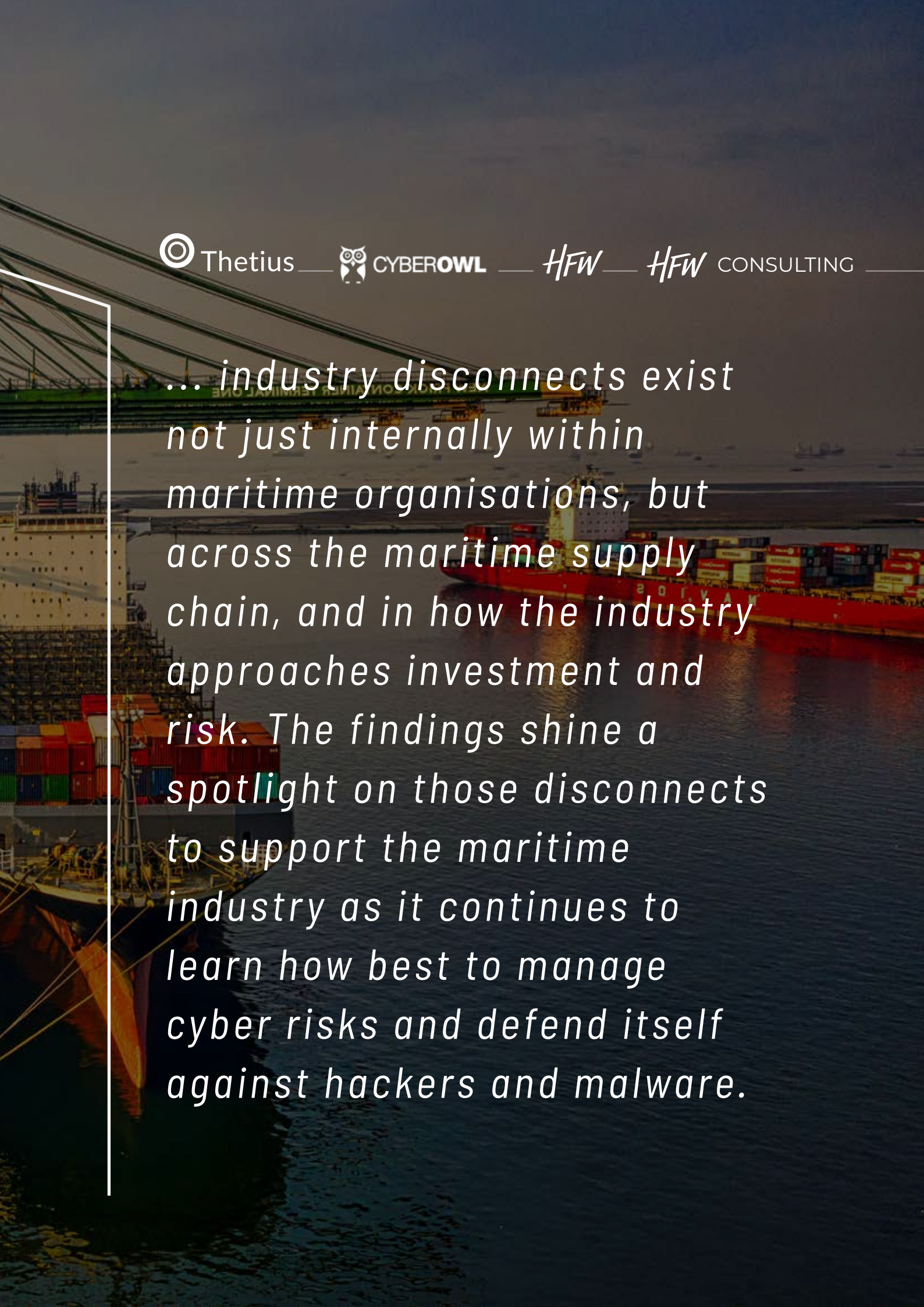
THE GREAT DISCONNECT

The state of cyber risk management in the maritime industry

Nick Chubb, Patrick Finn & Daniel Ng

Foreword by Guy Platten, Secretary General of the International Chamber of Shipping

NPCT 1
801



Thetius CYBEROWL HFW HFW CONSULTING

... industry disconnects exist not just internally within maritime organisations, but across the maritime supply chain, and in how the industry approaches investment and risk. The findings shine a spotlight on those disconnects to support the maritime industry as it continues to learn how best to manage cyber risks and defend itself against hackers and malware.

CONTENTS

EXECUTIVE SUMMARY 6

INTRODUCTION 8

UNDERSTANDING MARITIME CYBER THREATS 10

- Organised crime and opportunists 11
- The impact of nation states 12
- Collateral damage 13
- Spoofing positioning systems 14
- Targeting choke points 15
- Case study 16
- The unintentional insider 17

THE GREAT DISCONNECT: WHAT MAKES THE MARITIME INDUSTRY VULNERABLE? 20

THE ORGANISATIONAL DISCONNECT 21

- Ownership 21
- Awareness 23
- Readiness 24

THE SUPPLY CHAIN DISCONNECT 26

- Responsibility 27
- Control 28
- Regulation 29

THE RISK DISCONNECT 31

- Ransom 32
- Insurance 33
- Investment 34

BEYOND COMPLIANCE: CONCLUSIONS AND RECOMMENDATIONS TO INDUSTRY 35

- Set up a dedicated cyber security directorate within fleet operations that covers both IT and OT security 36
- Implement a comprehensive cyber incident training and drill programme 37
- Develop minimum security standards for suppliers and partners 38
- Conduct an urgent review of insurance policies and seek specific legal guidance on ransom payments 39

Acknowledgements 41

Additional Notes 41

References 42

FOREWORD

Shipping has changed more in the last two years than it did in the entire decade before that. Digitalisation has given the industry new ways of working that has kept world trade moving through a global pandemic as well as enabling a multitude of new efficiencies. But the shipping industry's increasing reliance on digital tools is not without risks.

Today, it makes no difference if you work at sea or work ashore, there is no escaping the need to properly manage cyber security risks and protect against those that may attempt to harm the industry.

this report is an important contribution to the industry's growing body of knowledge on cyber security and I would encourage you as a reader to take stock of its findings and recommendations.

As Secretary General of the International Chamber of Shipping, I have seen firsthand the impact that cyber security incidents can have, not just on maritime organisations, but on the individual people that rely on them. Today, it makes no difference if you work at sea or work ashore, there is no escaping the need to properly manage cyber security risks and protect against those that may attempt to harm the industry.

The maritime industry has made great progress in recent years to improve how cyber risks are handled, with the introduction of the IMO's Maritime Cyber Risk Management resolution acting as an important first step. But as this report demonstrates, there are a number of areas where the industry needs more support.

The first of those areas is ensuring that maritime organisations have the right structures, tools, and skills in place to prevent attacks from happening, and limiting their damage when they do happen. The second is to support the industry as a whole to improve security in the maritime supply chain and ensure that every industry stakeholder knows what is required of them. Finally, ship operators need support from regulators and insurers to balance the cyber security risks they face on a daily basis.

As the global trade association for ship owners and operators, the International Chamber of Shipping represents 80% of the world merchant fleet. We have been working to support our members on cyber security issues for many years including the development of industry Guidelines on Cyber Security Onboard Ships, now in its fourth edition; publishing the Cyber Security Workbook for Onboard Ship Use, and providing a voice for ship operators to the IMO and other regulators.

I'm delighted to welcome the publication of The Great Disconnect. Having taken in the views of so many industry stakeholders, this report is an important contribution to the industry's growing body of knowledge on cyber security and I would encourage you as a reader to take stock of its findings and recommendations.

Guy Platten

Secretary General, International Chamber of Shipping

EXECUTIVE SUMMARY

This research explores the maritime industry's relationship w ith cyber security risks and makes recommendations to ship owners and operators to improve how those risks are managed within their organisations.

The Great Disconnect takes into account the views of more than 200 industry professionals through a combination of an industry survey and research interviews conducted with cyber security experts and stakeholders.

The Great Disconnect takes into account the views of more than 200 industry professionals through a combination of an industry survey and research interviews conducted with cyber security experts and stakeholders.

There is a wide range of actors that could choose to target ships. These can vary from individual opportunists to highly sophisticated state sponsored teams and organised crime groups. For the majority of sophisticated attacks, there is a financial motivation at play. Despite the recent conflict between Russia and Ukraine, attacks by nation states are thankfully rare. But when they do happen, they are often more severe. Indiscriminate ransomware attacks on critical infrastructure, spoofing of positioning systems, and targeting of critical choke points are all trademarks of nation-state actors attempting to disrupt the industry.

Within maritime organisations, there is a disconnect between the perceived and actual readiness to respond to an attack. Whether at sea or ashore, the more senior a member of staff is, the less likely they are to know if their organisation has suffered from a cyber attack. At sea, 26% of seafarers do not know what actions are required of them during a cyber security incident, and 32% do not conduct any regular cyber security drills or training. Ashore, 38% of senior leaders either don't have a cyber security response plan or are unsure if their organisation has one.

Similar issues exist across the maritime supply chain, with a disconnect between the security standards ship operators are working to and the standards that the industry's suppliers work to. This problem is compounded by the fact that many operators have little to no control over the security of

systems that are installed onboard, creating a disconnect between the exposure for the ship operator and their ability to control the risks. This supply chain disconnect is built into regulations too, with the IMO Cyber Risk Management resolution placing the burden of regulatory compliance solely on ship owners and operators.

44% of industry professionals reported that their organisation has been the subject of a cyber attack in the last three years. Of those, 3% resulted in a ransom being paid by the victim to the attacker, at an average cost of US$3.1million. Though it is rarely expressly forbidden, paying ransoms is a legal grey area for ship operators around the world. This issue is compounded by the facts that only 34% of industry professionals report that their organisation has cover for cyberattacks and 54% of ship operators spend less than US$100,000 per year on cyber security management. These figures may appear reasonable for smaller fleets, particularly when you consider that the mean average annual cost of cyber attacks to ship operators is US$182,000. But they don't take into account the large downside risk that all operators face. For 1 in 12 ship operators, the average annual cost of cyber attacks is US$1.8million. Every ship, whether it is part of a small or large fleet is at risk of being targeted by cyber criminals and every ship operator is exposed to a disconnect between the risks their ships are exposed to and the protections they have in place.

Every ship, whether it is part of a small or large fleet is at risk of being targeted by cyber criminals and every ship operator is exposed to a disconnect between the risks their ships are exposed to and the protections they have in place.

To support the industry to overcome these cyber risk disconnections, the authors make four recommendations. The first two recommendations are aimed at tackling the organisational disconnect. They include setting up a dedicated cyber security directorate within fleet operations and implementing a comprehensive cyber incident training and drill programme. The third is aimed at tackling the supply chain disconnect and involves developing minimum security standards for suppliers and partners. Finally, the fourth is aimed at closing the risk disconnect and includes conducting an urgent review of insurance policies and seeking specific legal guidance on ransom payments.

INTRODUCTION

In August 2021, two hackers in a Las Vegas hotel sat down at their laptops and attempted to hack into a small commercial ship. The hackers had no experience of maritime technology and no documentation to help them understand how the ship's systems worked.

While the industry has made great strides to improve cyber risk management to date, significant gaps remain.

After gaining access to the ship's network, they monitored the data traffic alongside the ship's movements to try and reverse engineer the correct commands to take control of equipment. After a few hours, they were able to jam the ship's rudder hard to port. A few hours more, and they could push the throttle full ahead and full astern. In all, despite having no maritime knowledge or experience, the hackers were able to take control of the ship's steering, engineer controls, and fire main in less than half a day.

Thankfully, the Las Vegas hotel hackers had been taking part in DefCon, one of the world's largest whitehat hacker conferences. They took part in the Hack the Sea Challenge, a simulation that invited hackers to attempt to sink a ship. Although the DefCon ship was simulated, all of the software was industry standard and complemented by many real-life operational technology hardware and equipment. The output target was no less genuine than a small commercial ship or a large yacht.

The challenge set multiple teams to a series of tasks working toward the overall goal of sinking the simulated ship. Most of the competitors would complete all the tasks in about 14 hours, including taking complete control of the vessel. The top teams took significantly less time, despite none of them having any experience of maritime control systems.

Hack the Sea aims to engage with the hacker community and help build interest in maritime cyber security. While events like Hack the Sea have served to help the cyber security industry learn about maritime, a growing number of cyber security incidents are forcing the maritime industry to learn about cyber security.

While the industry has made great strides to improve cyber risk management to date, significant gaps remain. This report summarises a research effort taking in the

views of more than 200 stakeholders from across the industry, including cyber security experts, seafarers, shoreside managers, industry suppliers, and C-suite leaders. Cybersecurity is a wide subject matter. So for the purposes of this report, examples are drawn from across maritime organisations, but the analysis and recommendations are focussed on systems onboard vessels.

This research has uncovered three great disconnects that exist across the industry: These disconnections are found where expectations and reality don't match up, cyber risk management efforts are lacking, and where risks are unique to maritime. These disconnections exist internally within maritime organisations, but also across the maritime supply chain, and in how the industry approaches investment and risk. The findings shine a spotlight on those disconnects with the aim of enabling the maritime industry to come together and join up efforts to better manage cyber risks and defend itself against hackers and malware. The recommendations included with the report are aimed at supporting industry stakeholders to drastically improve their position and build new, stronger connections.

These disconnections exist internally within maritime organisations, but also across the maritime supply chain, and in how the industry approaches investment and risk.

UNDERSTANDING MARITIME CYBER THREATS

Thanks in part to several high profile attacks, perceptions of cyber risk across the maritime industry have evolved in recent years. Just five years ago, the commercial shipping industry was seen by many as an unlikely target for hackers.

In recent years, seven of the world's top ten container carriers have publicly acknowledged they have been victims of cyber attacks

But in recent years, seven of the world's top ten container carriers have publicly acknowledged they have been victims of cyber attacks, with all of the leading four carriers being among the victims.[1]

Despite this growing cyber security threat, the industry's understanding of cyber attacks and where they come from remains relatively poor. So too is the industry's understanding of its responsibilities, risks and liabilities. The situation will be improved by forging new connections where today we see disconnects. But in order to build those connections effectively we must understand the landscape of threats that we are trying to defend against.

There are a range of drivers that could motivate attackers. These vary from the benign, such as intellectually curious whitehat hackers with a desire to improve security; to the hostile, such as the desire to inflict physical damage on infrastructure, cargo, or people. The range of actors that might target the industry can vary from highly sophisticated state sponsored teams and organised crime gangs to activists and individual opportunists who have spotted a vulnerability.

But for the majority of sophisticated attacks, there is financial motivation at play. Cybercriminals can monetise their operation by selling extracted data or extorting their victims. Hackers are known to act on bounties posted by nation-states or organised crime groups and cyber crime can be a lucrative career for those with the right skills.

1 Analysis by Thetius, sources: Alphaliner top 100, AXSMarine, ZDNet, The Loadstar, SeaTrade Maritime News, Splash 24/7

By direct extortion, theft or trafficking, the sources of wealth that hackers can extract through digital means is diverse and creative.

ORGANISED CRIME AND OPPORTUNISTS

Worldwide criminal syndicates are increasingly using cyber crime as a source of revenue. Whether by direct extortion, theft or trafficking, the sources of wealth that hackers can extract through digital means is diverse and creative.

In 2011, hackers gained access to the Port of Antwerp's terminal operating system. The compromised database contained precise locational information of each container within the facility. In tandem with the cyber breach, drug traffickers smuggled a steady flow of narcotics in and out of the port for at least two years. Packed within otherwise legitimate containers loaded with timber and bananas were large hidden volumes of cocaine and heroin. The information stolen from the port's operating system allowed the mafioso to break into the secure facility and pinpoint their contraband amongst the thousands of nondescript containers for retrieval. The operation was so effective and discreet that the cargo's lawful owners took no notice as their merchandise was left untouched. Authorities remained unaware until the criminals became overzealous and began removing entire containers from the facility, eventually leading to the operation being uncovered.[2]

In 2016, a group of hackers broke into the content management system of a major container carrier's website, giving them access to the cargo manifests for merchant ships operating globally. In turn, the manifests were sold on the dark web directly into the hands of Somali piracy syndicates. A spate of coordinated attacks ensued where these seafaring criminals targeted specific ships with the highest value cargo onboard. Once on the vessel, the pirates could quickly locate and empty only the relevant containers carrying precious cargo before fleeing. These attacks went on for months before the company eventually identified the pattern and secured the vulnerability.[3]

Though smuggling drugs and stealing cargo can be lucrative, these operations have an inherently poor risk-reward ratio. In contrast, criminals can extort money with minimal risk and significantly greater reward through software categorised as ransomware. Ransomware exploits are comparatively simple to execute and can be either a bespoke design for a unique target or a software package bought on the dark web in the form of ransomware-as-a-service. This code can infiltrate and encrypt critical computer networks, locking rightful users out of the system until a fee has been paid in exchange for its release. While this type of attack has been around for many years, the recent prominence of cryptocurrencies has afforded criminal operators anonymous payment

2 Police warning after drug traffickers' cyber-attack, Bateman, BBC News, 2013

3 Verizon Data Breach Investigations Report, Verizon Security, 2016

methods, making it an increasingly popular form of cyber crime.

As in other industries, ransomware attacks have now become a common occurrence in shipping. This last year Swire Pacific Offshore, who operate a fleet of 50 vessels, became yet another victim of a ransomware attack. Fortunately, the ships were not materially affected, although it was a significant loss to the company and its employees. With varying uncertainty as to the extent of the fallout, analysts believe that stolen data included employee passports, emails, payroll, and banking information.[4] While such personal details have a direct, monetary value on the dark web they could also indirectly enable greater impacts through more targeted future extortion, blackmail and socially engineered attacks on critical systems aboard.

The ransomware threat continues to evolve. In 2021, ransomware threat actors focused their tactics in two areas that should be particularly worrying for the maritime industry.5 The first shift in tactics relates to targeting systems that incorporate operational technology, causing physical and occasionally safety-critical equipment to fail.

The most high profile case in 2021 relates to the attack on the Colonial Pipeline, a major system of petroleum infrastructure that runs from Houston to New York. About 45% of all fuel consumed on the United State's East Coast arrives via this pipeline. In 2021, Russian-linked hackers executed a ransomware attack that shut down the pipeline's operations. With the system down and in critical condition, the owners had no choice but to pay out the US$4.4 million in Bitcoin that the hackers demanded in exchange for restoring operational control.[6]

Secondly, but equally concerning, ransomware threat actors are increasingly targeting supply chain organisations to subsequently compromise and extort their customers. Supply chain attacks tripled in 2021.[7] This includes very high profile attacks on SolarWinds and Kaseya, vendors of software that are commonly used either directly by ship owners and operators, or other organisations within the maritime supply chain.

Ransomware threat actors are increasingly targeting supply chain organisations to subsequently compromise and extort their customers

THE IMPACT OF NATION STATES

While criminals carry out a significant proportion of attacks, nation states have the ability to carry out a significantly more dangerous type of attack. At the time of writing, the world is dealing with the fall out of

4 Ransomware Attack on Swire Pacific Offshore Breaches Personnel Data, Maritime Executive, 2021

5 2021 Trends Show Increased Globalized Threat of Ransomware, Cybersecurity & Infrastructure Security Agency (CISA) Alert (AA22-040A), 2022

6 Ransomware Attack Shuts Down A Top U.S. Gasoline Pipeline, Penaloza, NPR, 2021

7 Software Supply Chain Attacks Tripled in 2021: Study, Security Week, January 2022 - https://www.securityweek.com/software-supply-chain-attacks-tripled-2021-study#:~:text=2021%20can%20be%20described%20as,%2Dparser%2Djs%20and%20Log4j.

Russia's full-scale invasion of Ukraine. A number of successful cyber attacks have been launched throughout January and February 2022, targeted specifically at Ukrainian organisations.

Of the incidents that have been discovered and reported by the global community of cyber defenders at the time of writing, the most concerning relate to a new destructive, "wiper" malware employed on attacks on Ukrainian organisations and attributed to Russian state actors.[8] Unlike ransomware that is designed to encrypt systems, then decrypt them once a ransom is paid, wiper malware is designed to destroy networks and files forever and, sometimes, indiscriminately.

Understanding what makes the industry uniquely vulnerable is critical to overcoming the small shortcomings in security protocol that can result in staggering losses.

COLLATERAL DAMAGE

If the use of "wiper" malware against Ukraine sounds familiar then it's of course because perhaps the most infamous cyber attack on the maritime industry was the NotPetya attack of 2017, also "wiper" malware and also targeting Ukraine. Although the maritime sector was not a direct target, the attack was indiscriminate and brought down digital infrastructure across the globe. NotPetya took down the IT of Maersk Line, FedEx, and US food manufacturer Mondelez International and critical infrastructure such as power plants in the US and throughout Europe as well as several hospitals.

It took several days for Maersk Line to rebuild their network, which they estimated to cost between US$200 million and US$300 million in lost revenue.[9] FedEx estimated the attack cost them US$400 million.[10] Mondelez International made a claim of US$100 million, but their insurer denied it on the grounds that the event was an act of war. Mondelez subsequently brought their insurer, Zurich, to court. At the time of writing, the case is still pending.[11] The ensuing case will likely have a significant impact on the future of cyber insurance.

Though industry players will inevitably become deliberate targets, a substantial proportion of cyber attacks that hit the maritime industry are not necessarily directly targeted to do so. For maritime industry stakeholders, it is crucially important to understand how to protect operations from both targeted attacks and virulent shrapnel arriving from the otherwise unsuspected external digital ecosystem. Understanding what makes the industry uniquely vulnerable is critical to overcoming the small shortcomings in security protocol that can result in staggering losses.

8 Security researchers spot another form of wiper malware that was used against Ukraine's networks, Palmer, ZDNet, 2022

9 Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk, Palmer, ZDNet, 2017

10 FedEx Corporation Annual Report, FedEx, 2019

11 Cyber-insurance shock: Zurich refuses to foot NotPetya ransomware clean-up bill – and claims it's 'an act of war', McCarthy, The Register, 2019

SPOOFING POSITIONING SYSTEMS

Global Navigation Satellite Systems (GNSS) are central to the proper functioning of equipment throughout a ship's navigational systems. But GPS is particularly vulnerable to external influences because the receiver interacts with low-energy signals from space and these weak signals can be easily overpowered with false information. This process is known as spoofing, and has become a serious issue worldwide. Disruption to a small area is simple to execute as amateurs can purchase the equipment required for basic attacks for less than US$100. With the resources of a nation state, a sophisticated spoof on an entire region or sea is not just a possibility, it is a reality.

There is a steadily growing list of large-scale occurrences of GPS spoofing. In 2017, a Russian military exercise was clearly interfering with the positioning systems of over 50 commercial vessels. Fortunately, it caused minimal trouble as the inconsistencies were so great that many ships' digital charts displayed their location far inland near a regional airport.[12] The positioning problem was obvious to those involved onboard and officers proceeded with due caution. However, when the spoofing is subtle, the ship's navigation team may not realise they are under attack, resulting in far more severe consequences.

The Strait of Hormuz is a notoriously difficult stretch of water to navigate. Ships transiting the Strait have to make a difficult turn in crowded water that is shared between Iran and Oman. On the 19th of July 2019, the UK-flagged vessel Stena Impero transited the strait en route to pick up cargo in the Persian Gulf. The ship's regular course keeps it well within the Oman waters, away from the border with Iran. But on this occasion, the ship's crew experienced unusual deviations from their voyage plan and had to continuously adjust the vessel's course to stay on their intended track line.[13]

GPS is particularly vulnerable to external influences because the receiver interacts with low-energy signals from space and these weak signals can be easily overpowered with false information.

Though not confirmed by Iranian or UK authorities, experts widely believe that the ship's GPS was spoofed to force it to cross into Iranian waters unintentionally. Raw Automatic Identification System (AIS) data captured from the vessel by Lloyd's List Intelligence show that the GPS was reporting position data inconsistent with the vessel's true course and speed.[14] Though it is not clear whether the ship actually crossed into Iranian waters, it was boarded by Iran's Revolutionary Guard and detained for two months as part of an escalating diplomatic crisis between Iran and western governments.

12 Mass GPS Spoofing Attack in Black Sea?, Goward, Maritime Executive, 2017

13 Seized UK tanker likely 'spoofed' by Iran, Bockmann, Lloyd's List, 2019

14 Ibid

Whether through spoofing GPS, or hijacking a ship's control system, the ability of a nation state to manipulate the movement of maritime vessels can cause billions of dollars of disruption

TARGETING CHOKE POINTS

40% of the world's oil supply passes through the Strait of Hormuz, making it a crucial choke point in the global supply chain.[15] But Hormuz is only one of a small number of critical waterways that can be manipulated to disrupt world trade. The straits of Dover, Malacca, and Bosporus are equally important narrow channels that occur naturally around the world. Further, man made waterways such as the Panama and Suez canals are vital routes for maritime trade.

The grounding of the Ever Given in the Suez Canal was not caused by a cyber attack but it stands as an example of the fallout of such an event. For six days, the ship remained wedged into the sides of the Suez Canal. It is estimated to have cost the global economy between US$6 billion and US$10 billion per day in lost trade.16 Should malicious actors need an example of the power and simplicity of putting the rudder in a hacked steering system hard-over, they need look no further than the headlines in the news.

Whether through spoofing GPS, or hijacking a ship's control system, the ability of a nation state to manipulate the movement of maritime vessels can cause billions of dollars of disruption, shock the global supply chain, increase the cost of goods, and even instigate international conflict. The Ever Given and the Stena Impero are just two illustrations of hackers' potential power to manipulate maritime assets. Fortunately, direct attacks by nation states are rare; the industry is far more likely to suffer an attack from an unintentional insider.

15 Clarifying Freedom Of Navigation Through Straits Used For International Navigation: A Study On The Major Straits In Asia, Cataldi, Questions of International Law, 2020

16 The Suez canal ship is not the only thing clogging global trade, Allianz Economic Research, Allianz, 2021

CYBEROWL

CASE STUDY

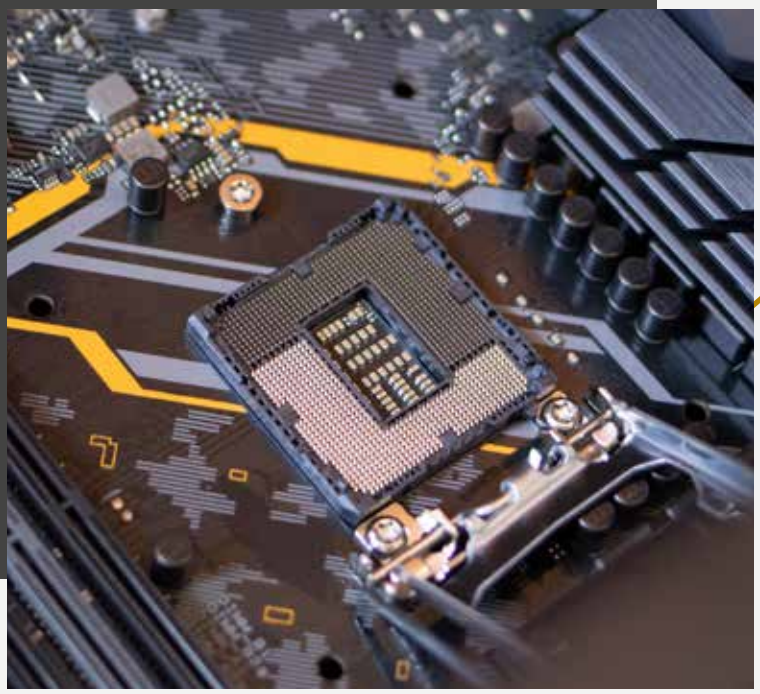
CYBEROWL DISCOVERS NATION-STATE MALWARE ON A FLEET OF COMMERCIAL VESSELS

In February 2022, maritime cybersecurity startup CyberOwl discovered nation-state malware on systems onboard seven separate vessels belonging to a large liner fleet. The malware belonged to the PlugX family, which is designed to provide the attacker remote access to the affected system, followed by full admin control of the machine without permission or authorisation. This includes the ability to manipulate files, execute commands and spread locally. The particular malware variant was first discovered in 2020 and linked to political espionage on foreign nations. This means the malware could have been onboard the vessels for up to two years prior to CyberOwl installing their systems and discovering the malware.

There was no evidence that this particular case was either targeted or has links with the current geopolitical tensions. But this incident serves as an alarming example of how the onboard systems of a commercial shipping operator can get caught in the crossfire of nation-state attacks, as collateral damage.

There are two particular lessons. Firstly, there are particular complexities that raise the likelihood of attacks on shipping systems, even those based on old malware where patches and updates have long been rolled out on land-based systems. Limitations in connectivity, years of underinvestment in technology and the difficulty of gaining access to onboard systems makes it challenging to discover advanced attacks early and remove them before losses are suffered. In this particular case, the malware evaded advanced antivirus software that was already in place on some of the affected machines. The most likely explanation is that the malware was transferred via USB sticks, was not initially detected by earlier versions of the antivirus software, proceeded to behave stealthily for up to two years even when the antivirus was updated and was therefore never discovered.

But how were seven vessels in the same fleet affected? Another important lesson is that vessels are no longer “cyber islands”, where implications of a cyber attack are isolated only to single vessels. A likely explanation is that the malware was delivered via visitors from a specific port, the engineers of a specific vendor or a specific shipyard, making it a real-life example of how concentration risks in cyber attacks could play out in shipping, resulting in fleet-wide losses.



95%

of the cyber incidents on vessels CyberOwl monitored during 2021 could be linked back to the unintentional insider. This demonstrates the pervasiveness of the problem.

THE UNINTENTIONAL INSIDER

Of all the threats to the industry, perhaps the highest frequency of them all comes from the insider. Insider threat comes from a person who has been given authorised access to or knowledge of an organisation. The threat can be either intentional or unintentional. The actor could be an employee, contractor, vendor or simply a visitor to the ship.

In many ways, insider threat is the most unpredictable. Insiders know the weaknesses of the organisation's cyber security and the location and nature of the sensitive data and systems they can abuse. Most of the time they may be circumventing controls with good intentions but this doesn't mean the consequences will be good. If an insider chooses to deliberately breach a system for ill effect, they can be very targeted and accurate with their actions and intent. Because they know the systems, the potentially harmful activities of insiders can be harder to detect than those of external actors.

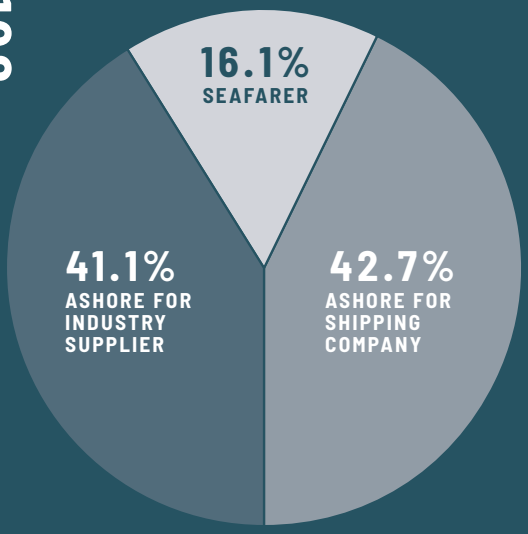
According to data from CyberOwl, over 95% of the cyber incidents on vessels it monitored during 2021 could be linked back to the unintentional insider. This demonstrates the pervasiveness of the problem.

The vast majority of this relates to actions that explicitly contravene the cyber security policies of the organisation, which is often directly referenced within the Safety Management System. Over 60% of computers monitored by CyberOwl have various unofficial or crew-installed software, and 30% of computers make frequent use of the local administrator account giving the user full rights to the machine. The team frequently detects network configuration changes, such as connecting a computer to 4G tethering to download files or software.

Thetius

SURVEY RESULTS AND SUMMARY OF KEY FINDINGS

192 RESPONDENTS



52%

of industry professionals believe their organisation has a process in place for gathering intelligence on cyber security threats.

36%

of industry professionals believe their organisation has been the victim of a cyber attack in the last three years.

BREAKDOWN BY SENIORITY ASHORE:

44% OF EMPLOYEES IN OPERATIONAL ROLES

37% OF EMPLOYEES IN MANAGEMENT ROLES

19% OF EMPLOYEES IN LEADERSHIP ROLES

3% *of cyber attacks resulted in the respondents' organisation paying a ransom.*

$3.1 MILLION *...Is the average ransom paid*

73%

of respondents believe their organisation has a cyber security incident response plan.

BREAKDOWN BY DEMOGRAPHIC:

90% OF SHORESIDE PERSONNEL AT SHIPPING COMPANIES

71% OF SEAFARERS

55% OF INDUSTRY SUPPLIERS

61% OF SENIOR LEADERS

34%

of industry professionals believe their organisation has insurance in place to cover cyber attacks.

> *We regularly conduct cyber security training and drills in my organisation.*

83% *of shoreside employees at shipping companies agree with this statement but only...*

67% *of seafarers agree.*

54%

of shipping companies spend less than $100K per year on cyber security management.

> *My organisation has appropriately addressed cyber risks in the fleet's safety management system.*

87% *of seafarers and shoreside employees at shipping companies agree with this statement.*

$182,000

An average, cyber attacks cost ship operators $182,000 per year.

*For **1 in 12** ship operators (8%), the average cost of cyber attacks is:*

$1.8MILLION PER YEAR

THE GREAT DISCONNECT: WHAT MAKES THE MARITIME INDUSTRY VULNERABLE?

Though maritime faces many of the same cyber risks as other industries, specific vulnerabilities are unique to the sector. For many decades, a ship's best defence from cyber attacks was its isolation.

Without a digital connection to the outside world, it was virtually impossible to infiltrate a ship's system without physically taking action onboard the vessel.

However, in the modern era ships have become more connected, and that defence has gradually deteriorated. Today, ships and the infrastructure that supports them are more vulnerable than ever before. Increasingly complex computerised technologies and systems are being deployed throughout the world's fleet.

Through interviews conducted with cyber security experts, industry leaders, and suppliers alongside an industry first survey taking in the view of over 200 maritime professionals worldwide, we have identified three great disconnects that exist across the industry. These include how maritime organisations function, how the maritime supply chain works and how risk is managed from a financial and legal perspective.

We have identified three great disconnects that exist across the industry. These include how maritime organisations function, how the maritime supply chain works and how risk is managed from a financial and legal perspective.

THE ORGANISATIONAL DISCONNECT

1. DISCONNECT IN LEADERSHIP AND OWNERSHIP

Are you aware of a cyber attack in your organisation in the last 3 years?

2. DISCONNECT IN READINESS

Do you conduct cybersecurity drills and training?

3. WHO TAKES ACTION DURING A CYBER INCIDENT?

Do you know what actions would be required during a cybersecurity incident?

While the industry needs to focus on raising the floor across the industry, including the maritime supply chain, significant internal structure issues exist across many shipping companies that need addressing. These include the visibility of cyber risks to leadership, end to end responsibility for cyber, and the readiness and resilience of the whole organisation.

OWNERSHIP

In most shipping organisations, cyber security falls under the remit of the IT team. The IT team is usually responsible for all information technology assets onboard and ashore. But a common theme uncovered through interviews conducted as part of this research is that the IT team's responsibility stops short of taking full responsibility for Operational Technologies.

Two types of technology are required onboard a ship for it to function: OT and IT. Operational technology (OT) is software and hardware that monitors or controls the vessel's physical equipment. It is distinctly different from information technology (IT), which uses computers to create, store,

and exchange digital information. On a ship, OT generally comprises computer systems that can control engines, steering gear, pumps, or valves. IT, however, is used to provide digital navigation interfaces, facilitate company business, and recorded compliance communication, and provide crew entertainment.

OT usually falls under the duties of the onboard Chief Engineer. While all Chief Engineers are highly trained and skilled professionals, there is currently no provision for them to become experts in OT cyber security alongside their day-to-day roles. OT used to be physically disconnected, granting it cyber protection through isolation, but increasingly that is no longer the case. The risk is that onboard networks are not particularly well-managed. According to maritime cyber security startup CyberOwl, 26% of vessels they monitor have connectivity between onboard OT systems and the shore.[17]

Maritime leaders neither have the complete picture of the risks throughout their technology stack nor the whole picture of the threats they face every day.

As the prevalence of OT attacks on maritime infrastructure grows, the need for a unified approach to managing the security of IT and OT assets grows with it. However, there is an ownership gap for many maritime organisations between the IT security team, which is not wholly responsible for OT, and the engineering team, which is not entirely responsible for security.

This issue compounds because cyber security does not get the internal visibility it needs. Our research found that leaders in maritime organisations do not have a full overview of cyber security issues as they happen. The more senior a staff member is, the less likely it is that they are aware of their organisation being a victim of a cyber attack. 44% of employees ashore in operational roles believe their organisation has been attacked in the last three years. This drops to 37% for employees in management roles ashore and just 19% for senior leaders in C-suite roles.[18]

The study found similar results for those people who work aboard ships. 50% of ship's officers believe their organisation has been the victim of a cyber attack in the last three years. This drops to 33% of ship's masters,[19] pointing to a similar pattern of under-reporting at sea.

The combination of an organisational design flaw that sees no one take end-to-end responsibility for cyber risk management alongside the industry-wide pattern of under-reporting to senior leaders creates a vacuum of unnecessary risk. It also forces senior leaders to make decisions on cyber risk management in the dark. Maritime leaders neither have the complete picture of the risks throughout their technology stack nor the whole picture of the threats they face every day.

17 ReCAAP, Maritime Cyber Security, CyberOwl, 2021

18 State of maritime cyber risk management survey, Thetius, 2022

19 Ibid

AWARENESS

Last year, a ship received an email in its company inbox. The document appeared official and genuine, requesting information on the vessel's future schedule, the cargo carried, the number of crew aboard, security personnel, and if the ship was sailing with defensive weapons aboard. The officer who opened the email clicked the link without caution and dutifully filled in the official forms as requested. Hundreds of miles away, a different ship received a similar email. An officer there responded directly to the email with the requested information and moved on with their day.

The correspondence, however, was not an official email from a port official or stakeholder but rather a spear-phishing attack aimed at obtaining sensitive data from the ship's crew. Fortunately, in this instance, these emails were sent as part of a training exercise developed by the Hamburg based maritime cyber security consultancy Waterway. Across a fleet of 100 ships, 292 "malicious" emails had been sent as part of a penetration test. Crew members across the fleet opened 269 (92%) of them. Of those that opened, a third of them (90) clicked the link in the email and half of those (44) went on to fill out the form, handing over sensitive data about the ship to the attackers. Just over 10% of seafarers that were sent the email (31) replied directly to the email with sensitive information about the vessel.[20]

Although this was a training exercise, it highlights a common tool for extracting sensitive data. Attacks of this nature can create other risks too. Beyond crew inadvertently distributing sensitive information, simply clicking on a link in an email can allow malicious files or software to be downloaded to the ship's computer. A half-step further in poor network security management, and an attacker could critically compromise the vessel and its defences.

Akin to physical security measures, cyber security is an ever moving target. Cyber criminals are constantly creating new attack methods and searching out vulnerabilities.

The fact is that a ship's most significant liability for cyber risk can also be its biggest asset. The human element has the biggest role to play in allowing a cyber breach, inadvertently or otherwise. The crew are also often the first and last defence. While the role mainly pivots on those seafarers, it could also be anyone temporarily on board during a standard turnaround in port. Surveyors, superintendents, loading masters, engineers and contractors can all expose a ship to attack. Every time a device communicates with either the IT network or isolated OT equipment for maintenance, it creates new vulnerabilities.

In light of this, for maritime organisations to build resiliency, there remains a significant need for improved knowledge, skills and training. The current status for skills training is relatively positive across the industry for those in shoreside roles. 83% of shore-based personnel working for shipping companies report regularly conducting cyber security drills and training. This figure drops to 66% for C-suite leaders. 93% of shoreside personnel in shipping companies know what actions would be required of them during a cyber security incident.[21]

20 Cyber-attacks: how hackers are targeting seafarers, Youd, Ship Technology, 2019

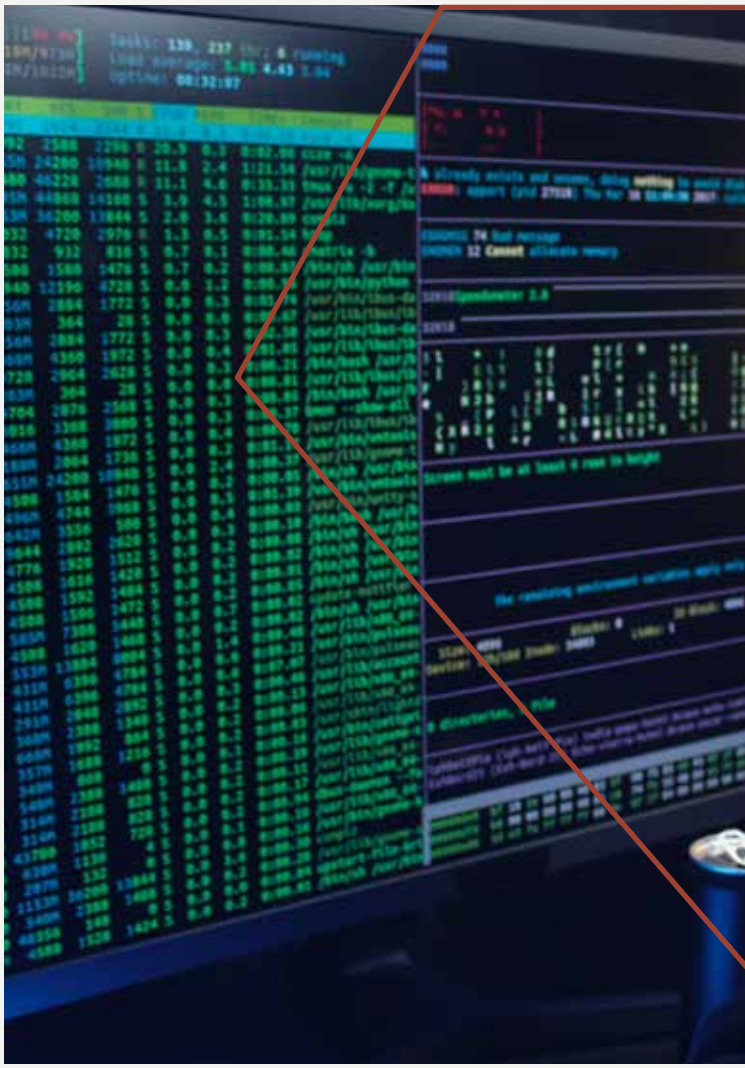
21 Ibid 14

But at sea, the picture is very different. More than one in four seafarers (26%) do not know what actions are required of them during a cyber security incident. Worse yet, nearly one in three seafarers (32%) do not conduct any regular cyber security drills or training.[22]

All shipboard personnel must undertake security training as part of the requirements under the International Ship and Port Security (ISPS) Code. Under the regulation, at least one crew member must be certified through enhanced security training to fill a Ship's Security Officer role. Similarly, at least one member of the shoreside team has to undertake enhanced training for designation as the Company Security Officer. Unfortunately, the ISPS Code, and therefore the training required, only covers physical security–there is no specific provision for cyber security.

In direct line with the industry's organisational issues, the regulatory shortcomings disincentivise any unified approach to cyber security protocol. As ships become increasingly advanced and interconnected to the world wide web, a vessel's physical and cyber security becomes the same.

Akin to physical security measures, cyber security is an ever moving target. Cyber criminals are constantly creating new attack methods and searching out vulnerabilities. As well as understanding the basics of good cyber hygiene, everyone in an organisation has a responsibility to continuously learn about the latest vulnerabilities that the cyber security community has identified. Without a continuous programme of professional development covering the latest relevant cyber threats, the industry will remain exposed to unnecessary risk.

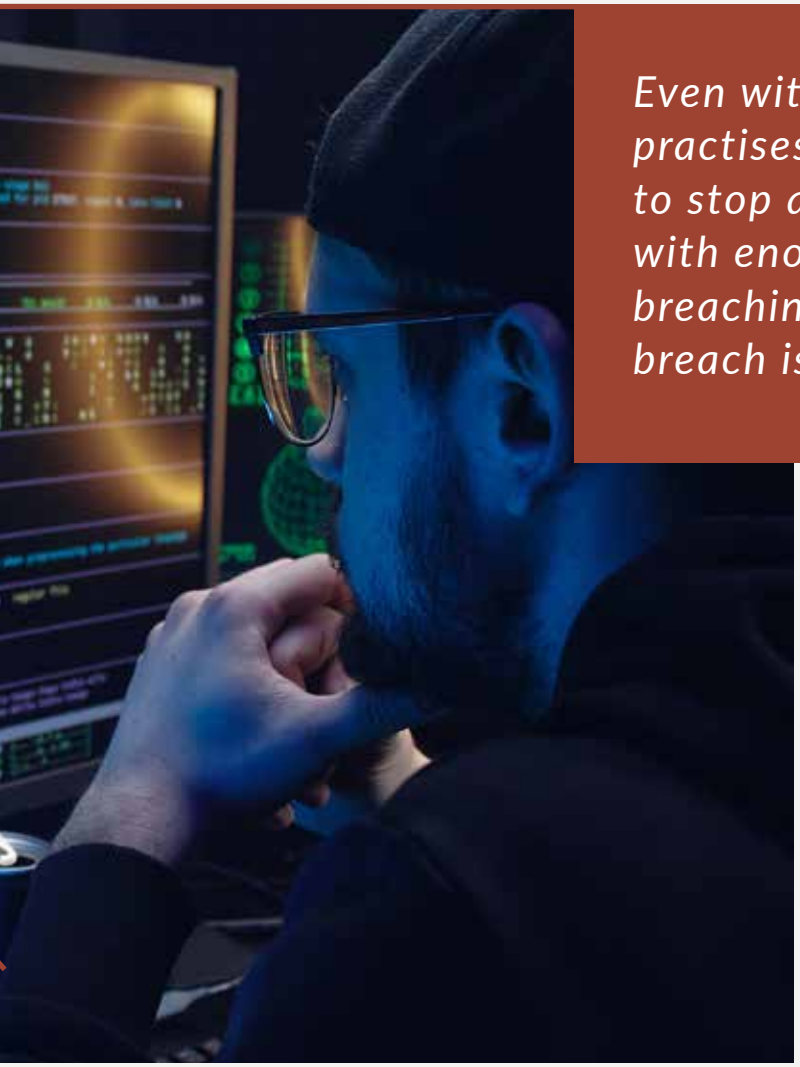


READINESS

Even with the very best cyber security practises in place, it is nearly impossible to stop a highly determined attacker with enough time and resources from breaching a system. Undoubtedly, a breach is simply a matter of time; therefore, it is critical to establish the right contingency plans for business continuity to facilitate an efficient recovery.

A cyber security response plan is crucial to ensuring an organisation knows how to respond when an attack does happen. These plans should be shared and available throughout an organisation based on an individual's role and seniority. Access to the most detailed and sensitive aspects of the plan should be restricted to leadership and security

22 Ibid 14



Even with the very best cyber security practises in place, it is nearly impossible to stop a highly determined attacker with enough time and resources from breaching a system. Undoubtedly, a breach is simply a matter of time

personnel. At the same time, basic plans that detail the actions required of an individual employee should be readily available to them.

When a threat is detected, it needs to be thoroughly analysed to understand which systems are affected and how. From there, it is possible to contain the incident and carefully recover the affected systems. A well rehearsed cyber security response plan should be backed up by high quality intelligence to support a swift recovery.

Our research found that 38% of senior leaders in the industry either don't have a cyber security response plan or, alarmingly, are unsure if their organisation has one. Further, 35% of senior leaders report that their organisation does not regularly conduct cyber security training or drills to ensure they are able to respond to, and recover, from a cyber attack.

Just as the industry regularly conducts safety drills, so too should organisations conduct cyber security drills that stress test cyber security response plans. Wide participation in the drills provides better assurance of the stress testing. For cyber drills in shipping, this should as far as possible include seafarers and key suppliers. Excluding those in leadership positions, 90% of industry professionals who work for shipping companies report that their organisation has a cyber security incident response plan. This figure drops to 71% for seafarers, and just 55% for industry suppliers.[23]

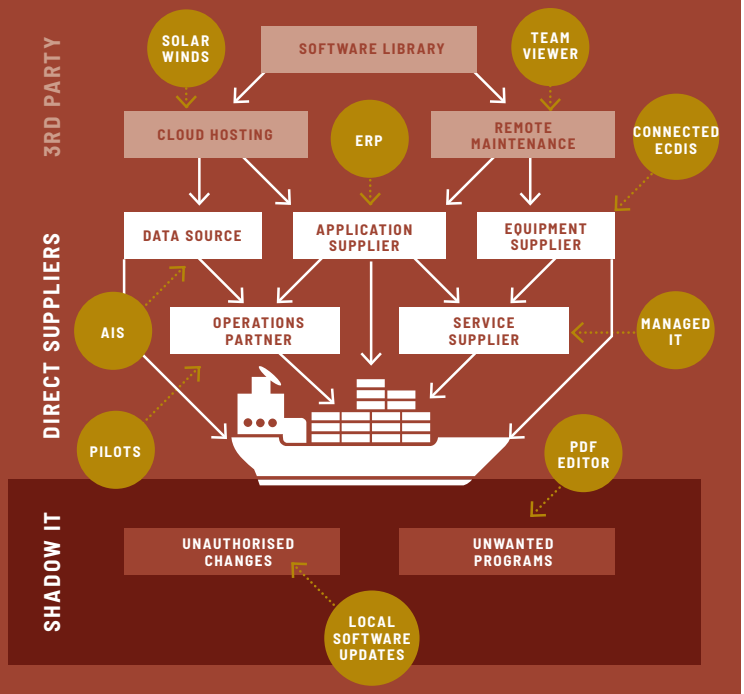
A cyber security response plan should be a living document that adapts based on changing conditions, circumstances and threats. Organisations should have systems in place to gather intelligence on cyber security threats and learn from cyber security incidents, and their organisation's response, after the fact. While 80% of industry professionals report having systems in place for learning from cyber security incidents, only 52% of industry professionals report having a process to gather intelligence on cyber security threats.[24]

23 Ibid 14

24 Ibid 14

THE SUPPLY CHAIN DISCONNECT

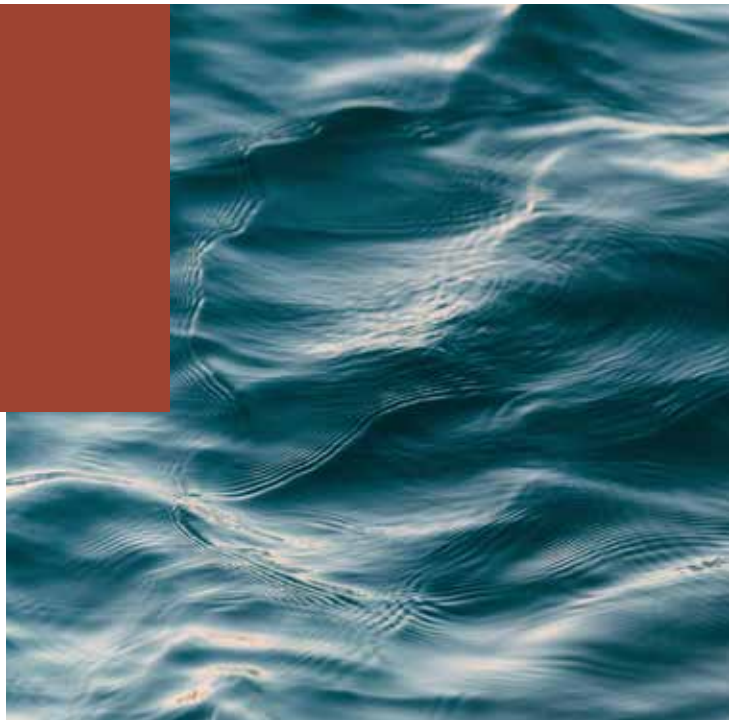
SUPPLY CHAIN VARIETY



The maritime industry serves a critical role in the global supply chain. But the industry also relies on its own supply chain. Everything from fuel for the engines to food for the crew needs to be delivered to ships around the world for the industry to function. This supply chain extends to the supply and maintenance of onboard computing equipment and applications that support vessel operations. The ship owner and operator frequently relies on the supply chain to ensure such equipment and applications are always up to date, well maintained and secure. Every software component onboard a vessel creates some cyber risk, but this research has identified specific areas of concern including the imbalance of responsibilities, the ship operator's lack of control and the disconnect in regulation.

Every software component onboard a vessel creates some cyber risk, but this research has identified specific areas of concern including the imbalance of responsibilities, the ship operator's lack of control and the disconnect in regulation.

Under a charterparty, the ship owner has an express obligation to ensure the ship is seaworthy before, at the beginning of and throughout the voyage.



RESPONSIBILITY

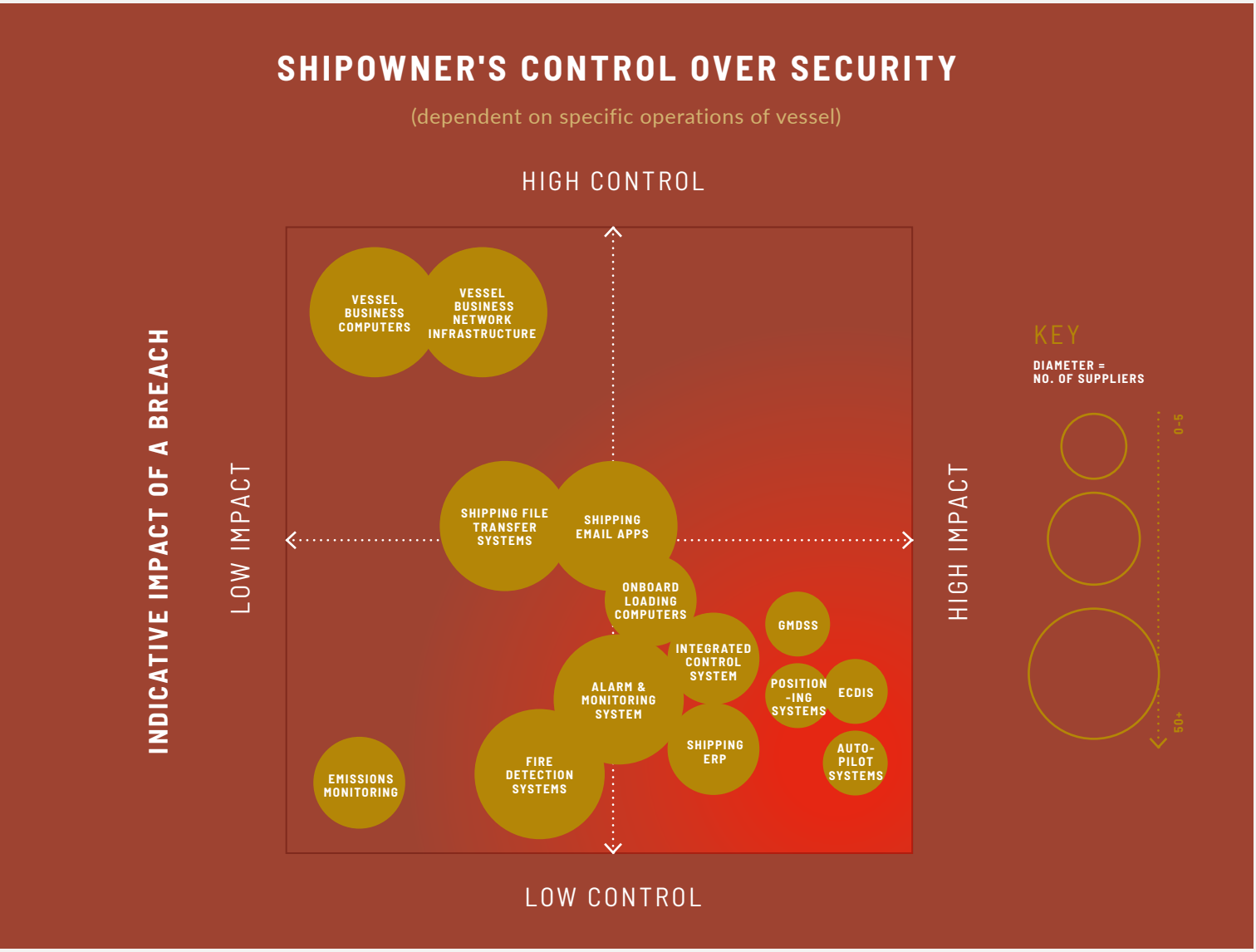
Under a charterparty, the ship owner has an express obligation to ensure the ship is seaworthy before, at the beginning of and throughout the voyage. The owner must demonstrate that they have exercised due diligence to ensure seaworthiness of the vessel.

The obligation on seaworthiness cannot be delegated to third parties. This means that the ship owner must demonstrate they have exercised the due diligence to ensure that any onboard systems must be secure enough not impact the seaworthiness of the vessel, even if the system is supplied, installed or maintained by a third party.

According to our industry survey, conducted as part of this research, 78% of shoreside employees at shipping companies have cyber risk management procedures in place for dealing with third parties such as suppliers. However, the same survey found that just 55% of industry suppliers are asked by customers to prove they have cyber risk management procedures in place. This statistic demonstrates a clear gap in the industry's due diligence of managing supply cyber risk.

Cyber experts interviewed in compiling this report repeatedly pointed to significant risks that exist across the maritime supply chain caused by suppliers not working to an acceptable standard of security. This spans everything from developing systems that are vulnerable even to basic cyber intrusions in the first place, poor practices during installation to insecure practices when visiting the vessel for system maintenance.

The responsibility of the supply chain in relation to cyber risk management of vessel operations is not clear. Equipment or service supply contracts generally clarify responsibilities and obligations in relation to defects in the supplied equipment or deficiencies in the service. However, responsibilities requiring the supplier to ensure a reasonable level of cyber risk management are not explicitly stated in most cases. To make matters worse, shipping cyber emergency response plans are not often developed in cooperation with key suppliers. Where they are, it is rare that exercises or drills are performed involving the supply chain, so lessons on the critical actions that ship owners need their suppliers to perform during a cyber incident are never uncovered, tested and improved.



CONTROL

Though a ship's hull and machinery may remain the same throughout its life, the average commercial vessel has at least 50 distinct systems that contain computing and software components[25]. To the ship operator and their crew, these components are often "black boxes" and there is very little technical knowledge beyond the minimum necessary to operate them, identify a fault or make minor fixes. Certainly, the ship operator is not able to integrate any cybersecurity controls, such as deploying antivirus software or test for any existing defenses, without explicit permission from the equipment manufacturer. Any attempt to do so is generally considered to violate conditions for warranty.

While a small number of system manufacturers have proactively taken steps to shore up the cyber protection of the equipment they manufacture and the applications that are provided alongside these, the vast majority of shipping equipment manufacturers have done very little to provide ship operators assurance around this.

This problem is exacerbated by integrators that are not sufficiently knowledgeable in cybersecurity, making decisions leading to

25 The Guidelines on Cyber Security Onboard Ships Version 4

Operators are not entirely powerless. There are actions they can take to regain some control of securing the supply chain of onboard systems.

insecure configurations and integrations that may undo the security designed into the equipment in the first place. The nature of shipping operations means that when equipment breaks down and needs replacing or repair, it must be dealt with quickly and efficiently as delays can be incredibly costly. Replacements are frequently bought on short order, and purchases are determined by convenience, not security.

This results in a major disconnect between the exposure for the ship operator and their ability to control the risks.

However, operators are not entirely powerless. There are actions they can take to regain some control of securing the supply chain of onboard systems. Getting a clear understanding of the inventory of these computing systems and how they are connected is an excellent starting point.

According to data from CyberOwl, 54% of the ships monitored by CyberOwl have between 40 and 180 connected devices onboard. This includes expected devices such as business workstations, PCs, printers and company phones. Most alarming is that on many vessels monitored by the company, systems that were thought to be isolated, such as cargo computers and engine monitoring systems, were found to be connected to the onboard business IT network somehow.

Interviews conducted during this research suggest the lack of clarity and some level of prescription is creating confusion and frustration.

REGULATION

The main regulation for cyber risk management in shipping relates to the IMO resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management System (SMS). The resolution gives effect to a requirement for an approved SMS to incorporate cyber risk management. Shipping administrations must ensure that cyber risks are appropriately addressed in the SMS no later than the first annual verification of the company's Document of Compliance (DoC) after 1 January 2021.

As this regulatory instrument is implemented via the DoC, it places the burden of regulatory compliance solely on the ship owner. This also follows in the majority of maritime cyber risk management guidelines, that are mainly focused on the actions ship owners can take to cyber secure their ships.

Of those maritime organisations that reported being the subject of a cyber attack in the last three years, 3% said the attack resulted in them paying a ransom. The average ransom paid was US$3.1 million.

For the manufacturer of onboard systems and provider of software-based services for shipping systems, the requirements are a lot less clear.

Several Classification Societies have developed some type approvals specifically relating to incorporating minimum cyber security standards within the design of ship equipment and systems. However, unlike for equipment such as voyage or safety critical apparatus, these are voluntary and do not affect the certification of the ship. At the time of writing, based on a search of the public databases of the type approvals granted, there is minimal uptake of these voluntary type approvals.

Interviews conducted during this research suggest the lack of clarity and some level of prescription is creating confusion and frustration. It results in a level of subjectivity for the ship owner who is now required to ensure their SMS incorporates appropriate cyber risk management of their supply chain in order to be granted their DoC, but cannot point to any minimum standards that their supplier must comply with.

Though a ship's hull and machinery may remain the same throughout its life, the average commercial vessel has at least 50 distinct systems that contain computing and software components.

THE RISK DISCONNECT

CYBERSECURITY INVESTMENT

VS.

CYBERSECURITY EXPOSURE

VS.

THE SIGN OF THINGS TO COME

$100K

Average spend on cyber security management

$180K

Average annual cost of cyber attacks to ship operators

$1.8M

Average annual cost of cyber attacks for the top 8% of most severe cases in shipping

Ultimately, effective cyber security management in maritime requires effective risk management. Without fully understanding the risk profile of the fleet, it is impossible to know what mitigations will be appropriate. Though cyber attacks from nation-state backed groups are still rare, they can cause enormous damage and even cost lives if they are successful. Similarly, random malware infections are a daily threat, but may only have a small impact on a ship's operations. Many ship operators are exposing themselves to unnecessary risk through not being properly prepared for ransomware attacks, not understanding the limitations of their insurance, or under investing in cyber security management.

Those operators who cannot prove that they have taken reasonable steps to manage cyber risk may be operating vessels that are not seaworthy, and therefore not covered by any insurance.

Depending on the circumstances of an attack, paying a ransom may be the only practical solution to a cyber incident.

RANSOM

Depending on the hacker's objective, it is possible that recovering affected systems will require the payment of a ransom. The use of ransomware has been rapidly growing globally, and maritime is by no means immune. Of those maritime organisations that reported being the subject of a cyber attack in the last three years, 3% said the attack resulted in them paying a ransom. The average ransom paid was US$3.1 million.[26]

Depending on the circumstances of an attack, paying a ransom may be the only practical solution to a cyber incident. In 2018, when the SamSam ransomware virus hijacked the city of Atlanta's smart city infrastructure, officials elected not to pay the US$51,000 ransom. Several years on, the reported cost of rebuilding the infrastructure is estimated to be between US$11 million to US$17 million.[27]

Because of the industry's international nature, the legality of paying ransoms can be challenging to pin down. While paying a ransom under certain circumstances can be perfectly legal, it can be illegal in other cases. For example, a ship may be owned in Germany, flagged in Panama, managed in Cyprus, and crewed by Filipino nationals. In that case, it can be complicated to understand which jurisdiction ransom legalities fall under. The rules can also change if that vessel enters the territorial waters of another state or if the person deciding to pay the ransom is a national of a particular state.

Though very few countries have expressly banned the paying of ransoms during ransomware attacks, some laws expressly

26 Ibid 14

27 Ransomware: To pay or not to pay? Legal or illegal? These are the questions ..., Anscombe, WeLiveSecurity, 2021

prohibit payments in some circumstances. For example, in many jurisdictions it is a criminal offence to make payments to terrorist organisations. This can be problematic in the context of ransomware as some ransom demands could be politically motivated. Similarly, ransom payments cannot be made to sanctioned entities or individuals. For example, the United States Office of Foreign Asset Control (OFAC) bans any person under US jurisdiction from transacting with persons, organisations, or nation-states under sanction. In September 2021, OFAC issued an advisory notice with specific information relating to ransomware. The memo states that individuals may be "held civilly liable even if such person did not know or have reason to know that it was engaging in a transaction that was prohibited under sanctions laws and regulations administered by OFAC."[28] It is improbable for the victim of a ransomware attack to know with whom they are transacting, making it almost impossible to know with certainty if they will breach the OFAC rules. Similar laws also exist in England and Wales and across the EU regarding transactions with sanctioned entities and individuals.

Because of the industry's international nature, the legality of paying ransoms can be challenging to pin down.

Outside of specific cyber insurance, there is little in the way of common understanding of how cyber risks are handled in marine insurance.

INSURANCE

Similar uncertainties exist around the insurance sector and the likelihood of a successful claim. 34% of industry professionals report that their organisation has insurance to cover cyber attacks. Outside of specific cyber insurance, there is little in the way of common understanding of how cyber risks are handled in marine insurance.

Several common exemptions specifically exclude cyber risk from insurance policies. Further, where cyber is included, there can be major exemptions. For example, a cyber risk policy that does not cover war-risk. Many of the most sophisticated cyber attacks come from nation state teams or state-sponsored cyber criminals; whether those attacks are "acts of war" is currently a point of contention. There are currently several cases working their way through courts around the world that seek clarity on what constitutes an act of war, and therefore the question of whether state sponsored cyber attacks are covered or not.

The same issue applies to whether a vessel can be deemed seaworthy in light of the IMO 2021 Maritime Cyber Risk guidance. Those operators who cannot prove that they have taken reasonable steps to manage cyber risk may be operating vessels that are not seaworthy, and therefore not covered by any insurance.

28 Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, Department of the Treasury, United States Government, 2021

54%

of ship operators spend less than US$100,000 per year on cyber security management.

INVESTMENT

Over the last two years, the vast majority of ship operators will have invested in cyber security to some degree to ensure they are compliant with the latest guidance from the IMO. But effectively managing constantly changing cyber risks requires an ongoing investment in systems, management, and training for all staff and crew.

54% of ship operators spend less than US$100,000 per year on cyber security management. This figure may appear reasonable for smaller fleets, particularly when you consider that the mean average annual cost of cyber attacks to ship operators is US$182,000.[29] But these figures don't take into account the large downside risk that all operators face. For 1 in 12 ship operators, the average annual cost of cyber attacks is US$1.8million. Every ship, whether it is part of a small or large fleet is at risk of being targeted by cyber criminals. For those unfortunate enough to be successfully hit, the costs of recovery can be several million dollars. Ship operators can no longer ignore the need to invest in effective cyber security management. As the threat landscape continues to evolve, it will become critical to move beyond simple compliance.

US$1.8MILLION

For 1 in 12 ship operators, the average annual cost of cyber attacks is US$1.8million.

29 Ibid 14

BEYOND COMPLIANCE: CONCLUSIONS AND RECOMMENDATIONS TO INDUSTRY

The maritime threat landscape is constantly evolving, and the industry needs to remain alert to and learn to adapt to the threat continually. The measures introduced as part of the IMO 2021 guidance on cyber risk have been a solid catalyst for the necessary change.

87% of industry professionals who work for shipping companies at sea and ashore believe their organisation has addressed cyber risks in their fleet's safety management system in line with IMO 2021. 90% of the same population believe that their organisation takes cyber security seriously.[30] These are encouraging statistics and demonstrate that the industry's approach to cyber risk management has matured significantly in the last decade.

But as the 21st century progresses, the need to raise the minimum standards we all work to will only increase. It only takes one compromised ship to cause significant damage to maritime infrastructure. A major canal or port disruption can cause a ripple effect across supply chains.

Those who plan to attack maritime infrastructure will cast a wide net to catch the weakest vessels in the fleet. To some extent, this means that those who operate ships only need to have better cyber security than their peers to provide some level of deterrent to would-be attackers. To a much greater extent it means that, as an industry, we all need to work together to raise the minimum standard of cyber security in our operations.

This concept is critically important too when we compare maritime with other areas of critical national infrastructure. Cyber criminals who want to attack the infrastructure of nation states will always choose the easiest target that can inflict the maximum amount of damage. The maritime industry is comparatively an easy target compared to the relative security of the energy, aviation, landside logistics, or financial sectors. Though it was not cyber related, the Ever Given taught us that problems with a single vessel can have widespread consequences for the entire maritime community and the wider supply chain.

Standards need to be raised not just to protect a fleet operator's assets but strategic channels and the maritime industry as a whole. The four recommendations below lay out practical measures for ship operators, industry suppliers, and wider stakeholders that if adopted will help to raise the floor the industry is working to.

30 Ibid 14

1. SET UP A DEDICATED CYBER SECURITY DIRECTORATE WITHIN FLEET OPERATIONS THAT COVERS BOTH IT AND OT SECURITY

One of the most significant vulnerabilities uncovered during the research process has not been to do with any particular technology, vessel type or operating environment. Instead, the research has shown a significant disconnect between senior leaders in organisations that operate ships, those responsible for the security of IT systems, and those responsible for protecting OT systems.

Whether at sea or ashore, the more senior an individual is, the less likely they are to be made aware of a cyber security incident. Further, while information technology plays a critical role in the development of a cyber attack, it is operational technology that ultimately has the greatest potential role in causing real world damage. Despite this, OT systems seldom fall under the remit of a shore-based IT security team.

Taking a holistic approach to cyber security that includes both IT and OT systems alongside physical security is critical to maintaining protection in a fast moving world. Therefore, the authors recommend that ship operators set up a dedicated cyber security directorate responsible for monitoring and protecting both IT and OT systems and have direct communication with senior leadership ashore. This could be incorporated into another team or role. But, it is critical that the directorate takes overall responsibility for security and is given the authority and resources to be able to gather data-driven evidence of the actual state of cyber security within the fleet assets and operations on which to base its decisions for improvement. The directorate should be tasked with developing and reporting key performance indicators and metrics on the cyber risks and cyber security performance of the organisation to the management team on a regular basis. This will help close the communications and ownership gap that clearly exists across organisations and the industry as a whole.

Taking a holistic approach to cyber security that includes both IT and OT systems alongside physical security is critical to maintaining protection in a fast moving world.

2. IMPLEMENT A COMPREHENSIVE CYBER INCIDENT TRAINING AND DRILL PROGRAMME

The best defences in the world cannot prevent a determined attacker from breaching a system; therefore, everyone in an organisation, whether at sea or ashore, must understand what actions are required of them during a live cyber incident. Indeed, beyond the individuals involved, it is crucial to stress-test the systems and processes that have been developed to support an organisation during a cyber incident.

The cyber security response plan won't always run smoothly and any failures must be seen as an opportunity to improve. Just as ships need to conduct drills to test crew response to a range of safety incidents, the organisation should also test everyone's response to a cyber incident.

The authors recommend that all maritime organisations, particularly those involved in the operation of ships, implement a cyber security training and drill programme. The programme should be based on practical scenarios that reflect the actual setup and security posture of the organisation, its people, processes and technology.

At every level in an organisation, all personnel should understand what a potential attack looks like, what their responsibility is, and what their response should be. This is particularly true for those who work on ships, where the consequences of an attack can cause significant damage to people, the marine environment, cargo or the vessel.

Senior leaders in organisations should have an understanding of the decisions they are going to need to make during a cyber attack, in order to enable their organisation to deliver the best response to minimise losses and disruption. They should have confidence that systems and processes have been put in place to ensure that the right information gets to the right people to make the right decisions, quickly. This is not just about how the security team should respond from a technical perspective, but how the organisation should respond, communicate with and manage the wide variety of potential stakeholders and victims, both internally and externally. Exercises of this nature don't have to be expensive or time consuming, but if conducted regularly they can make a critical difference in the outcome of an incident and the extent of damage limitation for the organisation.

The cyber security response plan won't always run smoothly and any failures must be seen as an opportunity to improve.

3. DEVELOP MINIMUM SECURITY STANDARDS FOR SUPPLIERS AND PARTNERS

A clear pattern that has emerged from the data gathered through the industry survey was that maritime suppliers work to a much less stringent cyber security standard than the ship operators that they serve. On average, industry suppliers reported a 10% lower score than those who work for ship operators across all of the self assessment questions asked in the survey. The differences were particularly stark considering that 79% of shipping companies' professionals reported having cyber risk management procedures in place for dealing with suppliers. Still, only 55% of suppliers reported being regularly asked by customers to prove they have cyber risk management procedures in place.

As with any sector that relies on heavy assets, maritime is deeply dependent on its supply chain. The industry has made great strides in changing attitudes to cyber security, but without the proper controls in place throughout its supply chain, it remains highly vulnerable. In addition to the suppliers themselves, the equipment that is installed on vessels needs special consideration.

Particularly for older vessels where equipment has been replaced multiple times throughout the ship's lifespan, it can be a significant challenge to understand the on-board systems and how they all interact fully. It is doubtful that most crew members fully understand the dependencies between operational technologies used for navigation, engineering or cargo operations. It is critical that a complete end-to-end inventory of the on-board systems, their connections and their dependencies is developed through either observations via physical surveys by trained cyber security technicians or through analysing data extracted from vessel networks and systems. Without this, it is almost impossible for cyber security teams to understand the level of risk a vessel faces or how to protect it.

55%

Still, only 55% of suppliers reported being regularly asked by customers to prove they have cyber risk management procedures in place.

The authors recommend that all ship owners and operators create a cyber security standard that is incorporated into the procurement or counterparty due diligence processes. This can be designed as a supplier code of connection which sets a minimum cyber security standard for the supplier before they are permitted to connect to vessel systems or access to data from the vessels. A good supplier code of connection should also impose obligations on a supplier to support the ship operator in the event of a cyber incident. For smaller suppliers, this could take the form of a light-touch self certification that fundamental cyber security measures are being taken. For larger suppliers or those who provide critical connected equipment, a more in-depth due diligence process may be required. Not only should suppliers assess the risk of equipment before delivery to the vessel, but also the operating practices of all organisations involved in the supply chain.

4. CONDUCT AN URGENT REVIEW OF INSURANCE POLICIES AND SEEK SPECIFIC LEGAL GUIDANCE ON RANSOM PAYMENTS

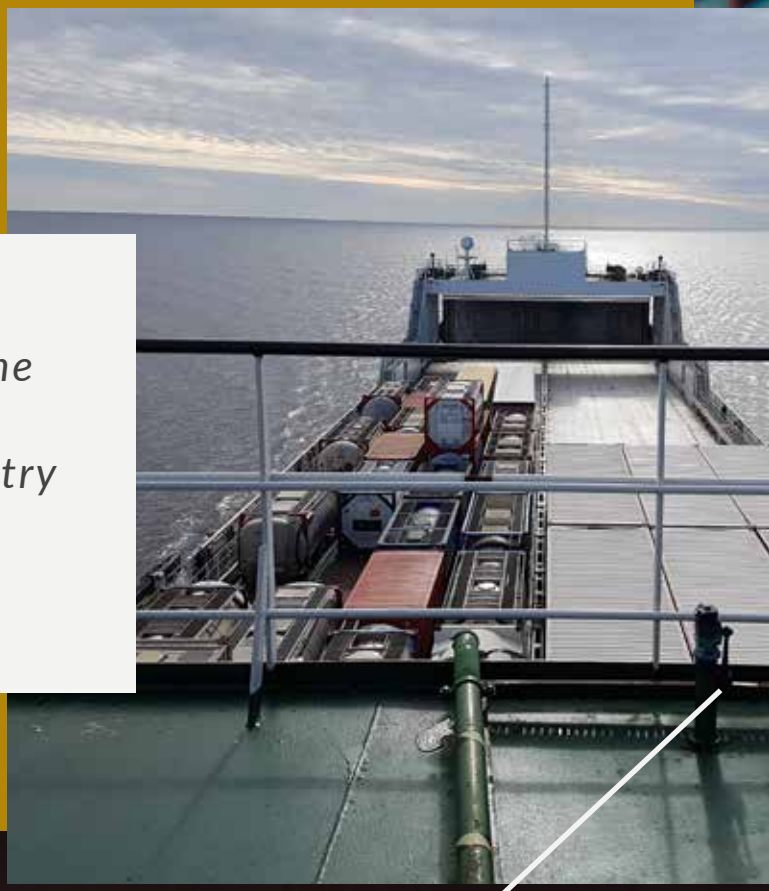
Cyber criminals represent a genuine financial risk to the industry. Major cyber attacks have cost the industry hundreds of millions of dollars to date. But we are yet to see the consequences of a catastrophic physical loss caused by a cyber attack. The cost of a sunk ship, significant oil spill, or a marine choke point blocked through a cyber attack could run into billions of dollars. As with any major financial risk, it is critically important to have appropriate coverage.

Without an urgent review of the insurance policies, the question of cyber risk cover lacks clarity. Only 35% of respondents to our industry survey confirmed that their organisation has insurance in place to cover cyber risks. Though many organisations may believe they are covered under existing policies, for many policies there are blanketing exemptions they should be aware of. Further, even if cyber threats are not specifically exempted, the circumstances of an attack and the failures of organisations to address earlier failures and vulnerabilities identified in cyber security systems and processes could lead to denied claims.

Another area that needs clarification is the legality of ransom payments. Ransom payments should only be a matter of last resort when safety is compromised. Even in those circumstances, the legality of making the payment can be challenging to assess in real time. This is true for victims of the attack, and for every entity and individual involved in facilitating the payment. Though it is impossible to review every scenario in advance, operators must understand their legal position based on the regular trading pattern of the vessel, the flag state, the country of ownership, and the country the ship is managed through.

The authors recommend that all vessel operators conduct an urgent review of insurance policies throughout their organisation to understand any risks that are not fully covered. Further, we recommend that operators seek legal advice on ransom payments specific to their circumstances and incorporate the findings into their cyber security response plan. In addition, the authors urge insurers from across the industry to issue guidance to clarify their conditions of coverage. Finally, we recommend that flag states give their own legal recommendations on the legality of ransom payments in their jurisdiction.

Operators must understand their legal position based on the regular trading pattern of the vessel, the flag state, the country of ownership, and the country the ship is managed through.

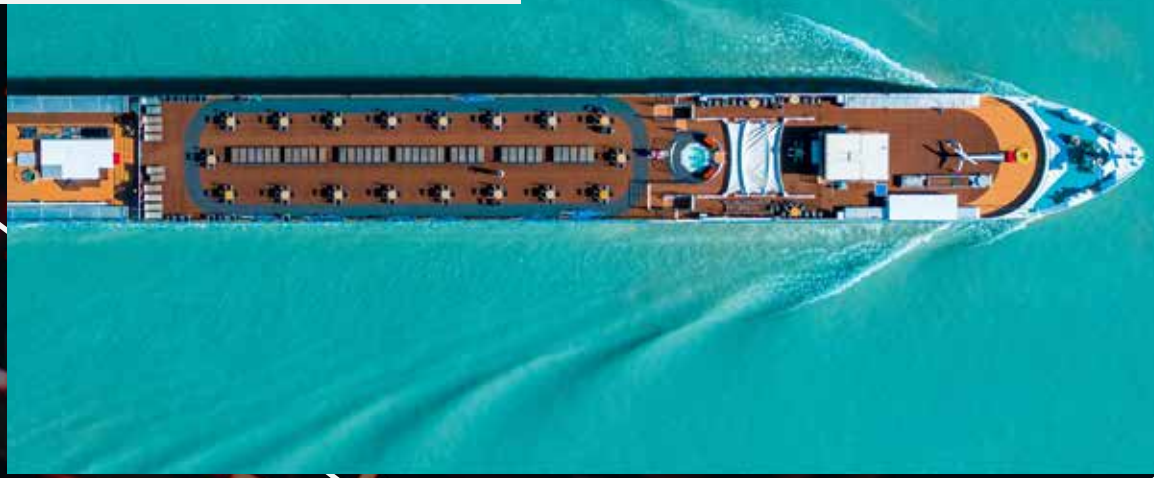


There is no doubt the industry has come a long way since June 2017, when the IMO adopted MSC.428(98). But there is a great deal more distance to travel. The results of the industry's first major survey into attitudes towards cyber risk show that stakeholders across the board take the issue seriously. With nine out of ten vessel operators reporting that they have incorporated IMO 2021 into their SMS, it is clear that significant changes to policy, and procedure have already taken place.

However, this research has also uncovered a number of significant disconnects between those whose work is central to maritime operations, those leading the industry, and the suppliers that support them. To a greater or lesser extent, every maritime stakeholder has worked to improve their own cyber security. But those efforts are currently siloed, with little sharing of information and best practice. This is true both vertically within organisations and horizontally across the industry.

Despite the genuine progress made, the industry must view compliance with IMO 2021 as a first step towards protecting the world fleet. The resolution affords the industry only the most basic of protections. In time, raising the minimum standard that we all adhere to is the only way to protect this vast industry.

The industry must view compliance with IMO 2021 as a first step towards protecting the world fleet.



ACKNOWLEDGEMENTS & NOTES

ACKNOWLEDGEMENTS

The authors would like to thank the many people from the shipping industry who gave up their time and expertise to help shape this report. This report is the result of the collective ideas, experience, and input from countless people at all levels of our industry. Particular thanks go to all those who took time to be interviewed, too many to mention individually. Beyond the interviewees, thanks go to the hundreds of people from across the industry who took time to contribute to our survey. Your honest feedback goes a long way to improving our collective understanding of cyber risks.

To all of the team at CyberOwl, particularly Sara Fortes and Russel Kempley for contributing so much expertise and so many ideas to this project. To all of the team at HFW and HFW Consulting including Tom Walters, Henry Clark, Paul Dean, Chris O'Callaghan, and Chris Johnson. Particular thanks goes to Sharon King for taking so much time to edit and improve the narrative of the report. Lastly, to Michael Salmon, for your outstanding contribution to visualising both the narrative of the report and the data collected throughout this project.

ADDITIONAL NOTES

This report is based on a combination of primary research including one to one interviews and a survey of industry stakeholders alongside high quality secondary sources including academic research, journals, and published media. 22 primary research interviews were conducted with industry stakeholders including ship operators, cyber security experts, and industry suppliers at various levels of seniority.

The industry survey received 192 responses. 43% of responses were from members of staff at shipping companies, 42% of responses were from members of staff at industry suppliers, and 16% of responses were from seafarers. The subsequent analysis of the data was conducted by Thetius analysts, with support from team members at CyberOwl and HFW.

The recommendations in the report are based on the findings of the survey, primary research interviews, and the expertise and opinion of the author team. They are intended to serve as a guide to all ship operators, regardless of the types of vessel they operate. We therefore would encourage all readers to consider how best to adapt them to suit the specific nature of their operation.

Whilst every care has been taken to ensure the accuracy of the report, the information is intended for guidance only. It should not be considered as legal advice.

REFERENCES

ANALYSIS BY THETIUS, SOURCES:

Alphaliner top 100, AXSMarine, ZDNet, The Loadstar, SeaTrade Maritime News, Splash 24/7

Police warning after drug traffickers' cyber-attack, Bateman, BBC News, 2013

Verizon Data Breach Investigations Report, Verizon Security, 2016

Ransomware Attack on Swire Pacific Offshore Breaches Personnel Data, Maritime Executive, 2021

2021 Trends Show Increased Globalized Threat of Ransomware, Cybersecurity & Infrastructure Security Agency (CISA) Alert (AA22-040A), 2022

Ransomware Attack Shuts Down A Top U.S. Gasoline Pipeline, Penaloza, NPR, 2021

Software Supply Chain Attacks Tripled in 2021: Study, Security Week, 2022

Security researchers spot another form of wiper malware that was used against Ukraine's networks, Palmer, ZDNet, 2022

Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk, Palmer, ZDNet, 2017

FedEx Corporation Annual Report, FedEx, 2019

Cyber-insurance shock: Zurich refuses to foot NotPetya ransomware clean-up bill – and claims it's 'an act of war', McCarthy, The Register, 2019

Mass GPS Spoofing Attack in Black Sea?, Goward, Maritime Executive, 2017

Seized UK tanker likely 'spoofed' by Iran, Bockmann, Lloyd's List, 2019

Clarifying Freedom Of Navigation Through Straits Used For International Navigation: A Study On The Major Straits In Asia, Cataldi, Questions of International Law, 2020

The Suez canal ship is not the only thing clogging global trade, Allianz Economic Research, Allianz, 2021

ReCAAP, Maritime Cyber Security, CyberOwl, 2021

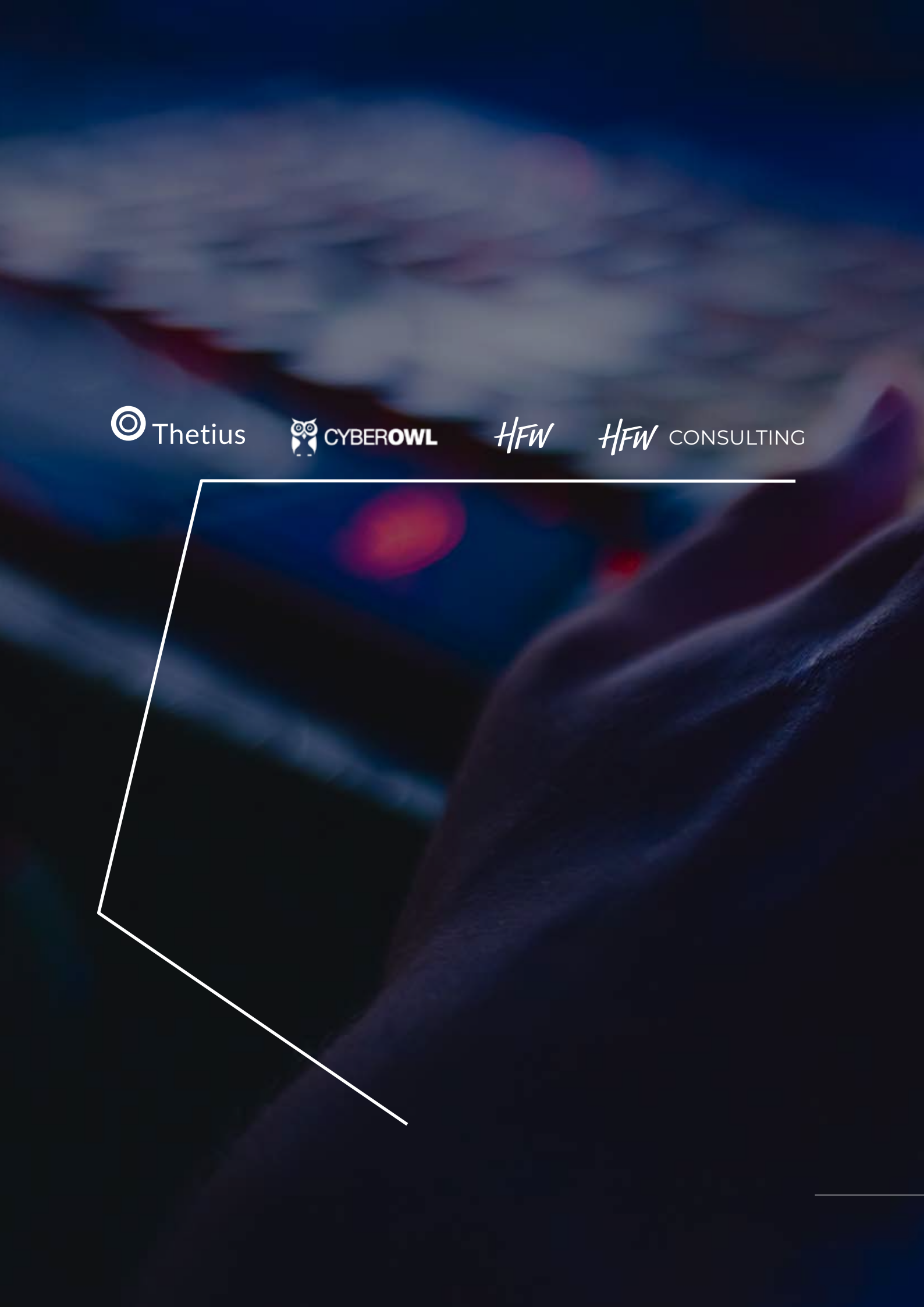
State of maritime cyber risk management survey, Thetius, 2022

Cyber-attacks: how hackers are targeting seafarers, Youd, Ship Technology, 2019

The Guidelines on Cyber Security Onboard Ships Version 4

Ransomware: To pay or not to pay? Legal or illegal? These are the questions ..., Anscombe, WeLiveSecurity, 2021

Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, Department of the Treasury, United States Government, 2021


Thetius
CYBEROWL
HFW
HFW CONSULTING