Navigating Cyberthreat: Exploring the implications of cyberthreat to the maritime sector.

Whitepaper 2021

The impact of cyberthreat

Technology is an ever-increasing presence in our lives and we're relying on it more and more. The technological advances that we're seeing provide us with great benefits, of course, but can also present us with problems, especially when progress is swift.

The maritime sector has seen rapid technological progress in recent years, in both informational and operational technologies, and whilst this has been excellent for increasing efficiencies across the sector, an unfortunate consequence is that the maritime industry is now more vulnerable to cyberattack.

Cyber, or cybersecurity, threats have been defined as *'malicious acts that seek to damage data, steal data, or disrupt digital life in general*[1]' and include threats like computer viruses, data breaches and Denial of Service (DoS) attacks.

According to Visma, a leading provider of business software, cybersecurity threats are becoming increasingly common[2], appear in a variety of forms and can be *'devastating to an individual, business, and to society as a whole*[3]'.

Joe Da Silva, Chief Information Security Officer at Electrocomponents PLC, explains that *'typically, most people would consider a cyberthreat to be a internet based attack on a computer system*[4]'. However, he goes on to clarify that actually *'cyberthreats can be much, much broader than that, and often don't involve any direct attack over public networks*[5]'. Sometimes a cyberattack could come *'from an individual person walking into a facility, whether that's a ship, a container ship, or a small yacht, and interfering with systems or obtaining data*[6]'. It's clear from this that although cyberattacks often originate from the internet, they can *'just as easily be perpetrated by an individual*[7]'.

Common examples of cybersecurity threats include malware, data breaches, phishing attacks and computer viruses, and the maritime sector has been victim to all of these at one time. Often cyberattacks are coordinated, which makes the threat even more serious.

The maritime logistics information and technology company Marine Digital explains that, within the maritime sector, cybersecurity has the huge potential to *'affect the safety of the crew, vessel, cargo and even ports*[8]'. Fortunately, however, as threats have increased globally more and more resources are being deployed to combat the increasing cyberthreat, with encouraging results.

1 Taylor, Hugh 'What are cyber threats and what to do about them' Prey Project
2 Visma 'Cyber security threats and vulnerabilities'
3 *ibid.*
4 Joe Da Silva interview
5 *ibid.*
6 *ibid.*
7 *ibid.*
8 Marine Digital 'The importance of cybersecurity in the maritime industry'

The challenges faced

A cyberattack is an attack that's mounted against our digital devices by means of cyberspace. Although cyberspace does not physically exist, it's commonly used as a metaphor to help us understand the digital weaponry that intends to harm us[9].

Although many cyberattacks are nothing more than annoyances, others can be very serious indeed, and some even threaten human lives. In shipping, the term 'cybersecurity' covers a range of potential threats, including the data protection of IT systems, onboard ships' hardware and sensors, and data leaks from unauthorised access, manipulation and disruption[10].

The growing problem of cybersecurity has gained a high profile in recent years because cyberattacks are becoming more widespread and much more sophisticated. A very early example of a highly coordinated and sophisticated maritime attack occurred in 2013 when the Belgian port of Antwerp was hit by an extremely well-planned, phased cyberattack which resulted in a serious security breach over a two-year period[11].

A group of drug traffickers began the cyberattack by emailing malicious software to port staff in June 2011. The criminals were then able to access data remotely, which enabled them to identify and intercept containers with smuggled drugs on board.

The security breach was only discovered when entire containers went missing from the port without explanation. Once the security breach was neutralised the attackers then went on to physically break into port offices and concealed computers within everyday objects in order to intercept data from port systems, including workstation screenshots and staff keyboard inputs. This allowed the criminals to gain wireless access to staff computers, meaning they could monitor shipments remotely.

The attack at Antwerp was a highly coordinated, complex and sustained attack that highlighted the dangers of cyberthreats to the maritime sector and was a huge wake-up call for the industry.

What's the real cyberthreat to maritime?

The maritime sector is attractive to cyberattackers and is at high risk because the sector comprises multiple stakeholders who are geographically distant from each other and use a broad range of networks with which to communicate. This means that the sector is very susceptible to cyberthreat[12] because every time a container is shipped, data will be transferred between (as a minimum) the following:

- the shipping company
- loading port
- destination port
- shipper
- consignee
- customs authorities
- dispatch company
- data portal intermediary
- banks

[9] Taylor, Hugh 'What are cyber threats and what to do about them' Prey Project
[10] Marine Digital 'The importance of cybersecurity in the maritime industry'
[11] Seatrade Maritime News 'Antwerp incident highlights maritime IT security risk'
[12] *ibid.*

There 'could easily be attacks being conducted now that we will find out about in six months or a year, or maybe two years' time'

This means there are multiple opportunities for cyberattackers to infiltrate data and exploit communication channels for their own gain. The fact that large monetary transfers, involving many stakeholders, also frequently take place is another reason why the maritime sector is so vulnerable.

Another problem is that because the stakeholders involved in the operational and financial chain are located across multiple countries and time zones, the various parties involved in shipping the container don't always have real-time conversations, which means that any cybersecurity issues can take time to discover[13].

As Joe Da Silva explains, '*the issue with a lot of cybercrime, is that it's often not detected until it's far too late.*[14]' This means there *'could easily be attacks being conducted now that we will find out about in six months or a year, or maybe two years' time'*.

What does cybersecurity mean for you?

Ships are becoming increasingly reliant upon systems that utilise digitalization, integration and automation and as these technologies develop shipping companies are understandably anxious about the impact that cyberthreats will have on their operations.

With advances in digital and communication technology, information technologies (IT) and operational technologies (OT) have become integrated meaning that there is greater potential for risk to critical systems and processes as vulnerabilities arise from '*inadequate operation, integration, maintenance, and design of cyber-related systems, as well as from intentional and unintentional cyberthreats.*[15]'

Marine operational technologies include systems such as:

- Satellite Communications
- Vessel Integrated Navigation System (VINS)
- Automatic Identification System (AIS)
- Global Positioning System (GPS)
- Radar systems and electronic charts

Anastastios Arampatzis[16], an expert in cybersecurity, warns that any disruption to these OT systems may '*impose significant risk to safety of onboard personnel and cargo, cause damage to the marine environment, and impede the ship's operation.*[17]' It's clear from this that the maritime cyberthreat is both very real, and highly alarming.

Joe Da Silva reports that a lot of older industrial systems are used within maritime businesses, such as cranes and conveyors for example, that are computer controlled. These computers are typically very old, not very easy to replace and have lifespans that are measured in decades. Very often these systems do not get updated but are connected to other systems as businesses develop. As older systems are integrated with newer ones, vulnerabilities occur as the '*cyberattack surface is expanded*[18]'.

[13] Seatrade Maritime News 'Antwerp incident highlights maritime IT security risk'
[14] Interview with Joe Da Silva
[15] Arampatzis, Anastasios 'The biggest challenges and best practices to mitigate risks in maritime cybersecurity'
[16] Arampatzis, Anastasios 'writer bio'
[17] *ibid.*
[18] Interview with Joe Da Silva

What happens when security is breached?

All four of the biggest maritime shipping companies in the world have now been the victim of cyberattacks. Since 2017, APM-Maersk, Mediterranean Shipping Company, COSCO and CMA CGM have all been hit by serious ransomware/malware attacks and this is especially concerning because no other industry has had all of its biggest players hit by major cyberattacks one after the other[19]. Although all the attacks were different, they show a 'preferential targeting of the maritime shipping industry[20]'.

Ken Munro, a security researcher at Pen Test Partners, a UK cybersecurity company, doesn't believe that the maritime sector is any more or less vulnerable than other industries, but states that the issue is that it's '*brutally exposed to the impact of ransomware*[21]' because after Maersk was hit by the NotPetya crypter in 2017, criminals realised the potential to bring down a critical industry. This meant that payment of a ransom is perhaps now more likely with maritime than with other industries. As Joe Da Silva explains, '*the bottom line is that organized crime is making money out of ransomware so there's going to be more of it*[22]'.

What's the scale of cyberthreat to the maritime sector?

In 2013, for the first time since the terrorist attacks of September 11, 2001, cyberthreat was named by the Director of National Intelligence as the '*number one strategic threat to the United States*[23]', and in July 2019, the US Coast Guard issued a safety alert warning all shipping companies of the potential of serious maritime cyberattacks[24].

Nick Davies, CEO of maritime security company Gulf of Aden Group Transits (GoAGT), believes that '*supply chain security in the future will be critical especially in the USA and mainland Europe*[25]' adding that '*the sheer volume of mega ships that can carry 14,000+ teu presents the biggest security challenge for any port authority and customs network*[26]'.

In a leading transport survey by international law firm Norton Rose, 87% of respondents from the shipping industry believed '*cyberattacks would increase over the next five years*[27]'. Joe Da Silva finds it really hard to anticipate the scale of the problem, '*other than to say that it's growing*[28]'.

[19] Cimpanu, Catalin 'All four of the world's largest shipping companies have now been hit by cyber-attacks'
[20] *ibid.*
[21] *ibid.*
[22] Interview with Joe Da Silva
[23] Maritime Cyber Security. University Research Phase I - Final Report
[24] Arampatzis, Anastasios 'The biggest challenges and best practices to mitigate risks in maritime cybersecurity'
[25] Security World Market 'Maritime criminals become more sophisticated'
[26] *ibid.*
[27] Saul, Jonathan 'Global shipping feels fallout from Maersk cyber attack'
[28] Interview with Joe Da Silva

Navigating cyberthreat

In a 2019 paper[29], Ivan Mraković and Ranko Vojinović suggest that a holistic approach is required for cybersecurity management because '*there is an increase in complexity, digitalization, and automation of systems in maritime industry*[30]'.

Because there are '*numerous interconnected systems between ship and shore*[31]', and these are increasing on a daily basis, the maritime sector is becoming more and more vulnerable to cyberattacks.

As marine systems become more advanced and IT and OT systems become more and more integrated, shipping companies across the globe will have to increase their vigilance as the risk of cyberthreat grows. It's important to take a holistic approach because every aspect of a ship's operations needs to be looked at to ensure that they're protected and resilient against the increasing threat. In today's digital age, a comprehensive cybersecurity plan is needed. As Nick Davies explains; '*business leaders are forging ahead with their digital business initiatives, and those leaders are making technology-related risk choices every day*[32]'.

One of the key areas for concern in relation to cybersecurity is the human element and in a 2017 survey conducted by IHS Fairplay[33], 47% of those questioned believed that their organization's biggest cyber vulnerability was the staff[34], which highlighted the need for extensive additional training across the sector.

Phil Tinsley, Manager of Maritime Security at Bimco, has found that '*there is unfortunately still a lack of awareness of the potential severity of a malicious cybersecurity attack on board a ship*[35]'. This is because IT and OT systems are not always fully understood by all ships' crews. Tinsley warns of the potential for an incident to occur through '*negligence, misuse or even deliberate acts*' when working with onboard systems that are interconnected and mutually reliant.

Joe Da Silva urges the prioritisation of staff training and not just by rolling out 'click through' annual training. For Da Silva, training has to be about '*making sure that all individuals have the proper awareness of what could be possible*[36]'. The key is to '*get people's hearts and minds and help them to understand that this is a business risk that goes down to all levels of the organization*[37]'.

Fortunately, the United States Coast Guard has been proactive in the fight against cyberthreat and has paired with the Transportation Security Administration in an attempt to reduce cybersecurity threats in the shipping industry. The two organisations are also collaborating to ensure that mariners are trained in cybersecurity and have the knowledge to combat cyberthreat[38].

[29] Mraković, I. and Vojinović, R. (2019) "Maritime Cyber Security Analysis – How to Reduce Threats?"
[30] *ibid.*
[31] *ibid.*
[32] Visma 'Cyber security threats and vulnerabilities'
[33] Rider, David 'Cyber security at sea: The real threats'
[34] *ibid.*
[35] Valour Consultancy 'Maersk cyber-attack: A lesson learned?'
[36] Interview with Joe Da Silva
[37] *ibid.*
[38] Maritime Institute of Technology and Graduate Studies 'Guide to ship cybersecurity'

Working together

Relationships between shipping companies and their suppliers have become increasingly important during recent years and the global pandemic of 2020/2021 has further highlighted the need for collaboration across the sector.

Freddy Ingemann, Founder and CEO at Moscord, found the biggest positive change since Covid is that people are working together across the maritime sector to find solutions to common problems[39] and it's hoped that this will also be true of the cyberthreat.

Kevin Shakespeare, Director of Stakeholder Engagement at The Institute of Export and International Trade, makes the point that communication with customers and suppliers is going to become more and more important, and understanding that industry problems are shared problems will make it easier for the maritime sector to work together to resolve common issues[40].

According to Adrian Constantin Stanila, Information Security Officer in Visma, cyberthreats are growing more serious and '*pervade every organisation*[41]' which is why it's important for stakeholders to work together to reduce the risk to the sector as a whole.

Looking to the future

As a result of the global coronavirus pandemic there's been huge investment in UK ports[42] as part of the economic recovery plan, and this investment will almost certainly be mirrored across the globe as governments all around the world seek to support the maritime sector. It's expected that any investment will include the upgrading of port cybersecurity to ensure a prosperous future.

We know that in addition to the ongoing integration of IT and OT, the future will also bring Maritime Autonomous Systems (MAS) which are based on artificial intelligence. The adoption of MAS has huge implications for the sector and it's possible that the next generation of ships could be remotely controlled from the shore[43]. This is incredibly exciting but also has the potential to disrupt. As a result, mariners will need to be hyper-aware of possible increased cyberthreats and ensure that all crews are adequately trained.

[39] Interview with Freddie Ingemann
[40] Interview with Kevin Shakespeare
[41] Visma 'Cyber security threats and vulnerabilities'
[42] 'Ports Coronavirus Hub' by British Ports Association.
[43] Arampatzis, Anastasios 'The biggest challenges and best practices to mitigate risks in maritime cybersecurity'

Navigating cybersecurity with RS Components

It's clear that the cyberthreat has already had a significant impact on the maritime sector, but RS Components is confident that our knowledge of global shipping places us in the best possible position to help our customers to confidently navigate the threat. Our purchasing processes are streamlined and, because our customers only have to work with one supplier, the number of communications and transactions are reduced, making for a less vulnerable and more robust process.

As a large, well-established global supplier, we can also provide both the stock and the export services that smaller suppliers might struggle with. Our global supply chain network includes distribution centres across Europe and we're investing £30m in additional stock in order to improve our service. This means that we're in a stronger position than most to assist shipping companies who are impacted by cyberattacks.

How we help

RS Components work to proactively keep information safe, including employee, customer and supplier data, and performance and business information. We have an active and ongoing programme of Information Security improvements including conducting regular tests of our own systems. We publish and regularly review Information Security policies which apply to all of our Group companies and employees, and also assess the information security risks of our third-party suppliers. We also educate and inform our people to ensure they are aware of the risk of not protecting information.

Information Security at RS Components is everybody's responsibility, and everybody is required to comply with Electrocomponents security policies, standards, procedures and practices in their daily activities. In addition, all of our staff must complete Information Security Training modules when requested by the Information Security Team.

Working together to navigate the future

We continue to work closely with our partners and suppliers to provide maritime customers with the relevant brands and products for all their repair and maintenance procedures, whatever the future holds.

Shipserv

Shipserv are an e-commerce trading platform which connects buyers to suppliers. We're proud to have Shipserv as a strategic partner and we're in the process of integrating our catalogue into Shipserv.com so that we can link seamlessly with all purchasers and so reduce the time and cost of purchase ordering.

Moscord

RS Components is working closely with Moscord, the recognised marketplace for the maritime and shipping industry, and is recognised by Moscord as a key supplier. Because RS have both the range of stock and the export experience to provide an expert service, it's anticipated that money spent on operating costs will be reduced due to the streamlining of purchase processes and having one single point of purchase.

Our priority is to do what we can to protect against the disruption of cyberthreats so you continue to receive a high level of service and support when you need it most.

Sources

Arampatzis, Anastasios *'The biggest challenges and best practices to mitigate risks in maritime cybersecurity'* Tripwire Website 2/8/2020

Arampatzis, Anastasios *'writer bio'* Tripwire Website 2/8/2020

Cimpanu, Catalin *'All four of the world's largest shipping companies have now been hit by cyber-attacks'* ZDNet Website 29/09/2020

Marine Digital *'The importance of cybersecurity in the maritime industry'* Website. Accessed 30/11/2021

Maritime Cyber Security. University Research Phase I – Final Report

Maritime Institute of Technology and Graduate Studies *'Guide to ship cybersecurity'* Website 7/10/2021

Mraković, I. and Vojinović, R. (2019) *'Maritime Cyber Security Analysis – How to Reduce Threats?'*, Transactions on Maritime Science.

'Ports Coronavirus Hub' British Ports Association.

Rider, David *'Cyber security at sea: The real threats'* The Maritime Executive. 10/3/2018

Saul, Jonathan *'Global shipping feels fallout from Maersk cyber attack'* Reuters. 29/6/2017

Seatrade Maritime News *'Antwerp incident highlights maritime IT security risk'* Website. Accessed 21/10/2013

Security World Market *'Maritime criminals become more sophisticated'*. Website 2/11/2013

Taylor, Hugh *'What are cyber threats and what to do about them'* Prey Project. June 16 2021

Valour Consultancy *'Maersk cyber-attack: A lesson learned?'* Website 4/8/2017

Visma *'Cyber security threats and vulnerabilities'* Website. Accessed 30/11/2021

Interviews

Joe Da Silva, Chief Information Security Officer at Electrocomponents PLC. Interviewed by RS on 8th July 2021

Freddy Ingemann, Founder and CEO at Moscord. Interviewed by RS on 17th November 2020

Kevin Shakespeare, Director of Stakeholder Engagement at The Institute of Export and International Trade. Interviewed by RS on 2nd October 2020