors closely associated therewith
- A belief that the cyber threats are chiefly theoretical in nature, usually linked to a doubt as to whether there is anyone with a genuine motivation to perform cyber attacks against their own particular maritime company

These three aspects are of course all interlinked. As we see it, they are usually founded in a general unawareness of the nature of cyber risks. The entire "cyber" discussion is seen as highly technical, and is as such delegated to a technical IT department. In doing so it is neglected that cyber risks can only be dealt with effectively by included standard business processes, and not purely relying on IT. Secondly such an approach also overlooks the fact that a successful cyber attack will have direct impact on commercial and/or operational business processes. Such contingencies should be viewed no differently than contingency planning for – as an example - security for vessels in pirate-prone areas.

The tendency by many business managers to view cyber security as a technical matter often deters them from seeking information pertaining to actual incidents in the industry. And in cases where headlines of an incident have been noticed, there is often limited, or no, follow-up in terms of examining how such incidents would influence the non-technical parts of the company. In turn this leads to a blind spot in terms of business contingencies, which is a significant liability once a cyber attack is successfully implemented.

In order to address the perception that cyber attacks are technical in nature, we will in this this section outline a range of cyber attacks from the perspective of also demonstrating the non-technical elements. This is in order to ensure a realistic, and not theoretical, approach to the rest of this report.

Actual incidents or proof-of-concepts

Within the arena of cyber security, the amount of known incidents is likely to be a significant underrepresentation of the actual amount and magnitude of attacks taking place. This is due to two primary reasons.

One reason is that victims of successful cyber attacks have a tendency to keep such incidents secret. This is partly to avoid broadcasting to other cybercriminals that they might be "easy pickings", and partly to avoid being seen as "unsafe" by their own customers. The fear is that if a company publishes the fact that they have been breached and data have been stolen, this can cause customers to move their business elsewhere in a, possibly futile, effort to secure their own data. In some cases it might also be because broadcasting the nature of an attacks will cause the cyber criminals to pull out and change the nature of their attacks, eliminating the possibility to identify similar attacks already in progress.

The other reason being that a number of companies might simply be unaware that they have been breached. If the attack is aimed at stealing information, it might simply not be discovered by the company unless they make a dedicated effort to monitor their own electronic infrastructure. A large company which have not discovered any breaches of their networks, but at the same time have never looked for signs of such attacks, cannot safely assume that such attacks will not, or have not, hit them.

However, the above notwithstanding, a number of actual incidents in the maritime sector have indeed been uncovered and made public over the past few years, with an increasing trend seen over the past 12 months. Given the amount of unreported - and possibly undetected - incidents, it cannot be said for certain whether this increase in reported incidents reflects an increase in the incidents themselves or simply an increase in the reporting frequency. However, most experts in the field tend to agree that they are indeed seeing not only an increase in the amount of incidents but also in the level of sophistication used in the attacks.

The following section is a review of cyber incidents seen in the maritime sector, whether performed maliciously or as part of a test of cyber safety standards.

Stealing money by changing bank accounts

The latest example is reported in CyberKeel's October 2014 issue of the "Monthly Maritime Cyberrisks" based on collaboration with Clearsky. Technical specialists in ClearSky made a detailed forensics analysis of an actual attack illustrating not only the specific modus operandi, but also in the process uncovering the names of additional companies in the shipping industry being primed for the same type of attack. This type of forensics analysis

was additionally an illustration of the need for an inter-industry forum where such actionable intelligence can be shared on a confidential basis.

Basically it is an attack aimed at deceiving a company into transferring large monetary sums to a bank account owned by criminals. Furthermore it is a type of attack which cannot be defeated by purely technical solutions. Subsequent to this, it was published that the fuel supplier World Fuel Services (WFS) recently fell victim to a bunkering scam reported to have cost the company an estimated $18 million, where the approach involved what appears to be the same mode of cyber attack. Additionally, CyberKeel have learned of a third recent similar incident which, however, was detected and avoided at the last moment.

The nature of the attack was already known from other industries, but this time it was targeted directly at a number of maritime companies. In December 2013 the US Federal Bureau of Investigation issued a warning pertaining to this type of attack in December 2013. In this warning they referred to 3 specific cases whereby 1.65 million USD were transferred to the fraudsters.

Simply put, it involves a criminal organization which is able to position themselves "in the middle" of the email communication taking place between two companies. As such, each of the companies believe they are communicating directly with each other, but in reality both are communicating with the criminals, who can alter the information in the email at will.

The hackers had placed software within the company systems monitoring email correspondence, and this software was set to look for legitimate requests on the part of a supplier such as a change of bank account. At this point the hackers would step in as the man-in-the-middle and take over control of the conversation, ultimately ensuring that the money transfer would go to their own account and not to the legitimate supplier's account.

In order to launch such an attack it is sufficient to penetrate the systems at only one of the two companies involved. Hence even companies with a strong cyber security setup are vulnerable to this type of attack.

Such attacks are most likely against targets wherein large sums of money are transferred. In the specific case seen in September 2014, the attacks appeared primarily aimed at relations between shipping lines and bunker suppliers as well as shipping lines and shipyards.

Due to the nature of the attack, a technical solution safeguarding against this does not exist. Instead, it is generally recommended to implement business processes designed to avoid such fraud. Basically, a verification routine should be established independently of the electronic transfer of information. Something as simple as requiring a phone call to the

supplier to verify the information in the email would be effective – provided the phone number to the supplier was known before initiation of the first email. Having a test-transfer of just one dollar, and have the supplier verify it is equally effective – provided the supplier verification is by phone and not by email, as the email is compromised by the man-in-the-middle.

Deleting carrier information as to the location of all cargo

The Iranian shipping line IRISL suffered from a successful cyber attack in 2011[1]. According to Mohammad Hossein Dajmar the Managing Director of the Islamic Republic of Iran Shipping Lines, IRISL, a number of cyber attacks were committed against IRISL in August 2011.

The attacks damaged all the data related to rates, loading, cargo number, date and place. This meant that no-one knew where containers were, whether they had been loaded or not, which boxes were onboard the ships or onshore.

Making matters worse, the attack also proceeded to eliminate the company's internal communication network.

Even though the data was eventually recovered, it led to significant disruptions in operations and resulted in sending cargo to wrong destinations causing severe financial losses. Additionally, it was stated that a considerable amount of cargo was lost.

Zombie Zero – barcode scanners used as hacking devices

This example borders the maritime industry in as much as it was directed at the logistics industry. The attack was termed Zombie Zero, tailor made to attack logistics companies and was discovered in July 2014 by the company TrapX[2].

It consists of a cyber attack hidden within a piece of hardware – in this specific case it was embedded in a hardware scanner used by logistics companies. The attack was verified to be present within at least 8 different companies. In a specific case study made public by TrapX, they found 16 out of 48 scanners at the company to be infected with the malware. It is important to note that the malware was pre-installed within the scanners before delivery to the logistics companies.

[1] http://www.globes.co.il/news/article.aspx?did=1000714597
[2] http://www.trapx.com/wp-content/uploads/2014/07/TrapX_ZOMBIE_Report_Final.pdf

When the scanners were plugged into the company's network it launched a series of automated attacks searching the company network for the ERP financial server. Once the server was found, the attack would proceed to compromise the server. Next step of the automated attack consisted of establishing a remote connection to a location in China – a location which would then not only have complete visibility into the financial ERP system, but would also have the ability to modify the shipping database and thereby make packages appear and disappear.

According to TrapX, the remote control established by the attack was directed to an establishment in China which has previously been linked to the People's Liberation Army. The manufacturer providing the scanner was also located in the same physical area as the location of the remote control.

Zombie Zero is merely a tangible example of what is being labelled hardware attacks. These are attacks whereby the attacks takes place from within hardware which is being installed in the company. As such hardware is granted significant access rights within the network, it is an ideal place to embed an attack in order to bypass normal security barriers. From a business perspective this implies that caution has be exercised when evaluating potential suppliers of critical hardware.

Icefog – Japanese and Korean shipbuilding and maritime operations targeted

Security company Kaspersky published information pertaining to a attacked termed "Icefog" in September 2013[3]. It was a type of attack which was shown to have been ongoing since 2011, and aimed specifically at Japanese and Korean targets in a few business sectors whereof shipbuilding and maritime operations were explicitly listed.

The attacks were aimed at providing a backdoor access into the targeted companies in order to extract documents, email account credentials as well as passwords allowing access to resources within the network.

In addition to the attacks themselves, another aspect should be noted. Usually such attacks is aimed at establishing and maintaining access over extended periods of time. Icefog attacks were lasting only days or weeks. The attackers apparently knew exactly what they wanted to extract, and once they had obtained it they cleaned up and withdrew. This clearly indicates industry knowledge, or the willingness to obtain industry knowledge, in order to design a targeted attack.

Port of Antwerp used for drug smuggling

[3] http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_exposes_Icefog_a_new_cyber-espionage_campaign_focusing_on_supply_chain_attacks

In late 2013 it was made public that the Port of Antwerp had been subjected to a persistent cyber attack, which had been ongoing since June 2011[4]. The penetration allowed the attackers to have remote access to the terminal systems, and thereby they were able to release containers to their own truckers without knowledge of the port or the shipping line. Furthermore, the access to port systems was used to delete information as to the existence of the container after the fact.

When the attack was initially discovered and the remote access removed, a second attack wave was implemented. This included fitting logging devices in keyboards and monitors enabling continued operation by the drug smugglers.

When the operation was uncovered, Belgian and Dutch police found a ton of cocaine, guns as well as more than 1.3 million Euro in a suitcase. But given the operation had been ongoing for 2 years this might only be a fraction of the true scale of the operation.

That smugglers exist, and use containers as a vehicle for the smuggling operations, is certainly nothing new. However the method is clearly new and exposed what can best be described as "ghost shipping". Obtaining access to port, or shipping line, systems essentially provides the ability to ship any commodity anywhere, without anyone even knowing it is there.

Additionally, the Port of Antwerp incident also shows that it is possible to obtain a level of access to a container port whereby it is possible to manipulate the data indicating which containers are on the premises. In addition to drug smuggling, such access can also be used to identify high-value containers to be stolen, or be used to disrupt terminal yard planning, in turn causing severe congestion.

Bypassing Australian customs

In 2012 it was revealed that crime syndicates had penetrated the cargo systems operated by the Australian Customs and Border protection. The penetration of the systems allowed the criminals to check whether their shipping containers were regarded as suspicious by the police or customs authorities. The consequence was that containers with contraband were abandoned whenever such attention was identified by the criminals.

Publication of these findings also included information that it was known that at least one privately owned cargo tracking program relied on data provided by Australian customs, and that this system could be easily accessed by the criminals.

CyberKeel container carrier penetration test

[4] http://www.woodland-group.com/news/display/cyber-attacks-a-new-tool-for-drug-traffickers/402/60

CyberKeel tested indications of cyber security related to the 50 largest container carriers' websites split over February 2014 and September 2014. The tests were quite simple, and by no means comprehensive, and consisted of two main tests. One was a simple test of whether free available applications such as track&trace, schedule look-up and email query forms appeared to have been safeguarded against injection of malicious code, and hence potentially vulnerable for penetration to operational systems behind the applications. The other test was a search for online hardware using the search tool Shodan. Once hardware belonging to a named carrier was identified, the metadata associated with the hardware was cross-matched with known, publically available, hacker resources. Based on this it could be determined whether unauthorized access was likely given already known exploits in the market.

These simple tests showed that 37 out of the 50 largest container carriers appeared vulnerable to relatively simple penetration attacks. Subsequent penetration testing by CyberKeel on behalf of a number of shipping lines have verified the existence of such vulnerabilities.

AIS spoofing

Ship owners and operators can themselves manipulate AIS data from their own vessel. The most frequent manipulation of data, or shut-down of the AIS, is for transits through high-risk areas such as the Gulf of Aden in order to prevent pirates from picking up the signals and use the data to better coordinate an attack.

In October 2013, Trend Micro demonstrated how the AIS system could be penetrated quite easily, providing the attacker with a range of possibilities[5]. The following scenarios were shown to be possible using equipment having a cost just 200USD:

- Modification of all ship details, including position, course, cargo, speed and name
- Creation of "ghost" vessels at any global location, which would be recognized by receivers as genuine vessels
- Send false weather information to a vessel to have them divert around a non-existent storm
- Trigger a false collision warning alert, for some vessels resulting in a course adjustment
- The ability to impersonate marine authorities to trick the vessel crew into e.g. disabling their AIS transmitter rendering them invisible to anyone but the attackers themselves
- Create "ghost" search and rescue helicopters

[5] http://www.slideshare.net/trendmicro/captain-where-is-your-ship-compromising-vessel-tracking-systems

- Create a fake man-over-board distress beacon, triggering the alarm on nearby vessels
- Cause vessels to increase the frequency with which they transmit AIS data, resulting in all vessels and marine authorities being flooded by data. Essentially a denial-of-service attack

The key problem with AIS is that it has no built-in security. All information is automatically assumed as being genuine and hence treated as correct piece of information. Additionally, AIS messages are not encrypted and therefore very easy for outsiders to tap into and manipulate.

Facebook as pirate intelligence source

Whilst not a cyber-attack in itself, it is an example of the risks associated with vessels, and their crew, becoming online 24/7 via satellite links.

An offshore vessel had transited the Suez Canal and was travelling south through the Red Sea towards the Gulf of Aden. As mentioned in the AIS example, it is not uncommon for vessels for either disable their AIS, or set their AIS to transmit erroneous data, in order to prevent pirates from obtaining actionable intelligence to be used for hijacking the vessel.

Prior to arriving in the Gulf of Aden, it was discovered that a person onboard the vessel had been uploading significant amounts of images to a Facebook account. Images which provided a detailed look into the safety measures in place on the vessel. This was discovered prior to entering the Gulf of Aden and the vessel changed its planned course.

As mentioned, this is not a cyber-attack as such, however it does show that information from vessels, which had previously been regarded as offline, can now be transmitted to parties outside the vessel and potentially used for nefarious purposes.

Attacks on offshore installations

In 2010 a drilling rig was being moved at sea from its construction site in South Korea towards South America. Its critical control systems became infected with malicious software to such a degree that it had to shut down for 19 days in order to clear the issue. According to Michael Van Gemert from Lloyds Register Drilling Integrity Services this was only one of several such incidents[6].

[6] http://fuelfix.com/blog/2013/04/29/malware-offshore-danger-lurks-where-the-chips-fail/

According to security company ThetaRay, a cyber attack on a floating oil rig off the coast of Africa was tilted slightly and was forced to shut down. This took a week to identify and fix.

Vessel navigation controlled by hackers

In July 2013 a research team from the University of Texas managed to take control of the navigational systems of an 80 million dollar 210-foot yacht in the Mediterranean. They accomplished this using equipment, which cost only 3000 USD to build.

Essentially they injected their own radio signals into the vessel's GPS antennas, which enabled them to steer the vessel as they saw fit. Whilst they were doing this, the vessel's GPS systems reported that the vessel was moving steadily in a straight line, with no indications of changes.

The captain of the vessel, who had given permission to perform the test, stated that:" *[they] did a number of attacks and basically we on the bridge were absolutely unaware of any difference*"[7].

GPS jamming

Powerful GPS jammers are readily available on the commercial market – whilst this is not legal everywhere, the fact remains that they are easy to obtain. Backback-mounted units with jamming ranges of up to 3-400 meters can be bought at price ranges of 10-20.000 USD. As vessels today are highly reliant on GPS navigation, disabling GPS can present a significant challenge.

The UK and Irish General Lighthouse Authority performed a test on a vessel, the Pole Star[8]. Powerful GPS jamming equipment was directed a specific patch of ocean and a vessel was sailed into the zone to record developments. As the vessel entered the jamming zone a range of services failed: the vessel's DGPS receivers, the AIS transponder, the dynamic positioning system, the ship's gyro calibration system and the digital selective calling system. The crew was able to cope with multiple alarms as they had been expecting this to happen. However on a modern vessel the bridge might on some cases be single-manned at night, causing significant problems should such a situation occur.

Although the Pole Star's crew was expecting GPS failure, material unexpected problems were seen. The vessel's Electronic Chart Display & Information System (ECDIS) was not updated due to the failure of the GPS input, resulting in a static screen. ECDIS is the normal mode of positioning on board Pole Star (with paper chart backup,) and during the periods

[7] http://cyberarms.wordpress.com/2013/07/26/hacker-team-takes-over-80-million-super-yacht/
[8] http://www.navnin.nl/NIN/Downloads/GLAs%20-%20GPS%20Jamming%20and%20the%20Impact%20on%20Maritime%20Navigation.pdf

of jamming some crew members became frustrated when trying to look at the ECDIS. This resulted in the monitor being switched off.

In addition to the vessels themselves, some automated container terminal systems use GPS to facilitate the automate placement and movement of containers and can similarly be jammed, which would cause significant congestion problems.

The ability to manipulate ECDIS data

In January 2014, the security form NCC Group demonstrated that ECDIS can be penetrated and manipulated[9].

ECDIS – Electronic Chart Display and Information System – is the computer system usually installed on the bridge of the ship and used by navigation officers as an aid to traditional paper chart navigation – often supplanting traditional navigation. Regulations from the International Maritime Organization call for ECDIS to completely replace the use of paper-based navigation.

ECDIS is interconnected with a wide range of other systems and sensors such as radar, Navigational Telex (NAVTEX), AIS, Sailing Directions, Position Fixing, Speed Log, Echo Sounder, anemometer, and fathometer. These sensor feeds are often connected to the shipboard network, which in turn has a gateway to the Internet. Navigational charts are either downloaded on to ECDIS directly via the Internet or loaded from CD/DVD or USB memory disk manually by the personnel.

NCC Group tested an ECDIS product from a major manufacturer of such systems with an aim to see whether penetration of the system was possible. Several security weaknesses were found including the ability to read, download, replace or delete any file stored on the machine hosting ECDIS.

Access to perform such an attack could be achieved by various means, such as the introduction of a virus via portable USB disk by a crew member or any other visitor to the vessel, or using an unpatched vulnerability via the Internet – either directly or via one of the multiple systems linked into ECDIS. Once such unauthorized access is obtained, attackers could be able to interact with the shipboard network and everything to which it is connected.

Penetrating maritime satellite communications

[9] https://www.nccgroup.com/media/481230/2014-03-03_-_ncc_group_-_whitepaper_-_cyber_battle_ship_v1-0.pdf

During October to December 2013, security company IOActive performed a study directed at security related to satellite communications using Inmarsat and Iridium SATCOM terminals. Most systems were found to have critical security issues, and these included marine VSAT and FB terminals[10].

One of the conclusions were that all devices under the scope of analysis could be abused. The vulnerabilities could allow remote attackers to compromise the products. In some cases simply sending an SMS from one ship to another ship could be successful in exploiting vulnerabilities.

Compromising a terminal deployed on a vessel as part of the satellite communication system would give an attacker full control over all information passing through the satellite link. This would, as an example, allow the upload of manipulated navigational charts to spoof ECDIS as navigational charts can indeed be updated via satellite. Weather information, file upload and download from the vessel and any other informational transfer could be equally compromised.

The study also showed that GMDSS (Global Maritime Distress and Safety System) could be compromised for certain setups, allowing attackers to control devices onboard the vessel, deliver false information and disrupt communication.

The SSAS (Ship Security Alert System) was shown to have vulnerabilities allowing an attacker to disable the system remotely, thereby preventing the vessel from sending alerts in case of e.g. attempted pirate attacks, as well as remotely disable safety systems prior to attacking a ship.

Penetrating Maritime Authorities

It is not only commercial companies in the maritime sector which are at risk. In September 2014 it was made public that the Danish Maritime Authorities discovered that they had been subjected to a successful cyber attack in 2012[11]. An attack which was likely initiated through a pdf document infected with a virus, whereupon the attack was spread from the Danish Maritime Authorities to other Danish government institutions.

Learning from other industries

Outside the maritime sector, a number of other industries are seeing cyber attacks which, in nature, are equally applicable to the maritime industry.

[10] http://www.ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf
[11] http://shippingwatch.dk/Rederier/article7043149.ece

Amongst these are examples of penetration of, and vulnerabilities in, industrial control systems. These are typically SCADA systems which are also found in maritime control systems on vessels as well as in ports. Generally it is found that many control systems are originally designed from the viewpoint that they are never online, and cyber security was unnecessary simply because you could not access such systems. Such a viewpoint is no longer applicable. Many systems are now online, and even onboard vessels we see equipment manufacturers needing satellite links in order to remotely monitor, service and upgrade software components on the vessels. And even in cases where systems are indeed offline, they can still be subjected to malicious software as the well-known example of Stuxnet showed when it penetrated Iranian centrifuge systems, which formed part of their nuclear program. Stuxnet, however, was not specific to only this application and is able to attack modern SCADA systems as well as Programmable Logic Controllers such as those also find in cars and power plants.

What is the motivation to attack the maritime industry?

During our conversations with senior people in the industry, the same question appears in most cases: What would be the motivation to attack the maritime industry specifically?

The shipping industry is an industry wherein people have gotten used to being part of an almost "invisible" industry. It does not get the level of awareness in society as is often levied on consumer-facing industries. Unless you happen to live near a major port facility, the average person is unlikely to physically see the actual scale of the industry. From this perspective it would seem reasonable to assume that the industry would also be relatively "invisible" in relation to cyber threats as other sectors would appear much more appealing – sectors such as the military or financial institutions. And clearly, such sectors do see a much higher level of aggressive cyber activity, but this does not mean that the maritime industry does not hold interest – as also evidenced by the examples listed in the previous section.

The maritime sector possess a number of attributes, which makes it attractive to cyber attackers. Most notable amongst these attributes are:

- A significant need for exchanging information across multiple stakeholders. As an example, shipment of a container will likely involve data transfer between 5-10 different stakeholders such as shipping line, origin port, destination port, shipper, consignee, customs authorities, trucking company, data portal intermediary and banks. These stakeholders will have different backend systems and different levels of

cyber security. The information will be quite detailed and hold value to a number of stakeholders should they be able to access it.
- Large monetary transfers take place involving a large number of stakeholders. Typically, these could be payments by shipping lines to bunker companies, shipyards or vessel owning companies as well as freight payments from shippers to shipping lines and vessel owners.
- Many stakeholders, who are involved in the financial and operational chain, are scattered across multiple different countries and time zones. This means that parties often act asynchronous without necessarily having real time conversations. Any duplicity will thus take some time to discover.

In the following, we take a closer look at the motivational factors, which are divided into four main categories: Stealing money, moving cargo, stealing data and causing disruption.

Stealing money

This is a relatively straightforward motivation, and can be accomplished in several different ways.

One way is to trick a company into transferring money directly to the criminals. The case uncovered in September 2014 using the man-in-the-middle attack directed at flows of money between shipping lines and bunker suppliers is just a simple example of such a financial motivation. This approach can be aimed at theft from virtually any money-transfer, but given the amount of resources needed in order to complete the attack, including the level of knowledge needed to pull it off convincingly, this approach is most likely to be aimed at high-value monetary transfers.

Another way is by using ransomware. Essentially this is a cyber attack whereby the victim's computer or database is encrypted by the attackers. The victim then has to pay a ransom in order to get the key to decrypt the data. In 2013 and early 2014 a popular tool used for this purpose was Cryptolocker. In April 2014, the Russian behind the attack was identified, and associated botnets used to facilitate the attacks were shut down. It is estimated that he, and his group, had managed to generate 100 million USD since 2011 from such cybercrime. Shutting down this group did not stop ransomware attacks, and a report from Dell SecureWorks in August 2014 labelled CryptoWall as the largest and most destructive threat presently, with more than 600.000 computers infected, 5 billion files held ransom and 1 million USD earned in the 5 months from mid-March to mid-August 2014.

Seen from a maritime angle, such ransomware is no different from the situation where pirates physically hijack a vessel and holds both it and the crew for ransom. For a shipping line, such an attack could include the encryption of customer databases or operational

databases, and for a container terminal, it could for example include the scrambling of the database keeping tabs of the container locations within the terminal.

Using the comparison with physical piracy and ransom, it is clear that the maritime industry tend to pay ransom, and hence it is a viable business model for criminal groups. According to a report published by the United Nations Office on Drugs and Crime, the World Bank and Interpol, pirates off Somalia managed to claim some 3-400 million USD in ransom from 2005 to 2012. Out of 179 hijacked vessels in the period, ransom was paid for 152 vessels, hence an 85% success rate in terms of extracting ransom from a successful hijack. Whilst the 85% success rate cannot be generalized to other forms of hijacking, such as ransomware, it does indicate a willingness to pay which is of interest to criminal elements.

Given the technological possibilities, additional avenues for extorting ransom from cyber attacks are entirely feasible. These could, as an example be the use of GPS jammers to disturb or disrupt operations of a vessel or port to a point where it is less costly for the victim to pay a ransom than to be subjected to the jamming attack. Such scenarios could for example involve jamming the navigational equipment of a cruise vessel in confined waters, or disabling critical GPS-reliant equipment on vessels or in ports.

A third approach involving a financial motivation would be the manipulation of market data. This could as an example be achieved in the tramper markets through the spoofing of AIS data making it appear as if either more, or less, capacity is available in a certain geographical area. For market players relying on such electronic information it might indeed interfere with market forces. Providers of such AIS market data state that they do indeed have routines in place to filter such spoofing out. However, we have also received information from other stakeholders that requests have be seen simply to the effect that an entity wanted physical confirmation that certain vessels were indeed in a given area, as the AIS data were not trusted.

Moving cargo

A slightly different motivation pertains to the illegal movement of goods. Whilst at heart the motivation for this is often also financial, we have labelled this as a separate motivational factor.

Two tangible examples of the movement of goods is the drug smuggling incident in Antwerp, and the breach of Australian customs systems listed in the previous section. These were cases wherein the penetration of systems allowed cargo to be moved without authorization. CyberKeel has mapped the flow of usual information exchanges from the point of booking a container until delivery at the endpoint. This mapping showed more than 50 possible attack points against which a cyber attack could be aimed. Penetration at these points would either allow, or facilitate, unauthorized movement of goods. Often the penetration of just one or two of such points would be sufficient to facilitate such

movement. The attack points reside at multiple different companies and organizations which themselves are often located in multiple different countries. These include shipping lines, logistics companies, manufacturers, ports, terminals, customs authorities and IT data portal providers.

Furthermore, attack points within a single company are often spread across departments located in different countries not using an identical IT infrastructure. This means that "ghost shipping" – i.e. the possibility of sending a shipping container from point A to point B without anyone knowing it is relatively straightforward to accomplish.

Stealing information

The data involved in shipping contains a great amount detail, which in itself has value to a number of different stakeholders. Hence, whilst the motivation is theft of information, the subsequent usage of the information varies.

One element is the theft of shipping data for tactical usage in more traditional criminal activities. One example would be stealing data showing which shipping containers are laden with high value goods, as well as which truck is supposed to pick the container up and when this is supposed to happen. If the truck, or container, is equipped with any sort of GPS tracker, penetration into this data stream will further enhance the likelihood of a success physical attack to secure the high value cargo.

Another example is theft of data in order to facilitate a pirate attack aimed at hijacking the vessel. The example using Facebook in the previous section was strictly speaking not a cyber attack as such, as no systems were penetrated, but gaining access to the vessel's data through for example ECDIS would help enable a pirate attack.

A different approach to the theft of data is rooted in industrial espionage. Successful penetration of shipping systems would allow visibility into supply chain details as well as details pertaining to the commodities being shipped in relation to a competing company. As developments in "big data" enables companies to optimize their business even further, feeding such detailed competitor information into a "big data engine" could provide significant value.

A fourth approach is the theft of financial data for investment purposes, or for the purpose of manipulating the value of investments.

In addition to industrial espionage, theft of shipping data could also be performed by nation-states as part of regular espionage efforts.

Causing disruption or loss

Whereas the other motivational factors are aimed at obtaining something, the final motivational factor is predominantly destructive. The motivation is to destroy value or deny access to certain resources.

Whilst in itself disruptive, or even destructive, the usage of ransomware is not motivated by causing disruption. In that case, disruption is merely a means to obtain financial resources.

The main public examples we have in the maritime sector of destructive attacks are the incidents related to the disabling of offshore drilling platforms, as well as the eradication of operational data in Iranian carrier IRISL. In these cases no financial advantage was gained, only the, temporary, denial of usage of a given resource. However, as the examples have shown, the potential for far greater damage is clearly present should groups or individuals be sufficiently motivated.

One motivational factor is financial terrorism. At one end of the scale this could be directed at a single company with an aim of inflicting financial losses. The reason for targeting one specific company would then have to be rooted in either the opportunity to benefit financially from the losses of said company, or be rooted in a strong specific animosity against a particular company. Whilst these types of motivations appear mainly unrealistic, they cannot be ruled out. As a theoretical example, consider a shipping line causing significant environmental damage through gross negligence and which subsequently by some groups are not seen to be held accountable to the degree they feel is necessary. In extremis, such groups could decide to target an individual company.

More worryingly is the other end of the scale where it is financial terrorism at a nation or cross-nation level. If port systems can be breached, this can cause a shutdown of port operations. Such a cyber attack could be accomplished in different ways. Automated terminals could for example be hit through SCADA systems forcing a shutdown. For a container terminal, the deletion all information as to which containers are located where within the yard would be sufficient to halt all operations until the thousands of containers – in some cases tens of thousands – are identified either manually or at such a point in time where access to the data are restored. According to statements from IRISL, this might have been the motivation behind the attack on their shipment data, as they have stated that subsequent to the attack, they received a phone call from a person stating that the reason attack was to target the movement of goods destined for the Iranian nuclear program[12].

Tampering with loading and stowage data could lead to the destabilization of a vessel. In many places, it is common practice to exchange stowage plans using unencrypted email attachments, which makes the exchange highly vulnerable to tampering. Provided the people involved are observant, such destabilization attempts would be discovered before

[12] http://www.globes.co.il/news/article.aspx?did=1000714597

a catastrophic event was to happen to the vessel. However, if it is not detected until late in the process, it will cause a significant disruption in port operations as cargo have to be unloaded and the vessel re-loaded once the proper stowage data are retrieved. The effect would be the de facto denial of usage of both port and vessel for a considerable amount of time.

In 2002, the container ports along the US West Coast were shut down due to a labor dispute for 10 days. The shutdown was estimated to cost the US economy 10 billion USD. A systematic cyber attack against port infrastructure could thus cause financial losses of an equal magnitude. Attacks directed at a single port or terminal would in many cases only cause local losses as other ports would be able to take over the cargo flow, but a simultaneous campaign against multiple facilities could effectively bring the import/export supply chain to a standstill.

Finally, as shown with GPS spoofing and jamming, the ability to steer a vessel off its planned course has a wide range of negative applications should any group decide to pursue such an action. Such an attack might not necessarily be directed at the shipping company owning or operating the vessel, but might instead be aimed at whichever structure or coast that the vessel is steered into. Hence the shipping line might in this case be targeted simply as a means to an end, and not as the primary object of attack itself.

Clearly a destructive motivation in itself would be the implementation of terrorist attacks on three different angles of attack. One would be physical – using control over systems to cause physical damage. The other is financial – destroying data to cause significant losses, and if done properly the damage could clearly extend beyond affecting just the maritime sector. The third is more psychological in nature, using destructive cyber attacks to prevent, e.g. the movement of food or aid goods to areas in need of such support.

Who are behind the attacks?

When examining the groups behind cyber attacks, they mainly fall in four categories: Regular criminals without cyber attack skills, Cyber criminals with the skills to perform advanced attack, hacktivists and nation states.

Regular criminals with no cyber attack skills are in themselves not a threat. However, they have access to a thriving black market wherein the required cyber attack skills can be procured as service. As a few examples of the cost of these services, a research paper by Trend Micro in 2012[13] indicated the following price levels from the Russian market for hacker services: 100-550 USD to have a malicious application installed on 1000 unsuspecting computers, webserver hacking from 250 USD, Trojan for bank account

[13] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

stealing 1300 USD, Trojan for web page data replacement in a client's browser 850 USD, 1 day DDOS (rendering your website inaccessible) attack 30-70 USD.

Essentially, all types of cyber attacks - no matter their size and complexity - can be bought as a service by criminal groups not possessing the skills themselves. These types of criminals are the ones who are already active in the maritime sector – typically involved in various types of cargo theft or, at the extreme, vessel hijacking. Their attack mode is therefore mainly in the form of information theft to maximize their chance of success in relation to existing criminal activities, possibly combined with the elimination of electronically based security measures.

Cyber criminals in possession of relevant skills can choose to work either for the criminal groups listed above or work for themselves. A report from CrowdStrike[14] in 2013 indicated that global cybercrime was dominated by 50 active groups – which in itself indicate that these groups are large and have extensive resources at their disposal. These are groups with the skills and resources to manage the types of attacks labelled Advanced Persistent Threats, and thus being able to execute attacks like the man-in-the-middle attacks seen in many industries, and now also in the maritime industry. These groups are financially motivated, and will thus only attack companies in the maritime sector if they stand to make money from the attack. Their attack mode will therefore mainly be in the form of either stealing money or using ransomware.

The third group consists of hacktivists. This is by no means a homogenous group, but merely a phrase used for any and all groupings who use hacking and cyber attacks as a means to express their own politically motivated agendas. Seen from a maritime perspective, these groups would predominantly be motivated by creating disruption or losses. Several aspects could cause maritime companies to be targeted by hacktivist groups. One approach would be a campaign against a company which is perceived by some groups as "deserving" a punishment the society is not giving it. The hypothetical example mentioned previously could be an accident with environmental consequences wherein a political group do not believe the company has been sufficiently sanctioned. It might also be the targeting of the entire industry for various political reasons. Such political motivations do not need to enjoy widespread acceptance, nor be founded in a rational reality, it merely requires that a small group of hacktivists find the cause worthwhile.

Maritime companies may also be targeted by hacktivists merely as collateral damage. A campaign might be directed at a specific country or region, and as a consequence all large known companies from the country in question could be targeted. However, irrespective of the political target of the hacktivists, the attacks are likely to be disruptive and destructive.

[14] http://news.techworld.com/security/3498393/global-cybercrime-dominated-by-50-core-groups-crowdstrike-report-finds/

The fourth and final category are nation states. The resources available at a nation state level also allows these groups to mount the most invasive and persistent attacks. The straightforward motivation for these groups would be the theft of information, however as it pertains to the maritime sector this might not be the full motivation. Given the importance of seafreight to any country's economy, obtaining the ability to be able to manipulate with this should not be ruled out as such an ability could be seen as yet another clandestine military or political tool.

What is the impact of an attack?

The conversations we have had with maritime industry leaders over the past 6 months indicate that a majority mainly think of a cyber attack as something with a predominantly technical impact, requiring technical solutions as well as technical action. And while it is correct that in the midst of a cyber attack you do need technically proficient people on hand to combat and eradicate the attack, the main impact has nothing to do with IT, but everything to do with standard business processes.

Of course the magnitude and complexity of the impact depends on the nature of the attack itself, but fundamentally speaking the approach has to be similar to the contingency planning maritime companies already have in place regarding physical disaster scenarios.

The first key question is: Who makes decisions? If your systems are penetrated, several considerations have to be made which are decidedly non-technical in nature. From the perspective of combating the cyber attack it might be desirable to keep all systems online for a while. Early interference could alert the attackers who will pull back, but if they have multiple entry points they will likely leave new backdoors or avenues of attack for themselves to be utilized at a later point in time. Hence in some cases it might be wise to wait until all their entry points are identified and take them all out before they have a chance to regroup. However, this has to be balanced against a number of commercial considerations. Not shutting down immediately could increase the risk of financial loss – and does the company have a contingency plan in place, whereby they can effectively tell the organization to use an alternate payment process for an interim period? And what impact would this potentially have on customers? What if the nature of the attack is such that the object of interest is the impact on shippers and not the shipping lines?

In this case the question comes back to the matter of decision making authority, as the IT manager might be in favor of staying online for a while, whereas the financial manager would be in favor of a quick shutdown. The commercial manager might have a third position related to the handling of customer facing communication in relation to the attack. If no set contingency plan is in place, valuable time could be lost trying to reach a

consensus decision on the matter – or, even worse, the business managers are not even informed, as the IT department attempts to fix the matter unilaterally.

It is clear that the potential ramifications of an attack has cross-functional relevance of both short term and long term nature. It is therefore important that high-level decision makers are familiar with these issues prior to any contingency appearing. This enables a decision making process whereby the strategic implications can be incorporated, and not merely the short time virtual firefighting.

Ranging beyond the company itself is the matter of knowing which external authorities to involve – ranging from local port or customs authorities to law enforcement agencies locally and abroad.

Is the attack over?

A key challenge is assessing whether an attack has been successfully repelled and eradicated. A shipping line operating agencies in dozens – in some cases hundreds – of physical locations will need to carefully analyze the modus operandi of the attack to ascertain whether it could have been spread to local agencies. If this is deemed to be the case, a contingency plan for dealing with such a situation should be in place.

Even in cases of just a single physical location, it is crucial to be able to analyze whether the attack has been designed to leave behind additional entry points for future use. Depending on the forensics of the attack mode, such analysis might need to include assessments of whether entrypoints are left behind in devices such as printers, external harddisks or other hardware.

Improving maritime cyber defences

As outlined, there is no shortage of neither motivation nor opportunity. Realistically, 100% security can never be achieved, and in this respect cyber risks are no different than the other more traditional risks faced by the maritime industry. The important part is to design, implement and maintain a risk-reducing strategy – and this should be done both from an individual company perspective as well as from an industry wide perspective.

It is important to note that the fundamental principles of cyber defence is no different than for any other industry facing similar risks, and should as such not be seen as uniquely difficult to do. Below outline is therefore only to be taken as a high level overview of considerations needed. It is therefore critical that each company makes a thorough analysis of the realistic risks they face, and make informed decisions as to which level of security they wish to implement versus the business impact and cost of such measures.

CyberKeel – www.cyberkeel.com

Look for attacks from the inside

Do not rely on keeping attackers out. If dedicated, they will come in no matter what. Firewalls and virus alerts only deflect the most simplistic attacks. The company needs to consider how, and to which degree, they want to install procedures to actively look for unauthorized usage within the system.

In principle this is no different than physical security. The firewall and virus program is the same as erecting a fence and having a security guard at the entrance. However, a dedicated efforts will always be able to penetrate such a defensive perimeter. Based on individual risk assessments, some companies therefore also install internal camera surveillance, heat and motion detectors or even hire security guards to walk around inside the premises. Every company makes a cost-to-risk analysis and then decide how many of these internal security features should be implemented in their company.

For the cyber risks the situation is exactly the same. In this case the surveillance cameras and motion detectors are replaced by automated monitoring systems and algorithms analyzing data patterns, and the patrolling security guard should instead be compared to a skilled computer programmer actively monitoring the systems for breaches.

Testing applications as well as hardware

Many maritime companies have software made for special purposes by a large array of vendors ranging from very small to large multinational companies.

When designing the specifications for such systems, the company should additionally specify cyber security tests which the system should be able to pass. In a company utilizing hundreds, if not thousands, of different types of software, it only requires one piece of vulnerable software to be open to an attack.

Given the case of the Zombie Zero attack lodged from within physical barcode scanners, companies need to assess to which degree hardware with access to critical systems need to be tested, as well as whether they should include considerations into the procurement phase related to trusted versus non-trusted vendors of hardware linked to critical computer systems.

The point about specifying tests also apply to industrial control systems, irrespective of whether they are add-on systems or come as an integral part of for example a vessel engine, a pump system or an automated gantry crane control system.

The human factor

A large part of successful attacks include a human element – usually termed "social engineering". This part takes on an almost endless variety, but includes elements such as getting employees to open email attachments containing viruses, getting people to click on links they should not click on, providing information over the phone which they should

not have divulged, trusting email content which is manipulated or tricking employees into plugging unauthorized hardware into the system.

These elements mainly cannot be addressed through technical solutions. Instead they have to be addressed through a combination of business processes and awareness training of the employees.

Awareness training pertaining to the most typical social engineering attacks can help improve defenses, but cannot eliminate it.

Business processes should be designed to reduce risks as well, but will always need to be balanced against business needs as well as the likelihood that the process is de facto implementable. An example of this dilemma can be found in the usage of USB memory sticks. USB memory sticks are a significant source of virus infections, and is therefore inherently unsafe in relation to cyber security. On the other hand they are extremely useful and versatile in a business environment. Hence a risk versus reward assessment need to be made in each individual company. If, then, the company decides to ban the usage of USB stick, the next question is whether they can actually enforce this ban. Realistically, such a ban can only be enforced if the decision is also made to physically remove the possibility to inject USB devices into the company network, such as in computers, laptops and printers – and again this is a business decision weighting risk versus reward.

Similar considerations of risk versus reward should be made pertaining to the usage of own devices such as smartphones and tablets within the company network, the ability to install software on local computers and apps on company tablets and smartphones. Essentially, all human interactions with the networks should be analyzes from a business process perspective, and decisions then made as to whether the process should be changed to reduce the risk, or whether the risk should be accepted and other steps then be taken to address the risk from a different perspective.

Become a cyber-resilient organization

Through the establishment of alternate contingency plans as well as well-planned backup systems, reduce the impact of successful cyber attacks. This approach is a supplement to a solid cyber defense, but aims at ensuring continuity even in the case of successful attacks.

Cyber resilience would include clear plans for alternate communication channels, alternate informational databases fully independent from daily systems as well as alternate tools and systems onboard vessels to ensure operations if normal systems are breached or jammed.

An industry-wide cyber security organization

Other industries have seen the establishment of forums of companies within the same industry where the aim is to share tactical cyber defense information as well as develop standards and processes to jointly improve industry cyber defenses.

CyberKeel is taking the initiative to launch such a forum shortly within the maritime sector. The key purposes of the forum will be to:

- Establish a trusted environment wherein companies can share specific technical details of ongoing cyber attacks to allow similar companies to easily scan, detect and deflect identical attacks
- Establish an forum for the development of practical cyber security standards which can be implemented to the benefit of all industry players
- Establish a forum to serve as the locus for joint-industry efforts to prioritize, and execute, testing into specific systems issues of relevance to the industry