SHIFTING TIDES, RISING RANSOMS AND CRITICAL DECISIONS

Progress on maritime cyber risk management maturity

Matthew Kenney, Fiona Macdonald

Foreword by Daniel Ng, CEO, CyberOwl and Tom Walters, Partner, HFW

CONTENTS

FOREWORD 4

EXECUTIVE SUMMARY 6

INTRODUCTION 8

THE RECENT PAST AND NEAR FUTURE 11

NEW DEMANDS AND DIFFICULT DECISIONS 16

RISK MANAGEMENT TEAMS 17

Why is it so difficult to understand the total cost of cyber risk? 18

Costs in anticipation of cyber crime 19

Costs as a consequence of cyber crime 21

Compliance is far from static. Why is this often misunderstood? 24

The challenge of getting insured 26

IT AND CYBER MANAGEMENT TEAMS 28

The challenge of resourcing security plans 28

An Interview with industry - The Tanker Fleet IT Manager 30

Finding unicorns - the need for combined maritime and cyber skills 33

To bundle or to disaggregate? 36

FLEET TECHNICAL AND SAFETY MANAGEMENT TEAMS 37

The challenge of empowering self-sufficiency 37

Facilitating the right relationships with OEMs 38

Going beyond compliance - tips from an OEM 43

The need for cross-functional cohesion 44

Connectivity - a double-edged sword? 46

SURVEY RESULTS 48

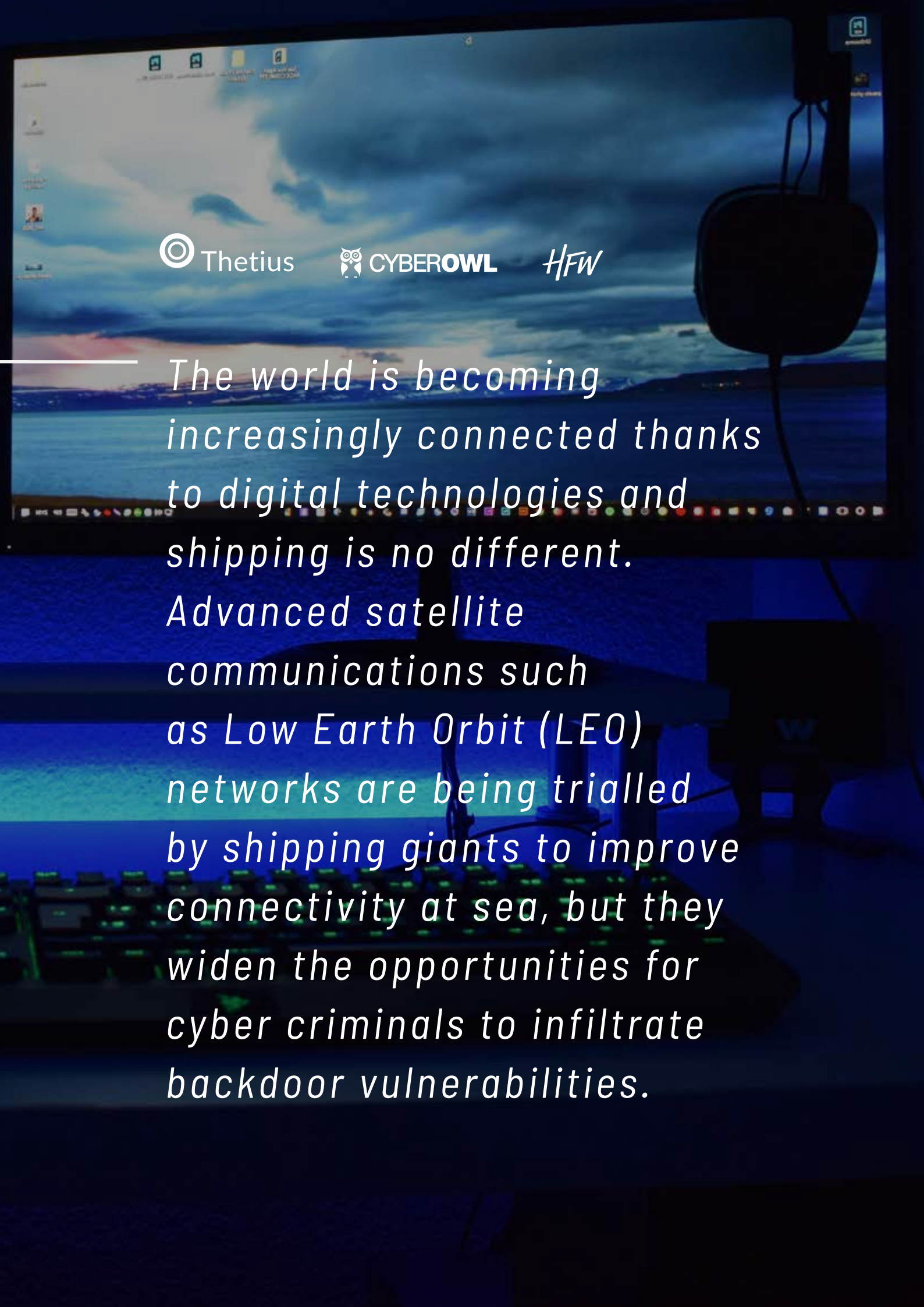
CONNECTING TRENDS - CHARTING PROGRESS SINCE THE GREAT DISCONNECT REPORT 50

SUMMARY AND RECOMMENDATIONS 52

Acknowledgements & Notes 56

References 57

Copyright © Holman Fenwick Willan LLP and CyberOwl Ltd 2023



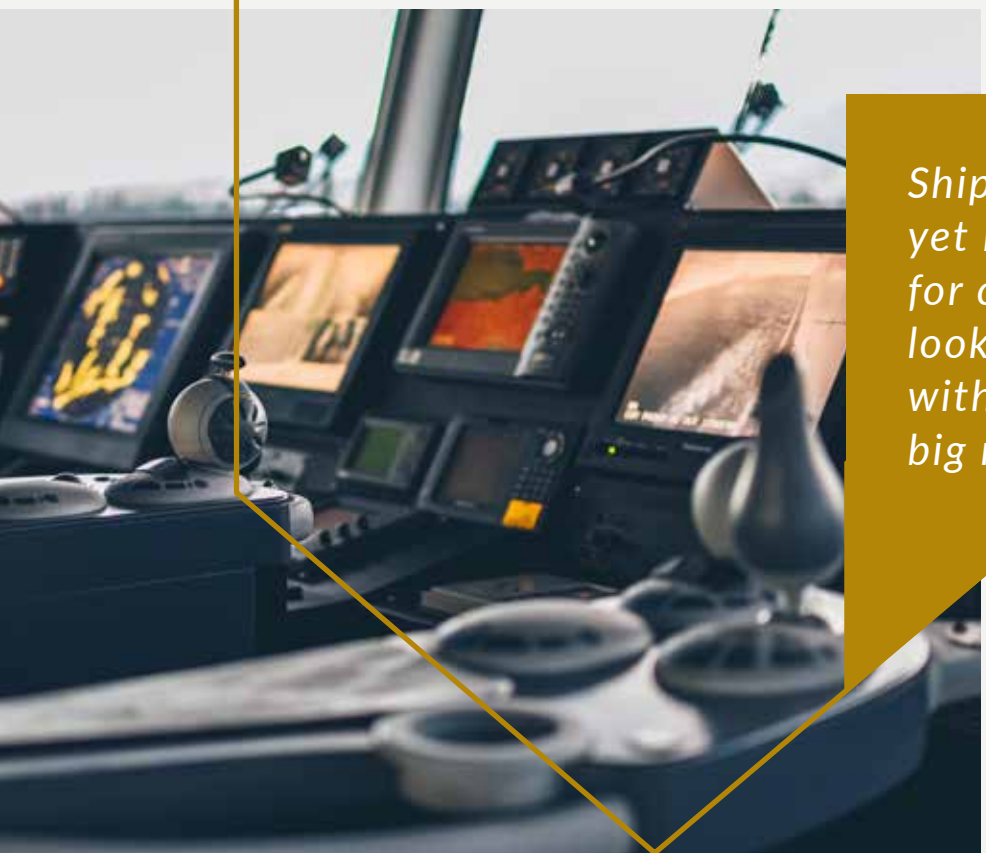
The world is becoming increasingly connected thanks to digital technologies and shipping is no different. Advanced satellite communications such as Low Earth Orbit (LEO) networks are being trialled by shipping giants to improve connectivity at sea, but they widen the opportunities for cyber criminals to infiltrate backdoor vulnerabilities.

FOREWORD

FOREWORD BY DANIEL NG, CEO, CYBEROWL AND TOM WALTERS, PARTNER, HFW

In the last few years, the shipping industry has received a substantial amount of media attention. Shipping keeps the world moving and when an obstruction arises, such as the pandemic, Russia's invasion of Ukraine, or the 2021 Suez Canal blockage, the role the industry plays in facilitating global trade is thrust into the spotlight. Those without a maritime background suddenly become acutely aware of the role ships and their crews play in bringing them their goods safely and on time.

The world is becoming increasingly connected thanks to digital technologies and shipping is no different. Advanced satellite communications such as Low Earth Orbit (LEO) networks are being trialled by shipping giants to improve connectivity at sea, but they widen the opportunities for cyber criminals to infiltrate backdoor vulnerabilities. Shipping is an exciting yet relatively easy target for cyber hackers who are looking for a quick thrill with the potential for big ransom payments. Beyond ransoms, the increased attention on the sector raises charterer and port authority sensitivities towards potential reputational damage. As a result, maritime organisations can no longer just budget for basic cyber protection systems.



Shipping is an exciting yet relatively easy target for cyber hackers who are looking for a quick thrill with the potential for big ransom payments.

In recent years, we have seen an increase in cyber awareness and maturity in the maritime community.

They must consider the financial pressures involved in protecting digital assets and networks from increasingly capable cyber criminals.

In recent years, we have seen an increase in cyber awareness and maturity in the maritime community. Collaboration and a focus on working together to address new cyber threats is evident, and the introduction of new requirements have been welcomed. The International Association for Classification Societies' (IACS) unified requirements (UR) E26 and E27 aim to better align classification societies on their general policies on cyber risk management. However, there is still huge room for improvement as this report demonstrates. Key roles and responsibilities within shipping operations are changing, new risks are emerging, and decisions on investments need to be made. This is not just to reduce quantifiable costs but also to limit reputational damages that can arise following a cyber attack.

Maritime organisations must understand the varying levels of risk across key roles. Ensuring these roles are properly resourced is critical. There are important differences between securing vessel systems and securing enterprise IT, requiring different processes, skillsets and technologies. Building relationships with third parties such as OEMs will be just as important

Maritime organisations must understand the varying levels of risk across key roles and upskill those that need it.

in successfully protecting assets against and surviving attacks, while getting the right insurance will be essential in limiting damage from any attacks that do arise.

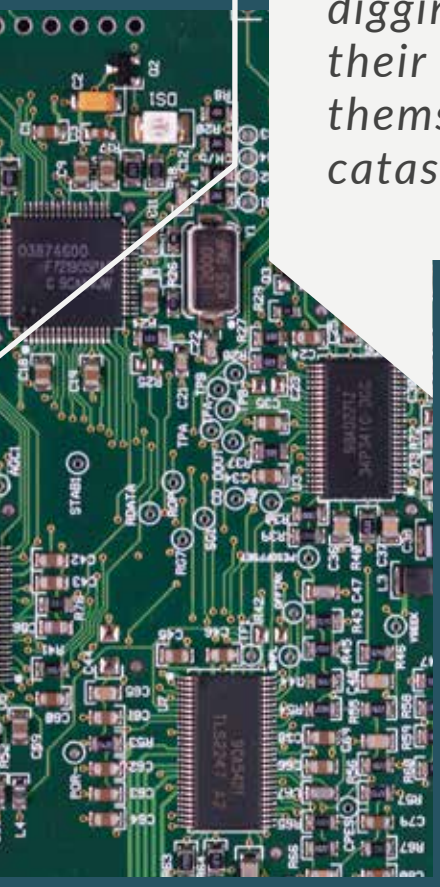
We are delighted to welcome the publication of Shifting Tides, Rising Ransoms and Critical Decisions: Progress on maritime cyber risk management maturity, which builds on The Great Disconnect report that we collaborated with Thetius on in 2022. This report, which considers a multitude of stakeholders' views and experiences, provides valuable insight on the progress that has been made on cyber security, and acknowledges the gaps that need to be addressed to protect the future of an industry that is indispensable to the world's economic growth.

Daniel Ng, CEO, CyberOwl

Tom Walters, Partner, HFW

EXECUTIVE SUMMARY

Within the last 18 months, the average cost of cyberattacks has risen by a frightening 200% and the frequency of ransom payments is up by an astounding 357%.



Larger players are recognising their vulnerabilities and digging deeper into their wallets to protect themselves from catastrophic events.

While it might be hard to conceptualise such an increase, Thetius' latest research in collaboration with CyberOwl and HFW found there is no doubt that cyber security continues to be a serious and complex challenge for the maritime industry today.

Taking into account the opinions and experiences of more than 150 industry professionals from interviews and a survey, we found that while the number of attacks has not risen dramatically since our 2022 research, there is an undeniable increase in the financial impact. Ransom demands have skyrocketed and cyber breaches have cost organisations, on average, US $550K over the last three years.

Another headache that remains largely unchanged since 2022 is the challenge of getting insured. In 2022, Thetius reported that 24% of industry professionals thought that their organisation did not have an insurance policy in place for cyber attacks. Ship operators were found to be unnecessarily exposing themselves to cyber risks by not understanding their insurance policies and limitations. Today's survey found 25% of respondents stating the same thing, while 37% confirmed that their insurance policy did not cover the claim they made following a cyber breach. A lack of maturity in cyber risk management means that many companies' regimes are not at the level they need to be to meet eligibility requirements for insurance policies.

Cyber security and compliance is far from static. Preparedness, including insuring against attacks, and emergency response has not shifted enough since 2022 to protect organisations from the growing intelligence of cyber criminals. Larger players are recognising their vulnerabilities and digging deeper into their wallets to protect themselves from catastrophic events. But this isn't enough. There is a need for different teams in an organisation

to clearly understand their roles and responsibilities when it comes to cyber risk management.

To progress the industry's cyber security readiness and response, it is vital for organisations to understand the changing roles and responsibilities of professionals across risk management, IT and cyber management, and fleet technical and safety management teams.

For risk management teams, the total cost of cyber risk is poorly understood. There is perhaps a misconception that cyber risk management and compliance is static. This is not the case. It requires ongoing maintenance and our research indicates that this is something that many departments are failing to understand or implement.

For IT and cyber management teams, the right security plans need to be resourced. A greater breadth and depth of resources is required and the right decisions need to be made to ensure the correct checks and balances are put in place. This remains one of the top concerns for shipping cyber practitioners at the moment.

For fleet technical and safety management teams, one of the major challenges is empowering self-sufficiency. Crew need ultimate primacy on decisions for safe navigation and operation of the vessel, but this is not always enabled. Moreover, the right relationship with OEMs is vital. An effective cyber security strategy comes from both one-off actions and continuous maintenance of security.

Ultimately, understanding the level of risk across key roles needs work. Roles are changing and there are increasing pressures and demands on people. Blending skills across all departments can provide a more effective strategy to cyber risk management. This can be done via cross-functional cohesion, which allows teams to better evaluate cyber threats and move beyond basic compliance.

Tides are shifting, ransoms are rising, and critical decision making is necessary to safeguard against the future security of the maritime industry.

Tides are shifting, ransoms are rising, and critical decision making is necessary to safeguard against the future security of the maritime industry.

INTRODUCTION

If global cybercrime was a nation state, it would be the third largest economy in the world after the U.S. and China. By 2025, cybercrime could be a US $10.5 trillion industry.[1] This is according to a 2022 cyber security report published by Cyber Security Ventures.

Both the value of a shipping company's digital networks and the amount of investment required to protect them is increasing.

The maritime sector is going digital. Shipping interests are realising the untold value of placing ships onto information exchange networks, and technology, economics, and political will are converging to bring about a notable transformation.[1]

Both the value of a shipping company's digital networks and the amount of investment required to protect them is increasing. More operational technology (OT) is being digitised and there is a greater reliance on information technology (IT) to manage business critical fleet operations. Thetius' previous research found that between January 2020 and March 2021, the average daily data consumption per vessel increased from 3.4 to 9.8 gigabytes.[2] The authors also suggested that the global maritime digital products and services market in 2021 was 18% bigger than previous forecasts predicted. This growth has continued into 2023. But while IT and digitalisation are absolutely critical to delivering efficient, compliant, safe and profitable maritime operations, many operators are still unaware of how much it has already affected shipping.

Robert Metcalfe was an engineer and entrepreneur who contributed to the development of the internet in the 1970s. In addition to co-inventing the Ethernet, he hypothesised that the value of a network is "proportional to the square of the number of users connected to the system." In other words, a network with only one user is worthless, but the value of the network increases exponentially with every additional user. This became known as Metcalfe's Law.

In 2009, Silicon Valley entrepreneur and former Director of the United States Cyber Security Centre, Rod Beckstrom, proposed a revision to Metcalfe's algorithm. In Beckstrom's Law, the value of the network is "equal to the net value added to each

1 Esentire, Cyber Security Ventures (2022) Official Cybercrime Report. Retrieved from https://s3.ca-central-1.amazonaws.com/esentire-dot-com-assets/assets/resourcefiles/2022-Official-Cybercrime-Report.pdf

2 Inmarsat, Thetius (2021) A Changed World. Retrieved from https://thetius.com/changed-world/

user's transactions conducted through that network, summed over all the users."[3] Beckstrom's Law suggests some network users are "bad actors". Malicious activity such as ransomware, Distributed Denial of Service (DDoS) attacks, or other threats, are designed to devalue or even destroy the network, therefore their presence alone cannot be considered value-adding.

Beckstrom sought to introduce the concept that the 'value' of a network could be reduced by the effect of a cyber threat actor and so, no matter how much time and money is spent creating a functional network, its value is eroded by every bad actor which gains access.

As Beckstrom further remarked in 2014: (1) everything attached to a network can be hacked; (2) everything is being attached to networks; therefore, (3) everything is vulnerable.[4] This effect of cyber threat actors on the maritime industry is crucial to understand as more stakeholders place increased reliance on digital networks.

Research conducted in 2022 by Thetius, HFW, and CyberOwl titled The Great Disconnect[5] found that while cyber maturity has increased over the last decade, the industry remains an easy target, "compared to the relative security of the energy, aviation, landside logistics, and financial sectors." But what has become clear over the last 18 months is that the maritime domain does not stand alone in its vulnerability to cyber attacks. Since Russia began its invasion of Ukraine, the risk of cyber sabotage to critical infrastructure used in the offshore industry and renewables sector has reached extreme levels. Data in fibre optic cables, oil and gas in pipelines and electricity in high tension cables, all of which are serviced by many maritime service providers, are just as susceptible to attack. Critical infrastructure requires critical protection, now.

Beckstrom sought to introduce the concept that the 'value' of a network could be reduced by the effect of a cyber threat actor and so, no matter how much time and money is spent creating a functional network, its value is eroded by every bad actor which gains access.

As operational technology (OT) and Internet of Things (IoT) networks proliferate on merchant ships, so does the potential for cyber security breaches. Generic and specific threats, including business interruption, financial exploitation, and significant damage or loss to critical systems are major concerns. But one of the most frequent and painful impacts of a cyber attack is the severe operational disruption it has the potential to cause. We saw the impact the grounding of the *Ever Given* had on the global supply chain in early 2021. It is conceivable that a similar situation driven by a breach in cyber security could lead to an event of equal consequence. In fact, DNV's latest research[6] suggests that a cyber attack could catalyse a closure of major waterways.

3 Beckstrom, Rod, U.S. Department of Homeland Security (2009) The Economics of Networks and Cyber Security. (p.7) Retrieved from https://www.researchgate.net/publication/259254523_Economics_Of_Networks_-_Rod_Beckstrom_National_Cybersecurity_Cente

4 Leisterer, Hannfried, Dr. Alexander von Humboldt Institut Für Internet und Gesellschaft (February 03, 2014). Law, Cyber security and Critical Information Infrastructure Protection. Retrieved from https://www.hiig.de/en/law-cyber-security-and-critical-information-infrastructure-protection/

5 Thetius, HFW, CyberOwl (2022) Global industry report: the great disconnect. Available at https://cyberowl.io/resources/global-maritime-industry-report-the-great-disconnect/

6 DNV (2023) Maritime professionals warn of insufficient investment in cyber security as risks escalate in the era of connectivity. Available at https://www.dnv.com/cybersecurity/cyber-insights/maritime-cyber-priority-2023.html

Employees are expected to operate complex technology in a complex environment and are not always given the tools to understand and navigate the additional security risks that come with it.

Malicious or harmful activity on a ship network, offshore installation or remote control centre ashore, could compromise communications systems, navigation suites, ballast water and cargo management systems, and engine monitoring and control systems among other specific threats. Equally, cross-infection could impact port and terminal operating systems, enterprise resource planning applications, and Radio Frequency Identification (RFID) and telematics systems. Some of these are classed by their host nations as Critical Infrastructure.

There is evidence to suggest that original equipment manufacturers (OEMs), service providers, and users are prioritising building defensive architecture around maritime OT, and at present, the volume of these threats are limited. But the relative nascency of digital development in the maritime sector requires constant vigilance across a range of threats, many of which, as we will see, are difficult to recognise.

The most startling results from the 2022 survey concerned a series of “disconnects”, or points of weakness in organisational structures, supply chain relationships, and risk sharing mechanisms, which made the shipping industry more vulnerable to cyber threats. In an environment where many maritime businesses lack maturity in some or all aspects of their approach to cyber security, finding ways to remain competitive while safeguarding sensitive data, such as confidential information, client and employee data, research and development findings, business strategies, and financial integrity, will become exponentially more difficult over time.

Ships are becoming part of complex nodes on global business networks and their reliance on connectivity and digitalisation is growing. As this happens, the demands, skill sets, and considerations of key roles are changing. Employees are expected to operate complex technology in a complex environment and are not always given the tools to understand and navigate the additional security risks that come with it.

While cyber risk management must remain high on the priority list, our research uncovers that this is not always the case. This report examines vulnerabilities across three tiers of business management: risk management, IT management and fleet safety management, and asks:

- How is maritime cyber risk management maturing?
- How are the demands and considerations of key roles changing?
- How are processes and procedures developing to cope with present and future threats?
- How can the shipping industry work with its trade partners to ensure that cyber security is threaded consistently throughout the supply chain?

THE RECENT PAST AND NEAR FUTURE

In 2021, the International Maritime Organization (IMO) adopted new cyber security provisions into the International Safety Management (ISM) code for merchant shipping. These provisions embedded more specific cyber risk management requirements into the ship safety management system (SMS), formalising deliberate cyber risk management practices into the operation of compliant merchant ships.

Building on less prescriptive requirements that existed in the ISM code prior to 2021, these guidelines offer the industry a defined pathway towards more cyber resilient practices.

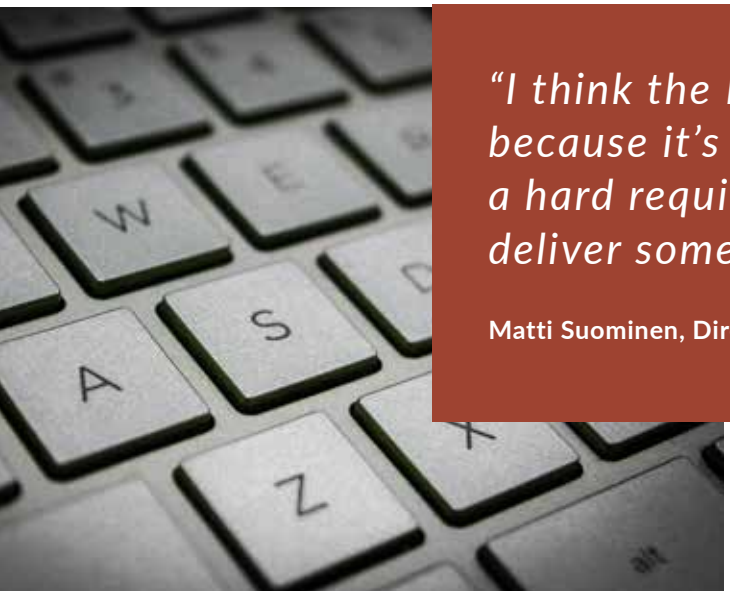
As with all new regulations imposed on an outwardly free market, they met with mixed reactions, but the general feeling from the global shipping community was clear: the emerging cyber threat was recognised and more guidance was welcomed.

Writing on the subject in The Maritime Executive in January 2021, U.S. Coast Guard Associate Director for Maritime Operations, Commander Michael C. Petta remarked, "These new guidelines are a milestone for maritime safety and security. This new model is a vital step towards forging a uniform approach for combating cyber threats against vessels."[7]

Some sub-sectors of the shipping industry had also formed voluntary cyber standards or guidelines prior to those of the ISM code. For example, basic cyber security standards for tankers were included in Oil Companies International Marine Forum's (OCIMF) Tanker Management and Self Assessment (TMSA) requirements as early as 2017. TMSA 3 introduced Element 13, focusing on maritime security and the management and assessment of cyber systems.[8] Following the adoption of the IMO guidelines, BIMCO,

7 Maritime Executive, The (2021) The IMO 2021 Cyber Guidelines and the Need to Secure Seaports. Retrieved from https://maritime-executive.com/editorials/the-imo-2021-cyber-guidelines-and-the-need-to-secure-seaports

8 OCIMF Tanker Management and Self-Assessment 3, published April 2017. Retrieved from https://www.ocimf.org/es/document-libary/175-tmsa3-faqs/file



"I think the IACS guidelines are interesting because it's the first time we have seen a hard requirement for OEMs to actually deliver something with specific features."

Matti Suominen, Director of Maritime Cyber Security at Wärtsilä

Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), InterManager, International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Union of Marine Insurance (IUMI), OCIMF, Superyacht Builders Association (Sybass) and World Shipping Council (WSC) produced "The Guidelines on Cyber Security onboard ships". The guidelines were intended to assist a stakeholder with the development of a proper cyber risk management strategy in accordance with relevant regulations and best practises on board a ship with a focus on work processes, equipment, training, incident response and recovery management.[9] The International Association for Classification Societies (IACS) produced IACS Rec 166 (Corr.1 2020): Recommendation on Cyber Resilience but set out non-mandatory recommendations for technical requirements that stakeholders may want to reference and apply to assist with the delivery of cyber resilient ships. However, generally, most of these publications specified nothing more than a need to address cyber security, leaving the operator to determine the most appropriate minimum course of action.

Recently, IACS announced a set of unified requirements (URs) which seek to align classification societies on their general policies on cyber risk management. Dubbed E26 and E27, these regulations will be applicable to all newly launched classed vessels starting from 2024.

UR E26 provides guidelines for the secure integration of OT and IT equipment into ship networks throughout their lifecycle – from design and construction to commissioning and operation. The guidelines emphasise cyber resilience across identification, protection, attack detection, response, and recovery aspects.

UR E27 focuses on enhancing the integrity of third-party supplied onboard systems and equipment. It outlines prerequisites for cyber resilience in equipment, as well as user interactions with computer-based systems. Additionally, it sets requirements for the creation

9 The Guidelines on Cyber Security Onboard Ships available at https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/ANNEX%20Guidelines%20on%20Cyber%20Security%20Onboard%20Ships%20v.4.pdf

and production of new devices. By leveraging international standards like IEC 62443, IACS will use the new URs to establish requirements spanning scope, threat identification, incident detection, response, and system security.

> *"Having a common framework will make for more efficient conversations and ultimately result in better cyber risk management outcomes. "*
>
> **Tom Barr, Wärtsilä Managing Counsel**

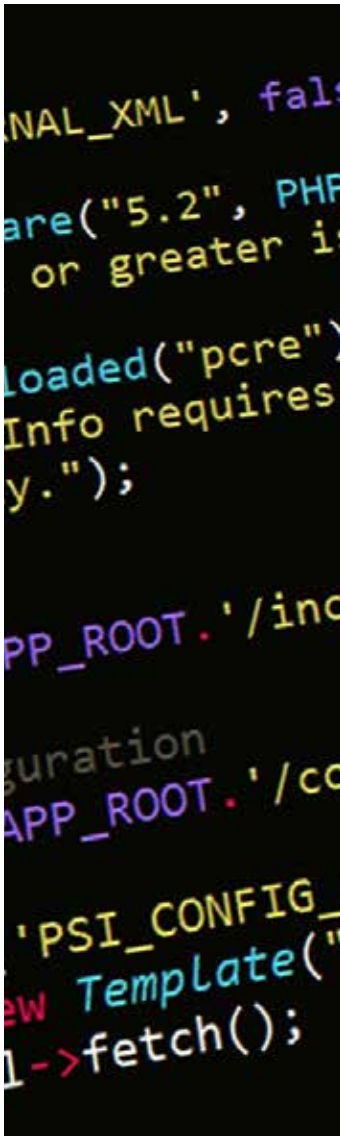
As one maritime cyber security expert observes, "There's the design documents, then there is the system 'as built'. What the IACS is doing with the unified requirements is standardising certain commitments upfront regarding the design documentation. I think that's a good step in terms of pre-empting the potential for the 'jury-rigging' that occurs on board ships."

Matti Suominen, Director of Maritime cyber security at Wärtsilä makes a similar remark from the perspective of the OEM: "I think the IACS guidelines are interesting because it's the first time we have seen a hard requirement for OEMs to actually deliver something with specific features."

Wärtsilä Managing Counsel, Tom Barr, agrees, and points out the value of a consistent approach, adding; "I think that more stringent cyber regulations present an opportunity for the maritime industry to frame the discussion and start talking about cyber requirements in a consistent way up and down the supply chain. Having a common framework will make for more efficient conversations and ultimately result in better cyber risk management outcomes. Rather than each party having their own interpretation, or trying to work out what best practice should look like alone, businesses will benefit from a common steer and that can only be a good thing."

Class societies are not just waiting for the IACS to act. As Mr Suominen says, "On top of the IACS requirements, we are also seeing new requirements emerging from the class societies. This tends to be for customers operating more critical vessels where the IACS baseline may not provide sufficient protections."

Unsurprisingly, cyber resilience across the shipping industry was not in a healthy state when the IMO guidelines were approved by the Maritime Safety Committee (MSC) in October 2021. That same year, one cyber security expert told a webinar audience that from over 750 ships, 600,000 threats, including 1,391 unique viruses were discovered. Each vessel had an average close to two unique virus infections. What's most interesting is that a 15-year old virus was found to be introduced by crew using unauthorised USB drives, demonstrating the low baseline of cyber resilience on ships at the time.[10]



10 Digital Ship. Getting Shipboard Cyber Security Right. 2021. Available at https://www.youtube.com/watch?v=4e6UQBdv6wU

This worrying picture was supported by the fact that 95% of the cyber incidents detected by CyberOwl in 2021 could be linked back to the "unintentional insider", showing the lack of awareness of cyber risk management practices among seafaring crews at the time. That year, there were a number of high-profile attacks in the maritime supply chain including HMM, K-Line, Transnet, Port of Houston, CMA CGM, Swire Pacific Offshore, Danaos Management Consultants, and Hellmann Worldwide Logistics. Attacks were rapidly increasing in scope and frequency, with cyber criminals seemingly becoming more and more interested in the sector. Investment in automation and the digitalisation of maritime operations was rising rapidly, but investment in the cyber security infrastructure to protect it was in deficit, despite a 900% increase in maritime cyber attacks in 2020 alone.[11]

The research carried out for this report goes some way toward bringing this picture up to the present day. The Maritime Cyber Attack Database (MCAD) created by the NHL Stenden University of Applied Sciences in the Netherlands has to date recorded 160 incidents, including the location spoofing of NATO ships visiting Ukraine in the Black Sea in 2021.

Two years after the ISM cyber amendments were implemented, can the industry produce evidence of a greater maturity in cyber security? There is more top-down guidance to come in the form of a wave of new regulations, including the Data Act, the Cyber Resilience Act, and the AI Act, but what will the industry baseline look like when these regulations come into force?

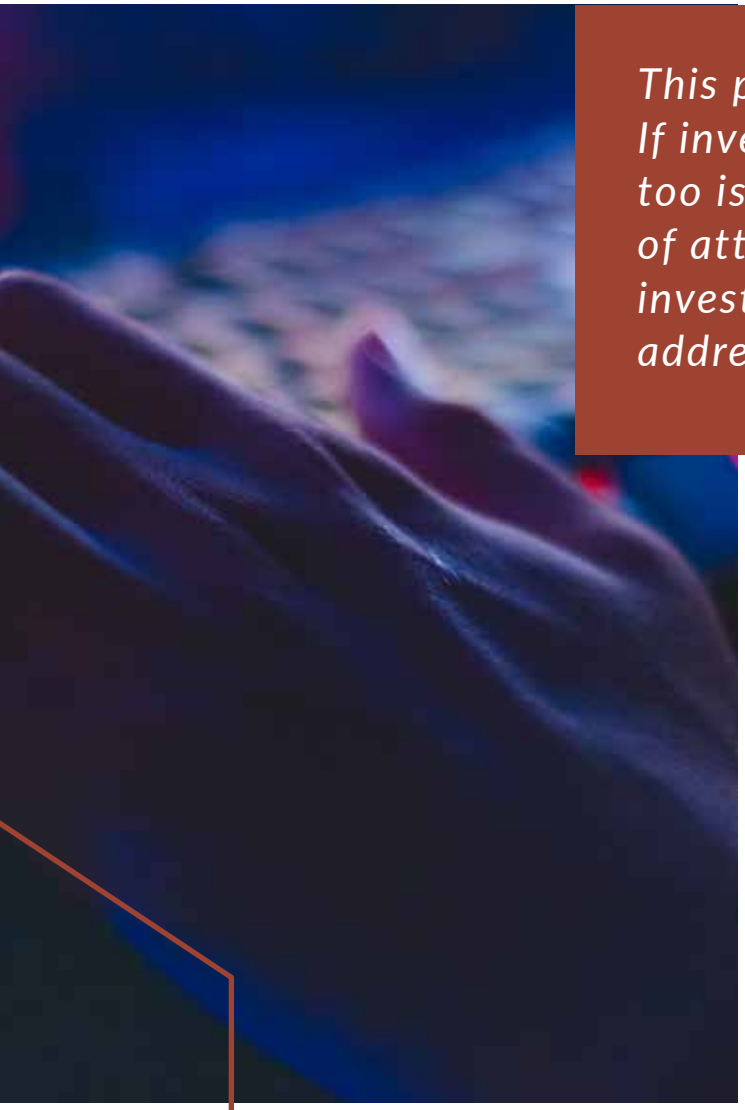
There is also evidence to suggest that, generally, the industry is making strides towards better awareness and understanding of the cyber threat landscape.

Recognising the need for better cyber resilience doesn't appear to be an issue for the maritime sector. According to a 2023 DNV survey, 87% of maritime professionals believe that the future of the maritime industry relies on a significant increase in connected networks between organisations, and 9 out of 10 respondents think that a serious disruption of ship and / or fleet operations caused by a cyber attack is likely in the near future. 79% believe that theft to property or cargo is likely, and more than half (56%) believe that a cyber attack could likely result in physical injury or loss of life.[12]

The DNV survey does reflect some optimism about the state of maturity in cyber risk management. For example, 75% of respondents said that OT cyber security is a higher priority for their organisation today than it was two years ago. However, less than one-in-five could agree that their organisations were very well prepared for responding and recovering from a cyber attack on vessels at sea.

11 Atlantic Council (4th October 2021). Introduction: Cooperation on maritime cyber security. Retrieved from https://www.atlanticcouncil.org/in-depth-research-reports/report/cooperation-on-maritime-cybersecurity-introduction/

12 DNV (2023) Maritime Cyber Priority 2023. Retrieved from https://www.dnv.com/cybersecurity/cyber-insights/maritime-cyber-priority-2023.html?gad=1&gclid=Cj0KCQjwoeemBhCfARIsADR2QCvUogGkYheJKTF_T9TyNV93e672NJnu5B5F6eE4y4yhnf-ztwN75zoaAl33EALw_wcB



This poses an obvious question. If investment is increasing, but so too is the frequency and severity of attacks, are maritime businesses investing in the right solutions and addressing the right problems?

There is also evidence to suggest that, generally, the industry is making strides towards better awareness and understanding of the cyber threat landscape. In the United States, the Maritime Transportation System - Information Sharing and Analysis Centre (MTS-ISAC), formed in 2020, aims to "Promote and facilitate maritime cyber security information sharing, awareness, training, and collaboration between private and public sector stakeholders." Executive Director, Scott Dickerson, told Thetius, "Within four months of its launching, the MTS-ISAC became international and has continued to grow ever since. Currently, there are approximately 70 stakeholders, including various international associations. We encompass multiple elements of the maritime sector: container shipping, bulk shipping, cruise lines, energy shore side, offshore platforms, and vessels. Our stakeholder group operates across six continents, over 160 countries, and contributes billions of dollars to the maritime economy."

He continued: "We're seeing more effort and more investment being made over the last two years. The larger players are definitely beginning to move quicker on cyber risk management because they are able to see the vulnerabilities and realise what could be at stake in the case of a successful attack." However, the general picture remains a concern. Mr. Dickerson concluded, "The attack stream is increasing in frequency and potential severity. Year after year, we see more and more attacks and a broader range of attacks."

This poses an obvious question. If investment is increasing, but so too is the frequency and severity of attacks, are maritime businesses investing in the right solutions and addressing the right problems?

NEW DEMANDS AND DIFFICULT DECISIONS

As shipping steams ahead into the 21st century, operations are changing and regulations are evolving. New technologies are being deployed and these come with their own set of cyber security challenges.

This rush of new demands makes it difficult for shipping leaders to keep up, prioritise investments and make decisions.

But while advancing cyber threats are anticipated, significant uncertainty remains around the impact these changes will have on current and future roles. Key roles and responsibilities within shipping operations are changing and new risks are emerging. Maritime professionals need to be upskilled in order to consider, understand, and manage these additional threats.

However, this rush of new demands makes it difficult for shipping leaders to keep up, prioritise investments and make decisions.

This report explores the 3 key roles that are most impacted by the changing cyber risk landscape - risk management, IT management, and fleet safety management. The research uncovers how these roles, long established in shipping companies, are now evolving to incorporate cyber risk management and the key considerations for each of these roles in decision making.

RISK MANAGEMENT

Refers to those within the organisation who have ultimate responsibility for financial risk and business continuity. In some of the larger shipping operators, this is a separate function with dedicated leadership. But in most shipping organisations, these are a combination of board-level or C-Suite leadership positions. Historically, this function has deep expertise in geopolitical risks, vessel technical risks, ship and fleet operational risks, port operations and physical safety. However, cyber risk is now increasingly on the shipping risk register. There is a significant amount of evidence which shows that good cyber risk management must permeate a business from the top down to be in any way effective, similar to building a good safety culture.

There is a significant amount of evidence which shows that good cyber risk management must permeate a business from the top down to be in any way effective, similar to building a good safety culture.

IT MANAGEMENT

Refers to teams with strategic and operational responsibility to plan and implement hardware and software solutions that enable the business to execute its functions and maintain regulatory compliance. It is common in the maritime industry for cyber resilience to be delegated to personnel with broader IT responsibilities, but this varies widely across the sector. Traditionally, the IT function is treated as a "back office" function in a shipping company, and is still rarely provided dedicated representation at the management team level. However, increasingly, IT teams are rightly or wrongly assumed to be the subject matter experts and enable innovation. As shipping regulation on cyber security strengthens, they are also being thrusted towards the coalface of managing inspectors, vetters and auditors, despite mostly being unfamiliar with the machinations of IMO, charterer bodies and the classification process. Their rapidly expanding remit and lack of authority can also make it increasingly hard for them to deal with emerging cyber threats. As a result, issues at this level can cause damage most immediately.

FLEET SAFETY MANAGEMENT

Has the remit to manage fleet safety and operations from a nautical and ship-technical perspective. Fleet managers are highly skilled maritime operations professionals, usually composed of ex-chief officers, masters or chief engineers. As such, they take responsibility for maritime risks, but do not usually have detailed knowledge and skills in cyber security. As IT and OT take more prominent roles in fleet operations, marrying cyber security skills with those in fleet management is vital. In addition, as the primary regulatory mechanism for cyber risk management of ships is fundamentally connected with safety management systems, strictly the safety function has technical ownership of cyber risk management.

RISK MANAGEMENT TEAMS

It is a long established principle of business that the culture of a company is cast by the senior leadership team. If the board are not concerned by cyber risk management and choose to prioritise other areas of the business, so too will middle management and ultimately the workforce themselves. Scott Dickerson, Executive Director of the MTS-ISAC, observes that cyber resilience firmly benefits from a top-down approach. He told Thetius, "Cyber resilience most definitely starts at the very top. If the

senior leadership team isn't engaged and isn't taking responsibility and owning that responsibility, how can they expect other personnel within the organisation to take it seriously? If management is not taking ownership, then it becomes a box-checking mentality versus one where cyber security becomes embedded, like good safety culture."

There are an increasing number of knowledge sharing, maritime focussed and multi-industrial initiatives that can help businesses to understand the threat landscape. But the first step toward building cyber resilience is overcoming the common scepticism that "it won't happen to us" and getting a better understanding of the total cost of cyber risk to the organisation. It can be equally damaging to assume that you're on par with industry peers. Businesses are reluctant to talk to anyone about their defensive infrastructure or level of investment. They are especially reluctant to talk about vulnerability.

The first step toward building cyber resilience is overcoming the common scepticism that "it won't happen to us" and getting a better understanding of the total cost of cyber risk to the organisation. It can be equally damaging to assume that you're on par with industry peers.

WHY IS IT SO DIFFICULT TO UNDERSTAND THE TOTAL COST OF CYBER RISK?

Many shipping professionals are yet to experience a large scale cyber incident. Whilst one can point to historic examples such as the incident that crippled the operations of Maersk for weeks and reportedly cost US $300 million, these seem remote and unrealistic to the majority of shipping operators who find it hard to relate to the enormous scale of Maersk's operations and the specificity of the particular attack they experienced. The total cost of a cyber attack varies widely and no two attacks will bear exactly the same cost signature. This leaves the maritime risk executive unstuck.

The UK Government has previously put forward a framework[13] for understanding, and budgeting for, the cost of managing cyber risk. They suggest classifying the cost of cyber crime into three categories to represent the distinct stages of how victims experience the costs of cyber crime, which are illustrated in the graphic that follows.

13 UK Home Office (January 2018) Understanding the costs of cyber crime. A report of key findings from the Costs of Cyber Crime Working Group. Retrieved from https://www.gov.uk/government/publications/understanding-the-costs-of-cyber-crime

COSTS

1. COSTS IN ANTICIPATION

... are defensive measures taken by businesses to prevent crime.

2. COSTS AS A CONSEQUENCE

... look at costs that occur as an immediate result of a crime, and typically takes the form of property damage, money lost, emotional and physical costs from crime and reputational damage.

3. COSTS IN RESPONSE

... look at costs that occur as a result of a decision regarding what to do in response to a specific crime.

COSTS IN ANTICIPATION OF CYBER CRIME

Our 2023 survey results indicate some very positive trends here. There is a clear and significant increase in investment in cyber defensive measures. 67% say they spend more than US $100K per year on cyber security management, whereas in 2022, this was only 44%. This indicates that shipping companies that continue to underinvest are rapidly getting left behind their peers and falling short of average practice, let alone best practice.

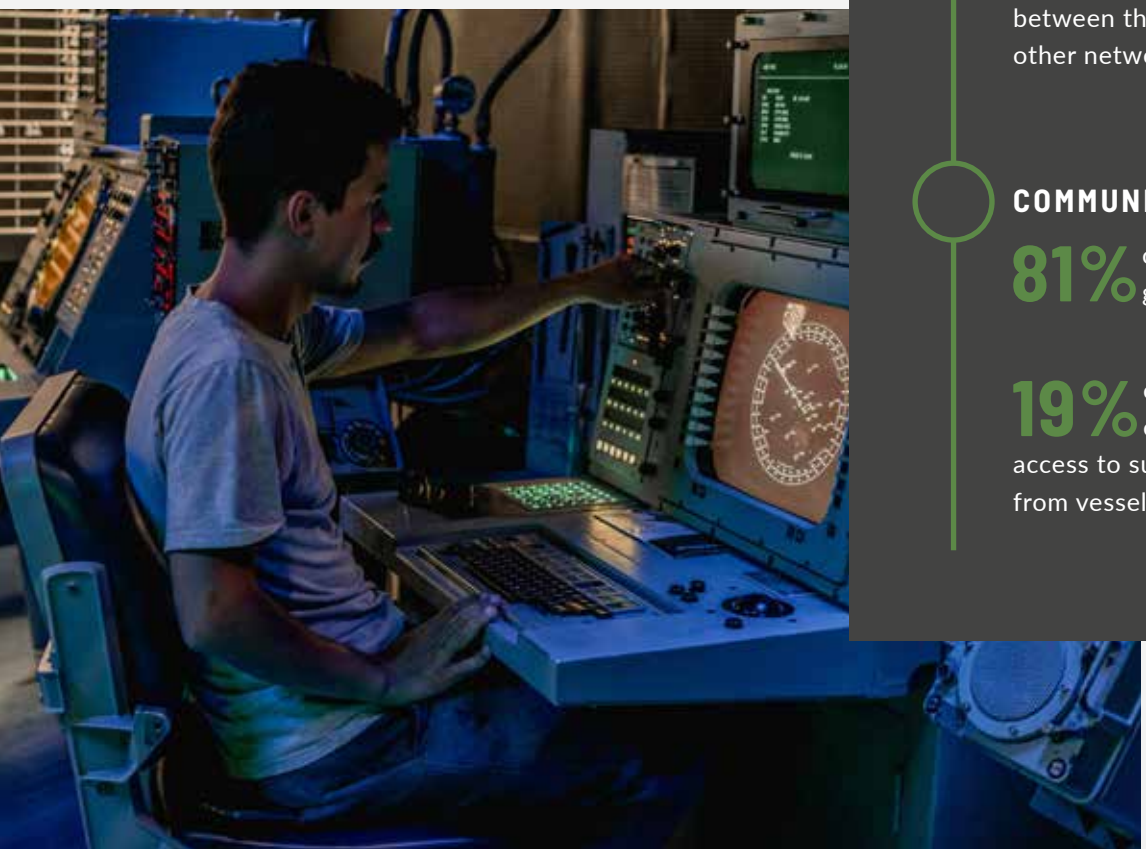
But exactly where are these investments being spent in defensive measures? Whilst there continues to be a very wide range across the sector, some trends are emerging.

There is a clear and significant increase in investment in cyber defensive measures. 67% say they spend more than US $100K per year on cyber security management, whereas in 2022, this was only 44%.

PROGRESS AND GAPS IN CYBER DEFENSIVE MEASURES FOR VESSEL SYSTEMS

It is no longer true that shipping companies are simply not investing in cyber risk management. Some progress is being made, even if this is still in early stages of maturity. To lift the lid on this, the CyberOwl team performed an analysis across the shipping companies they engage with worldwide to get a better understanding of where defensive measures are being strengthened, and which areas still require significant work.

Beyond the obvious costs for implementing cyber security management solutions, such as anti-virus software, staff and consulting costs, physical network security infrastructure, and training, it is important not to forget the hidden costs. For example, additional satcom bandwidth is often required for many cyber security protection solutions. Extra cloud storage may also be needed, and even the price of additional human resources needed to manage cyber security should be considered in the cost of the cyber management protection process. These metrics will also play a role in the overall cost of cyber protection, but are often forgotten.



PROGRESS AND GAPS IN CYBER DEFENSIVE MEASURES

Reviewing controls and risk mitigations that ship owners have put in place so far in 2023, analysis by the CyberOwl team concludes:

STRONGEST AREAS OF DEFENSIVE MEASURES

NETWORK INTEGRITY

77% of vessels have put in some controls to minimise risk of bridging between onboard networks that should be separated.

23% of vessels demonstrate signs of bridging between the vessel business and other networks (e.g. crew and OT).

COMMUNICATION PROTECTIONS

81% of vessels have implemented good web filtering systems.

19% of vessels have limited control and still allow access to suspicious websites from vessel computers.

ROOM FOR IMPROVEMENT

MALWARE SCANNING

30% of anti-virus, anti-malware systems installed on vessel computers are using out of date versions.

ACCESS PERMISSIONS

28% of vessels allow crew to have local admin access for onboard machines. This allows the user to make any changes to those machines as they please.

WEAKEST AREAS OF DEFENSIVE MEASURES

VULNERABILITY MANAGEMENT

68% of vessel computers use obsolete operating systems.

LEAST FUNCTIONALITY

(minimising available functions to users of onboard machines to required-only functions)

63% of vessels provide crew access to more functionality of computer systems than they need for day to day operations.

ONLY 37% have robust controls in place on what software can be uploaded onto the vessel computers.

A survey conducted as part of this research found that respondents believe cyber attacks have cost their organisation more than US $550K over the last three years.

COSTS AS A CONSEQUENCE OF CYBER CRIME

The consequential cost of a cyber incident begins with the immediate aftermath. Software, equipment, and databases may have been damaged, so there will be costs associated with the recovery effort. There may also be direct financial losses associated, such as business disruption, theft, ransom, loss of intellectual property or commercially sensitive information, and reputational damage to repair.

A survey conducted as part of this research found that respondents believe cyber attacks have cost their organisation more than US $550K over the last three years. This is a 200% increase from the results collected as part of our 2022 research.

The major factors contributing to the costs as a consequence of cyber crime were found to be:

- Business interruptions and delays.
- The cost of replacing or restoring systems.

The multi-industrial average cost of an enterprise data breach has risen 2.3% this year to US $4.45m according to a recent report by IBM. In the same report, researchers from the Ponemon Institute add that this cost has risen 15.3% since 2020.[14]

14 IBM (2023) Cost of a Data Breach Report. Retrieved from https://www.ibm.com/account/reg/us-en/signup?formid=urx-52258

THE INCREASING RELEVANCE AND COST OF REPUTATIONAL DAMAGE

It's important to note that in addition to these quantifiable costs, there are reputational costs to consider. Cyber attacks often hit the headlines and the harm they can do to the reputation of a company can be hard to recover from. Social media enables news to spread like wildfire, damaging the reputation of an organisation in an instant, before they have had a chance to commence damage control.

In 2017, Equifax lost four billion dollars in stock market value within a week of a cyber breach and by the end of the year, the breach totaled an additional US $439,000,000.[15] According to Palo Alto Networks, Equifax offered 147,000,000 customers free credit monitoring services for one year and a waiver of the requirement that all disputes be settled through arbitration. Equifax was also ordered by court to spend US $1,000,000,000 in enhancing cyber security measures.[16]

This reputational damage is long-lasting. There is no quick fix. Today people are still talking about the Suez Canal incident in 2021 in which the *Ever Given* vessel blocked the canal for six days, causing complete chaos along the supply chain until she was freed from her grounded position. She remained under arrest by the Suez Canal Authority until early July 2021.

Not only is it hard to recover from reputational damage, but a company's ability to trade with certain key customers will be affected.

While not the result of a cyber breach, the long term reputational damage that has been done is clear. Shipping used to be invisible. But as a result of the Suez Canal blockage and the global pandemic, there is a new appreciation for the role shipping plays in our day-to-day lives. Almost 95% of all worldwide imports and exports are moved by containers. The Just-in-Time supply chain model means that, when things go wrong, the consumer feels and sees the consequences and is immediately reminded of the alarming yet intriguing events such as the *Ever Given*.

Not only is it hard to recover from reputational damage, but a company's ability to trade with certain key customers will be affected. The Suez Canal incident also drew further attention to questions around negligence and culpability in cyber security.

15 Forbes (Nov, 2018) Protecting Your Reputation From Cyberattacks Isn't Impossible If You Do These 3 Things. Retrieved from https://www.forbes.com/sites/ryanerskine/2018/11/28/protecting-your-reputation-from-cyberattacks-isnt-impossible-if-you-do-these-3-things/?sh=3c5234624a66

16 Palo Alto Networks (Jun, 2021) The True Cost of Cyber Security Incidents: The Problem. Retrieved from https://www.paloaltonetworks.com/blog/2021/06/the-cost-of-cybersecurity-incidents-the-problem/

"Of all the risks related to cyber security, reputational risk is in fact one of the larger concerns for the charterer. Perhaps even beyond financial risk. This is because the impacts of reputational risk are longstanding and difficult to reverse."

Max Bobys, Practice Director at New York-based Hudson Cyber, told Thetius, "We don't see reputation being a primary driver of good cyber risk management yet for shipping organisations, but businesses are likely to become increasingly concerned when they begin to understand their potential liability for third party risk or supply chain risk. Once we start to explain that cyber threats are not always just a disruptive event, but they can also be an insidious and persistent exploitation which hides within their network environments; the risk of causing damage to trade partners becomes much more tangible."

Further, during CyberOwl's annual maritime cyber security conference, Cyber Secure at Sea, in Singapore on 18 April, Su Yin Anand, Head of Maritime at South32 at the time, commented that, "Of all the risks related to cyber security, reputational risk is in fact one of the larger concerns for the charterer. Perhaps even beyond financial risk. This is because the impacts of reputational risk are longstanding and difficult to reverse."

Ultimately, this means that shipping can no longer get away with not considering the potential reputational damage of cyber attacks. For many, it is only a matter of time as many marine stakeholders have demonstrated: Maersk was hit by NotPetya in July 2017, Mediterranean Shipping Company (MSC) suffered a malware attack in April 2020 that caused a data centre outage, and South Korea's national flagship carrier HMM was the subject of a cyber attack in June 2021 that impacted the company's email server. A month later, in July 2021, the South African port operator Transnet was hit with a "disruption" that halted operations at various port terminals. This was then followed in September 2021 by an attack on CMA CGM which targeted customer information.

The costs of consequences can be minimised by dedicating the right resources to security operations. But for shipping, matching the necessary cyber experts with those who have an understanding of this niche industry is a very present challenge. This issue is addressed in further detail later in this report.

COSTS IN RESPONSE TO CYBER CRIME

The cost of responding to cyber crime are costs associated with technical and operational response from the cyber incident, costs of recovering the affected systems and processes, documenting and reporting to law enforcement and regulators, planning and executing a public relations strategy for dealing with press and trade partner concerns, engaging cyber security analysts, investigators, litigators, and insurers etc. The extent of these costs depends on the nature of the business and the nature of the attack, but many of these costs may not be covered by insurance products and could be financially destructive.

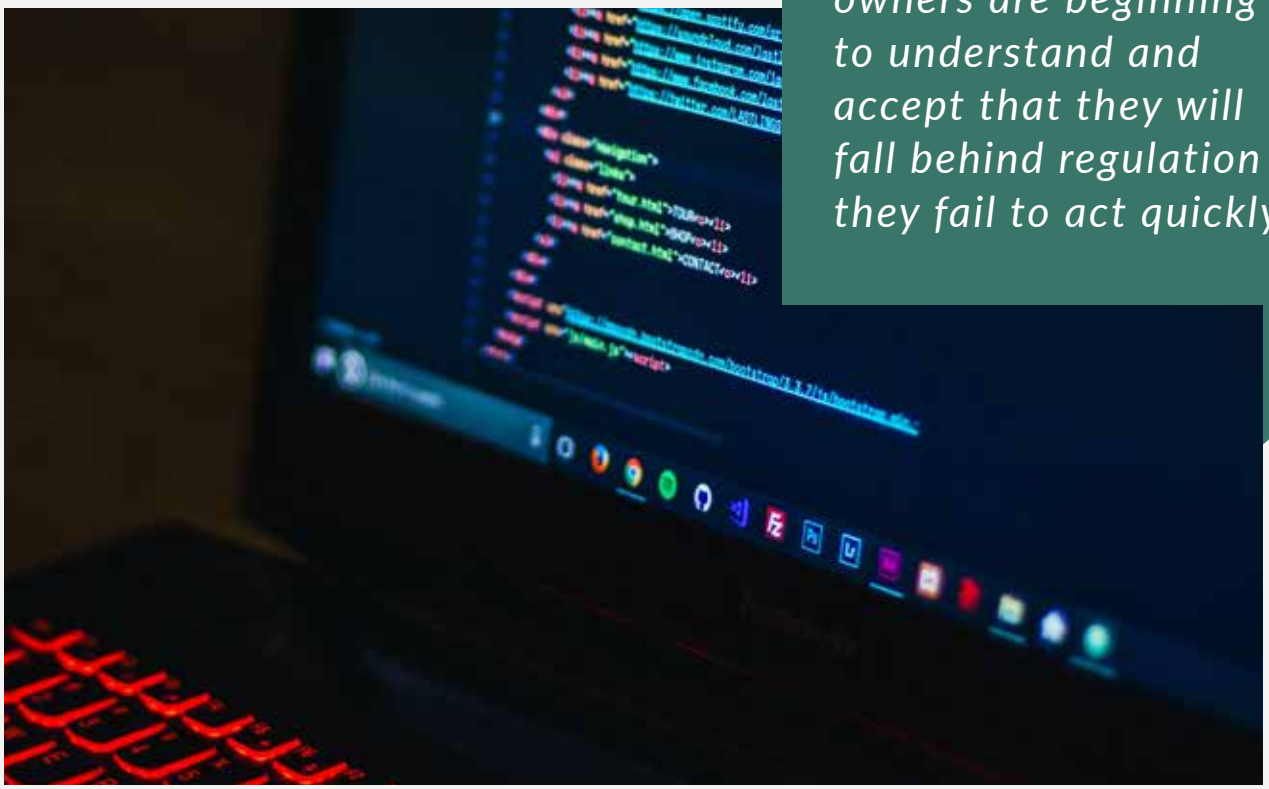
The 2023 survey conducted as part of this research found that only 25% of respondents believe that costs tied to cyber defence, remediation (including public relations costs) and restoration are covered by their cyber risk insurance policy. The majority of respondents believe they will have to pay the financial price for carrying out remediation activities following an attack.

COMPLIANCE IS FAR FROM STATIC. WHY IS THIS OFTEN MISUNDERSTOOD?

Compliance has catalysed change and today ship owners are beginning to understand and accept that they will fall behind regulation if they fail to act quickly. However, compliance is not static. It requires ongoing attention and management; it is not a one-off event. Misunderstanding around this is a major issue for cyber security today.

Reinforcing this point, Annex 2 of "The Guidelines on Cyber Security Onboard Ships" sets out the minimum measures that all shipping companies should consider implementing so as to address cyber risk management in an approved Safety Management System. The document sets out 11 areas of measures and actions. 9 out of the 11 recommended areas require

Compliance has catalysed change and today ship owners are beginning to understand and accept that they will fall behind regulation if they fail to act quickly.



"Many ship owners are used to tolerating high risks, and this is happening with cyber risk too. For some, the default approach is to meet new rules and standards at the minimum baseline."

continuous actions and proactive vigilance that the measure is kept up to date. These include continuous actions that require some investment to implement, such as maintaining up-to-date hardware inventory, software inventory, map of data flows, security audit logs and continuous detection and reporting of non-conformities relating to cyber incidents.

The latest draft of the IACS rules UR E26 (Cyber Resilience of Ships), at the time of print, has many similarities. Even more explicitly, E26 sets out how the one-off actions taken during the design, construction and commissioning phases of a newbuild vessel should be augmented by continuous measures during the operation phase of the vessel. It envisages implementation, annual and special surveys that ensure the measures are up to date throughout the life of the vessel.

Moreover, cyber compliance in shipping has a particular vessel-by-vessel approach to mirror safety and marine engineering regulation. This means that it is entirely possible for owners to choose compliance on some vessels but not others. A good illustration of this is the UR E26 regulation and the UR E27 regulation, mentioned earlier in this report. As these requirements only apply to newbuilds from 1 Jan 2024, some ship owners have actively decided to only aim for compliance on some of their vessels.

Choosing to comply for specific vessels, but neglecting others will create several problems, including:

- **INCONSISTENCIES IN POLICY MANAGEMENT -** will give rise to a range of exceptions that need to be considered, remembered and managed, making maintenance expensive, prone to error and leading to a higher total cost of cyber risk management.
- **MISALIGNED ATTITUDES TO RISK -** cyber risk is by definition not geography-specific and attacks can affect multiple vessels at once. It makes little sense to secure some vessels but not others within a fleet. Research for this report found that there are misaligned attitudes towards risk and compliance.

One tonnage provider told Thetius that in his view, a misaligned attitude to risk is confusing the role and purpose of regulatory compliance. He said, "Many ship owners are used to tolerating high risks, and this is happening with cyber risk too. For some, the default approach is to meet new rules and standards at the minimum baseline."

Pursuing compliance with regulations does encourage good behaviour of course, and even a minimum compliance approach can take a great deal of effort. But threat actors are also aware of the emerging standards and regulations. A minimised approach cannot address cyber risks properly because regulations are very much a starting point and not the final destination. As the tonnage provider concludes, "This seems to be overlooked by some in our industry."

THE CHALLENGE OF GETTING INSURED

As the costs associated with cyber attacks rise, shipping operators are increasingly considering insurance. However, uncertainty around cyber risks is complicating insurance products, exclusions, and claims processes.

Research from the Law Society of England and Wales found that 72% of companies across all industries have not purchased cyber insurance. Figures from Maritime London suggest that 92% of estimated costs arising from a cyberattack are uninsured.[17]

Research for this report found that 25% of respondents admitted that their organisation does not have cyber risk insurance, while 42% were unsure as to whether any cyber insurance even exists.

According to Law Society President, Lubna Shuja, "Although stability is returning to the market, the process of buying cyber insurance has become harder, with more paperwork involved and underwriters showing greater aversion to risk."[18] As a result, companies are still finding it difficult to purchase the right cyber insurance and are all too often investing in insurance policies that do not actually cover what they need covering.

This situation is not surprising Robert Dorey, CEO of Astaara, a specialist marine cyber insurer, told Thetius that, "The marine insurance market has been in a state of change as cyber exclusions have removed cyber cover from nearly all marine policies, following direction from insurance market regulators. However, there are still pockets of the marine insurance market where cyber cover is not specifically included or excluded but instead silent on cyber. This ambiguity is in addition to marine cyber solutions often excluding war and terror caused losses without clarifying this to the

insured. Many in the main cyber market do not understand the unique maritime environment and the operational technology interface with information technology. Complex risks need bespoke solutions."

Cover applications are being rejected, largely due to eligibility. This can arise from a lack of maturity in cyber risk management. The problem is that companies' cyber risk management regimes in place are not at the level they need to be to meet eligibility requirements for cyber insurance policies. In some cases, this may not be identified until they become the victim of an attack and realise that their insurance policy does not cover the breach.

Companies first need to check and possibly upgrade their cyber risk management solutions before they can even think about getting insurance. This adds further cost, delay, and complexity to the process.

17 Maritime London (Mar, 2021) Meeting the cyber threat challenge in the maritime industry – protection beyond regulation. Retrieved from https://www.maritimelondon.com/news/meeting-the-cyber-threat-challenge-in-the-maritime-industry-protection-beyond-regulation

18 Law Society, The (21 July 2023) Seven in 10 firms don't have cyber insurance. Retrieved from https://www.lawsociety.org.uk/contact-or-visit-us/press-office/press-releases/seven-in-10-firms-dont-have-cyber-insurance

Companies first need to check and possibly upgrade their cyber risk management solutions before they can even think about getting insurance.

One interviewee told Thetius that they "see some technology vendors say, 'use our tool and you'll get a discount on your insurance'. But it's less about discounts and more about eligibility. A lot of companies are getting cyber insurance cover applications rejected or seeing certain coverage restrictions put in place because their cyber risk management regime just isn't where it should be."

Rishi Baviskar, Global Cyber Experts Leader, Risk Consulting at Allianz Global Corporate & Speciality (AGCS), admitted in research published by Allianz Global in 2022 that, "More than half of submissions from prospective clients still do not meet our checklist of required controls entirely."[19]

In addition, there is a lack of specialist marine cyber insurance solutions available to help owners minimise and mitigate risk from cyber attacks, and the companies that do offer marine cyber insurance products often exclude many areas. Underwriters are increasing exclusions from cover to protect themselves from unknown scenarios. These exclusions can render coverage meaningless.

Furthermore, cyber insurance premium rates are rising, especially for ransomware attacks. According to Allianz Global,[20] this has led to organisations being unable to purchase the cover they previously had to protect themselves.

Vanessa Leemans, Head of Cyber, UK and Lloyd's at AXA XL, told S&P that, "There are now triple ransomware attacks". According to Ms Leemans, hackers first demand money to unlock the systems that they have encrypted, and then demand further ransoms to prevent the release of stolen data from the target company, and affected customers.

Despite this, there is also evidence to suggest that outside of the maritime domain, cyber insurance is playing a larger role in helping to boost security efforts. Ms Leemans was also quoted by S&P as saying, "Over the last two years, we have seen clients improve their security maturity, and I would say that cyber insurance has played a key role in those security efforts."

The report caveats this concern by replacing it with another: "It is important to put this risk into perspective. The level of coverage offered is low relative to the economic losses sustained by economic agents as a result of cyber events each year."[21] This is a less-than-subtle recognition that average pay-outs remain behind the total cost of a cyber attack to policyholders.

19 Allianz Global (2022) Cyber: The changing threat landscape. Retrieved from https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/agcs-cyber-risk-trends-2022.pdf

20 Allianz Global (2022) Cyber: The changing threat landscape. Retrieved from https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/agcs-cyber-risk-trends-2022.pdf

21 International Association of Insurance Supervisors (April 2023) Global Insurance Market Report (GIMAR) Special Topic Edition for Cyber. Retrieved from https://www.iaisweb.org/uploads/2023/04/GIMAR-2023-special-topic-edition-on-cyber.pdf

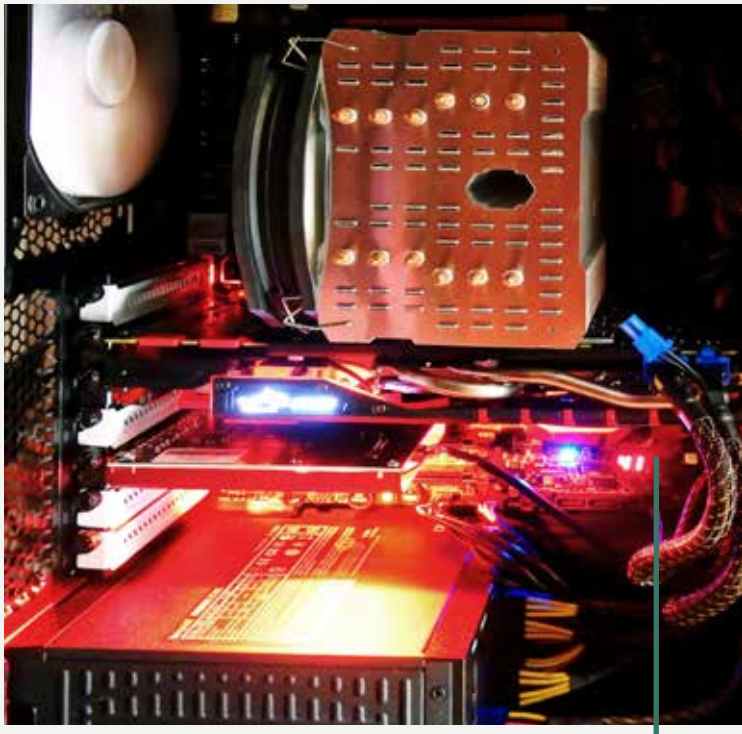
IT AND CYBER MANAGEMENT TEAMS

THE CHALLENGE OF RESOURCING SECURITY PLANS

Given the challenges in understanding and quantifying the total cost of cyber risk, addressed earlier in the report, securing the right resources to manage cyber risks properly can be a difficult task. Cyber risk management doesn't fall neatly into traditional business case categories of driving more revenue or reducing costs. Rather, it is more closely associated with reducing risks and potential financial exposure.

According to UK Government Research, qualitative data reveals a set of issues that prevent boards from engaging more in cyber security. These include a lack of knowledge, training and time, but the same data also highlights, "the importance of people in cyber roles being able to write persuasive business cases for cyber security spending, especially when they report directly to finance leads."[22]

Given the challenges in understanding and quantifying the total cost of cyber risk, addressed earlier in the report, securing the right resources to manage cyber risks properly can be a difficult task.



Thetius' 2023 survey results illustrates the challenge in shipping:

- 33% felt that one of the biggest challenges in improving cyber risk management is understanding the level of risk.
- 30% said that it was difficult to understand best practice.

For this reason, securing the right level of investment in resources is one of the top challenges for shipping cyber practitioners at the moment. Our 2023 survey results further indicate that there is a very wide range of investment in resources related to cyber risk management in shipping:

- At one end of the spectrum, 33% spend less than US $100K per year on cyber security management.
- At the other end, 3% said they invest more than US $10 million.

22 UK Government (April, 2023) Cyber security breaches survey 2023. Retrieved from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023

Ships operated by smaller and less well-resourced operators may be of equivalent size and complexity to those operated by the industry leaders. The challenges and risks associated with a successful attack remain equal. But those with a lack of resources and less ability to invest in and staff a cyber risk management function in house must rely on external assistance or maintain a higher tolerance to risk than their larger counterparts.

Investing in the wrong or insufficient resources can hurt the organisation in ways that are not immediately obvious. Many ship operators quantify one-off costs associated with cyber security solutions, but fail to consider the resources required to maintain the systems and controls they wish to put in place. An example of this is establishing individual logins and passwords. While this sounds like a good security policy in theory, it comes with the operational cost of maintaining up to date logins and passwords in practice, in the face of changing crews and vessel visitors.

Even in the cases where investment has been secured for in-house resourcing, the effectiveness can vary greatly. IBM has observed that only 1 in 3 data breaches were detected by in-house teams. 67% were reported by "benign third parties" offering cyber security monitoring services, or in some cases, announced by the attackers themselves.

One cyber expert told Thetius that there are several overlooked characteristics of the global shipping industry:

"Companies with fleets of around 100 vessels or more tend to have larger balance sheets that are capable of supporting meaningful investments in cyber security. They have greater staff and resource availability, and they are able to purchase tools and apply them in a sustainable way within the context of their operating environment. But then you have the majority of global shipping companies with smaller fleets where resourcing is more difficult and therefore considered less of a priority."

AN INTERVIEW WITH INDUSTRY - THE TANKER FLEET IT MANAGER

Thetius interviewed the Fleet IT Manager of a large tanker operator to discuss their approach and hear first-hand what it is like to be responsible for keeping hundreds of tankers operating without disruption. As we will see, this company takes cyber threats seriously and has the budget and resources to prioritise a comprehensive strategy. But, as the respondent explains, there is more to keeping their fleet safe than the level of investment.

"For us, cyber security is the main pillar on which we build all innovation."

How would you describe the company's general attitude to cyber risk management?

"For us, cyber security is the main pillar on which we build all innovation. Security is the first consideration and only when we're satisfied that it can be achieved to the right level do we launch a new piece of connected technology."

Has this always been the case?

"Cyber risk management has come more to the attention of our senior management in recent years, both the protection of the shoreside office infrastructure and the at-sea fleet. Whatever innovations we bring in, it's a company-wide responsibility to make sure that the risk is effectively managed. And that's something that's mentioned and emphasised again and again by our senior management."

Are cyber audits and inspections becoming more common in your experience?

"From a compliance perspective, we are dealing with an increasing amount of port state control requirements, flag requirements etc, and there are many requirements coming from many different parties. However, from my experience, despite some stories of highly technical audits being imposed on unprepared crews, I don't yet see compliance audits on live systems very frequently. Those that we do get are mostly based on procedures and not requesting snapshots of the state of our network controls, firewalls, anti-virus etc. Nevertheless, I believe this is coming. We are preparing for these kinds of reporting requirements when they are requested."

How about cyber compliance requirements beyond the shipping regulators?

"We are an exchange listed company, so compliance is quite strict in that sense. We have introduced a lot of processes and tools, and changed our whole way of working, from how we manage access to our servers to change management. We need to have security procedures and we are audited every quarter. These audits are massive! They can take up to a month to complete, and two months later you have the next audit. So this is already crazy and the requirements are going up."

"A key shift in attitudes for us has been to bring the issue of cyber security out of the confines of the IT department, bringing our safety management team to work with us on the operational technology side."

How do you treat your at-sea fleet from a cyber security perspective?

"We have a separation between office IT and fleet IT and these are managed by two dedicated teams. Working on fleet IT brings unique challenges. At any given time, our vessels are spread throughout the world. We treat each vessel as a remote office. In line with the introduction of the IMO 2021 guidance, we have undertaken a large-scale roll out of IoT and built a platform to liberate sensor data and combine it with vessel reporting data. We have operated this collaborative platform across our entire fleet for some time now and this has made us consider IT and OT across our business. We have invested heavily in enforcement equipment and security architecture with a comprehensive unified threat management suite as well as a central management tool for the fleet so that we can proactively monitor, update, and maintain our software and systems onboard."

What changes or adaptations has your business had to make to prepare for more connectivity and digital infrastructure across the fleet?

"A key shift in attitudes for us has been to bring the issue of cyber security out of the confines of the IT department, bringing our safety management team to work with us on the operational technology side. We bring cyber expertise, but it's very important for us to cooperate closely with those teams with expertise on the nautical and ship technical side. By having these experts working together, we can make much more informed decisions and it allows us to better assess risks holistically. I believe that effective cyber risk management does not come just from the software itself, but from combining in-house competencies from IT, with those of the safety department, the captains and the seafarers. They are very experienced in setting up procedures and compliance and flag regulations and whatever comes with it.

IT can provide their own technical expertise and their own view and together, a robust solution can be found. I think that's the only way forward; to combine those teams to sit down together with it in the safety departments or operations for whatever department plays a role in this. I don't think this is the case for every operator, but for us, IT has moved really close to the wider business in recent years. We're not just implementing systems. We are driving and managing change. What's going to be installed, how will it be installed, and crucially: how it can be secured and maintained. That's the biggest difference that I've seen more recently."

Some evidence suggests that the maritime sector is behind some of its peers when it comes to the maturity of cyber risk management. Why do you think this is?

"One of the main challenges in shipping is the sharing of threat activity and best practice. This is not a given, especially on a company to company level. We share some knowledge through, for example, AMMITEC - the Association of Maritime Managers in Information Technology and Communications. But

generally, I think many shipping companies are protective of their knowledge and of the issues they are having. That's what I see and I think it's understandable because shipping has long been quite a closed off and segregated industry. As we get younger generations coming up and new ideas filtering in, this is likely to change I would say, but this is a slow process."

"We, and many of our competitors, pursue cyber security insurance. I am seeing that, each year, to renew your contract, the requirements are getting harder and harder to fulfil."

What's now and next for cyber risk management in the tanker industry?

"High speed, high bandwidth connectivity will enable us to do so much more with OT, and this is a persistent challenge in my view. While the node is disconnected, it is safe from remote attack, but its operating system is also not being updated and deteriorating from a cyber security perspective. When the system is connected to the network for whatever reason, to administer support, or diagnose a fault, that system is particularly vulnerable. There are of course ways of managing this with manual updates and other things, but on ships this has its own challenges, getting the right skills and equipment administered to the physical hardware at the right time. Standalone machines that are disconnected from the network on ships can also act as incubators for malware. For example, a disconnected computer might be used solely for printing. Multiple users might be inserting USB sticks into the machine over a period of time and that machine may be infecting multiple USB sticks. Even though the machine is disconnected, it's still a failure of cyber security on the ship."

What about cyber insurance? What has been your experience getting sufficient cover for cyber risks?

"We, and many of our competitors, pursue cyber security insurance. I am seeing that, each year, to renew your contract, the requirements are getting harder and harder to fulfil. I believe that insurance companies understand the difficulties involved in being secure and they fundamentally don't want to cover the risks. They make it really difficult to get. It's not just about patch management, processes and reporting requirements, but it's about privileged access management and many other things. A security operations centre may be required and things like that."

What advice would you like to offer your industry peers?

"I think one of the big investments that maritime companies should make is in the human element. You can have as many systems as you want, but if your human element is weak and not trained highly enough, you will lose. There will be a phishing attempt that you cannot prevent, unless you have trained your people to be vigilant, know what to expect and be able to think about and verify everything. A company can have a big budget, sophisticated systems and antivirus software, but if you have a user that picks up the phishing call or opens the email and carries out the requested actions, there could be very little to prevent a successful attack."

One major issue remains - attracting cyber talent into shipping is like searching for unicorns.

FINDING UNICORNS - THE NEED FOR COMBINED MARITIME AND CYBER SKILLS

A lack of talent or human failure will be responsible for over 50% of all significant cyber incidents by 2025, according to Gartner.[23] The shipping industry needs a major refocus on people to minimise the chance of this predicted statistic becoming a reality. One major issue remains - attracting cyber talent into shipping is like searching for unicorns. There are several reasons for this:

1. Cyber practitioners are expensive and the cyber security job market is booming with an unemployment rate of less than 1%. This means that in reality, shipping would have to pay top dollar to secure these professionals. This isn't something we are likely to see anytime soon.

2. Maritime cyber security presents different challenges to managing enterprise IT cyber risk. One example is practitioners often have to deal with legacy and "mandrolic" systems onboard vessels. In addition, putting in place restrictive cyber security controls, such as strict login procedures, does not work practically, as shipping operations often require the pragmatic flexibility to complete tasks. This may be off-putting to cyber practitioners today.

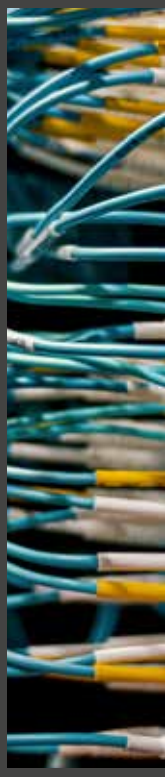
3. As it stands, cyber security isn't typically a separate role within shipping. It tends to be part of IT and often requires travel to vessels in remote and often extreme locations. Cyber security professionals are used to working remotely but do not necessarily have the desire to travel the globe. This makes the role unappealing.

23 Gopal, D et al. (25 January 2023) Predicts 2023: Cyber Security Industry Focuses on the Human Deal. Gartner. Retrieved from https://www.gartner.com/doc/reprints?id=1-2D7XIUC3&ct=230413&st=sb

Reviewing cyber incidents of vessel systems that have occurred so far in 2023, analysis by the CyberOwl team concludes:

"A typical fleet of 30 cargo vessels experiences an average of 7 cyber incidents a month, or over 80 incidents a year. Whilst the majority of these incidents are low impact, the larger issue is the time it takes to resolve them. The average cyber incident on a vessel system took 57 days to resolve. It is worth noting that IBM's research shows this is slightly higher than the general average of 54 days.[24] This is primarily due to the level of coordination required between the experts onshore with the non-cyber-technical crew aboard. The situation is made worse in scenarios where there is a lack of visibility to investigate the root causes and activate responses remotely. Unresolved incidents are at risk of escalating and generally lead to increasing losses."

UNIQUE CHARACTERISTICS OF MARITIME CYBER SECURITY OPERATIONS



In developing a maritime cyber risk management system, much can be borrowed from the lessons learnt protecting general enterprise systems. However, several technical and operational aspects of vessel systems and operations make maritime cyber security operations... a little different. An effective and cost-efficient vessel security operations capability should consider these differences.

The nature of the risks are... a little different

There are limitations that plague remote operational systems onboard vessels. Many of these systems are designed to operate over long lifespans, with limited to no updating. The typical approaches of robust vulnerability management and regular patching will not apply on many of these systems. It is common to find obsolete operating systems with widely known vulnerabilities. There is often very little that the ship owner can do to replace this. They are forced to live with the risk and design other mitigating controls.

It is increasingly common for original equipment manufacturers (OEMs) of vessel systems to be given remote access to vessel systems with the shipping operator having very little knowledge of what is being done to those

24 IBM (2023) Cost of a Data Breach Report 2023 Retrieved from https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf

A relationship exists between the port of call and the cyber risk of the vessel systems.

systems. The majority of use cases relate to OEMs requiring data collection or remote diagnostics. However, this creates a disconnect between the ship owner, who has ultimate responsibility for cyber risk management of the vessel systems, and the OEM who can impact those systems.

A relationship exists between the port of call and the cyber risk of the vessel systems. This is driven by the fact that a significant proportion of cyber incidents still link back to the human behaviour of visitors to the vessel and crew during port visits.

The options for controlling these risks are... a little different

The ISPS Code dictates that the Master has the overriding authority and responsibility to make decisions with respect to the safety and security of the ship. This means that typical approaches provide more local administrative privileges of onboard vessel systems. Where it is no longer acceptable for users to use unapproved USB drives, reconfigure machines and networks and download unapproved software on enterprise IT, that flexibility is still required for vessel systems. This enables the crew and visitors to the vessel to prioritise completing vessel operations and tasks within short time windows, above all else. Frequently, this means completing operations trumps security.

Moreover, implementing strong password protection or login procedures is difficult. Vessel ownership, charterers and crews change frequently and sometimes at very short notice. This makes the practicalities of identity and access management very challenging to achieve for fleet operators pursuing best practice.

OVER 75%
of incidents require response actions that involve the crew.

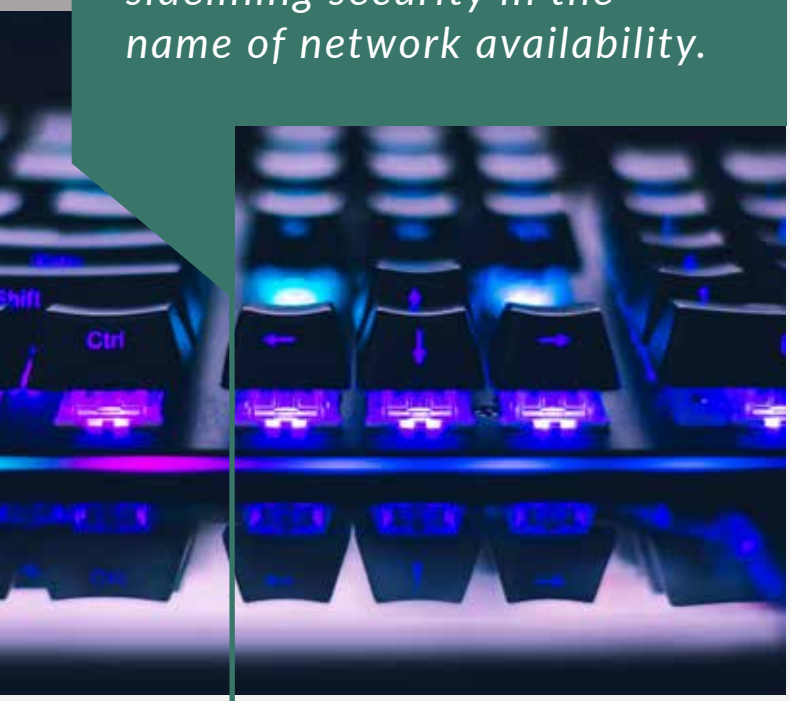
The way you handle cyber incident response is... a little different

CyberOwl's analysis of cyber incidents in 2023 so far demonstrates that over 75% of incidents require response actions that involve the crew. This could relate to a number of actions, including supporting incident investigation, execution of the responding steps or confirmation that the response has been effective. It is common for shipping cyber practitioners ashore to have to require the crew to send photos or videos of what they see on screen via mobile phones, as they take steps to contain a cyber incident. This means that the typical workflows and playbooks of enterprise security operations' teams are unlikely to be completely effective and will need to consider ship-to-shore interactions.

So, what is the answer? As hiring for dedicated roles is very difficult to do, our research leads us to believe that shipping needs to develop cyber responsibilities and decentralise ownership across the organisation. By blending maritime and cyber knowledge and skills, the industry is more likely to secure what it's looking for.

Our 2023 survey indicates that shipping professionals already recognise the need for greater breadth and depth of resources in cyber risk management. 62% of respondents said they feel that most typical cyber incidents on vessel systems require the involvement of other teams and cannot be handled by the IT team alone.

Keeping network and security operations as distinct peers with separate people, tools, and funding will help avoid sidelining security in the name of network availability.



TO BUNDLE OR TO DISAGGREGATE?

It is not uncommon for businesses, especially where money and resources are squeezed, to bundle cyber security functions, or even a Security Operations Centre (SOC) with IT operations, or an existing Network Operations Centre (NOC). To many leadership teams these functions are the same, or so closely allied that it makes sense to consolidate them.

Our 2023 survey results corroborate the pervasiveness of this approach. Based on specific cyber activities people are working on, this is what we found:

- More than 68% of respondents said their organisation's company or vessel IT team handles the cyber security for shipboard systems and fleet operations.
- 83% said their organisation's IT team would be the ones involved in the response and recovery of a cyber security incident on vessel systems.

But according to analysts from Mitre Corporation, while these two functions should be seen as equally important, understanding their differences is vital to a properly functioning cyber security operation. In a 2022 report,[25] Mitre analysts described how combining the two functions can lead to unintended consequences. They point out that, "While both organisations manage risk and incidents, the focus of a NOC is typically on availability and service level agreements, while the focus of the SOC is on data protection and cyberspace defence. Keeping network and security operations as distinct peers with separate people, tools, and funding will help avoid sidelining security in the name of network availability." The two roles are conflicted. The key performance indicators for a network operations director will be at odds with those of a director of cyber security.

25 Mitre Corporation (2022) 11 Strategies of a world-class cyber security operations centre. Retrieved from https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

FLEET TECHNICAL AND SAFETY MANAGEMENT TEAMS

Where dedicated cyber risk management functions are a relatively recent addition in many shipping companies, shore-based fleet managers are a long-established feature of modern ship operating. Many bring considerable experience as seafaring chief mates, captains, and chief engineers and they play a pivotal role in supporting officers with the safe management and operation of the fleet.

Executing actions on shipboard equipment without consultation with the crew could compromise the safety of the ship and those onboard. It is paramount that crew have ultimate primacy on decisions for safe navigation and operation of the vessel.

THE CHALLENGE OF EMPOWERING SELF-SUFFICIENCY

In the event of a cyber attack aboard a vessel, shore-based fleet management is likely to be a vital interface between seagoing staff and the response effort. Threats to OT and its associated equipment require particularly careful handling to ensure that response actions don't create their own problems. Executing actions on shipboard equipment without consultation with the crew could compromise the safety of the ship and those onboard. It is paramount that crew have ultimate primacy on decisions for safe navigation and operation of the vessel.

During normal operations, no unauthorised person would be expected to have decision making powers over equipment for which they are not qualified. Imagine for a moment that a ballast management computer is compromised. Before the hardware can be isolated and recovery actions carried out by a qualified IT technician, the state of the ship, its location, traffic, time of day, visibility and weather conditions, sea state, cargo condition, draft, and present manoeuvres must be fully considered. It could be imperative to shut the system down immediately, but it could be safer to allow the current ballasting operation to be completed first, or the vessel moved to a safer location or put to anchor.

As Mark Sutcliffe, Director of the Maritime Safety and Security Alliance (MSS Alliance) remarked, "Cyber risk management at sea is uniquely challenging. Often the ship is in a remote location, schedules are tight, there are opportunities for security standards to drop just to 'make do'." He adds, "If you've got cyber security personnel, they've got to understand how the fleet works or work in lock-step with people that do. It's so easy to make good cyber security decisions which are at odds with operational requirements. From a ship safety point of view, both things are important."

Scott Dickerson, Executive Director of the MTS-ISAC, agrees; pointing out that the expectation of a sophisticated response from seafarers to a cyber incident at sea is akin to conflating the role of a hospital surgeon with that of a cyber security expert: "Mariners spend many years rising to senior positions, acquiring specialist skills and knowledge. They cannot then be expected to acquire expert skills in cyber security. Imagine a chief surgeon at a hospital. While you would expect them to be highly proficient in surgical procedures, few would expect them to have specialist cyber security knowledge about the EKG machine. There's no expectation that the surgeon has verified that the machine is cyber secure prior to operating on a patient. Cyber security is a specialist field and beyond the remit of specialists in other fields to manage effectively."

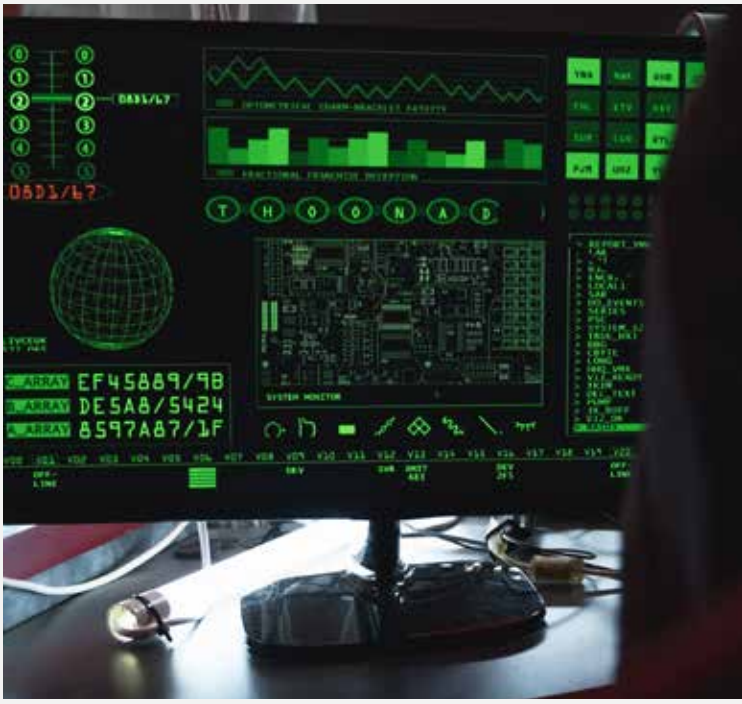
FACILITATING THE RIGHT RELATIONSHIPS WITH OEMS

Between 70% and 80% of the final output value of ship production is generated by the upstream supply chain, otherwise known as original equipment manufacturers (OEMs).[26]

Today ships are being continuously upgraded with digital technologies to improve their performance and augment value. This presents both an opportunity and a challenge when it comes to cyber security management as the relationships with OEMs tend to sit with technical and/or safety teams, and not IT departments.

OEMs play such an important role and are held to account by technical teams. But it's complex. Like a Swiss cheese model, ship technology has layer upon layer upon layer of attack surfaces. An engine management computer will be supplied alongside a propulsion system by the engine manufacturer, but the computer itself will use peripherals manufactured by one supplier, a chipset from another, printed circuit boards from another, power supplies from another and so on. If it's placed on a network, many pieces of componentry form part of the attack surface and may also provide a threat vector for infiltrating the most prized parts of the network.

Getting the balance right is tricky. Technical teams are pursuing performance and security requirements could slow things down. In addition, retrofitting security is very expensive. Now is the time to ensure enduring security controls and processes, so the total cost of maintaining the system is minimised over the lifespan.



This concept of trade partner risk is significant. As supply chains become further interlinked through digital technology, the chance that shipping companies become an infection pathway which causes harm to their customers and trade partners as a result of poor cyber risk management is increasing rapidly.

Supply chain cyber risk should be considered alongside protecting a company's own network. As Wärtsilä Managing Counsel, Tom Barr, explains, "For OEMs and the wider maritime sector, cyber resilience needs to be embedded throughout the supply chain. It's not just about making sure that our own house is in order, it is making sure that these standards are maintained up and down the supply chain."

Cost is one reason for considering supply chain risk carefully. Recent research from computer technology giant IBM shows that business partner supply chain compromises cost 11.8% more, and take 12.8% longer to identify and contain, than other types of breach.[27]

26 OECD. (2019a). Global value chains and the shipbuilding industry, OECD Science, Technology and Industry Working Papers. https://dx.doi.org/10.1787/7e94709a-en

27 IBM (2023) Cost of a Data Breach Report 2023. Retrieved from https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf

Increasingly, threats are trying to maintain a breach surreptitiously. These are designed to go unnoticed. It seems like nothing's happened, therefore nothing's wrong. But it could very well be the case that something is wrong, it's just not revealing itself.

As many companies are asking their suppliers and customers to interact with them in digital cloud environments, there is a heightened risk that infections and malicious software will be distributed up and down supply chains via these types of platforms. One expert told Thetius, "When a cyber threat manifests it can cause harm very quickly. Malware can propagate across networks, hopping from machine to machine. Many threats are readily identifiable because there's an immediate impact to the organisation. But increasingly, threats are trying to maintain a breach surreptitiously. These are designed to go unnoticed. It seems like nothing's happened, therefore nothing's wrong. But it could very well be the case that something is wrong, it's just not revealing itself. Instead it's using your network as a springboard to attack your service providers, charterers, or cargo owners".

Another reason concerns the legal responsibility that shipping companies have to their supply chain and trade partners. Since 1 January 2021, cyber security has been part of the requirements of the International Safety Management System (ISM) Code. Supported by the IMO Resolution MSC.428(98), ship owners and managers are required to assess cyber risk and implement relevant measures. The adaptation of new technology in the supply chain inevitably means that the owners of vessels are under a heavier burden and must become even more diligent with their checks. A ship owner who is found not to have carried out and discharged his obligations in relation to his shipboard cyber arrangements is likely to render his vessel unseaworthy.

Under English Law, the obligation to provide a seaworthy vessel arises multiple times and is set out in several situations – by statute giving rise to criminal and civil liability, by contract and at common law. Under the Merchant Shipping Act 1995 (section 42), it is a criminal offence to send or attempt to send an unseaworthy ship to sea. The Marine insurance Act 1906 implies a warranty that the vessel is "reasonably seaworthy in all respects". Breach of this warranty will result in the insurer not being liable for any loss attributable to unseaworthiness. With regard to the carriage of goods by sea, where the vessel is found to be unseaworthy, the owners could be held to be in breach of their obligations at common law or statute for their failure to provide a seaworthy vessel. The common law position is that a seaworthiness obligation should be implied into every contract of carriage. In the majority of charterparties, this implied undertaking is reinforced by an express term to the same effect, indicating that the chartered vessel is to be "tight, staunch, and strong and in every way fitted for the voyage" or words to a similar effect. The test of seaworthiness that is often used as a benchmark is found in McFadden v Blue Star Line [1905] 1 K.B. 697. This asks:

"If the defect existed, the question to be put is, would a prudent owner have required that it should be made good before sending his ship to sea had he known of it? If he would, the ship was not seaworthy within the meaning of the undertaking".

Furthermore, the obligation to make the vessel seaworthy is "non-delegable" such that if, for example, the unseaworthiness is caused by the Owner or OEM's failure to patch a software system, it is likely that the owners will be held liable for the negligence of the assistant technician or a contractor or the 3rd engineer who oversaw the work even if the shore side systems are perfect and the chief and 2nd engineers are paragons of virtue.

A finding of unseaworthiness could therefore result in a range of repercussions ranging from a fine to a breach of the insurance obligations resulting in the owners vessel being denied cover not being insured and/or cargo claims being brought against the owners by the charterers and/or cargo interests.

A finding of unseaworthiness could therefore result in a range of repercussions ranging from a fine to a breach of the insurance obligations resulting in the owners vessel being denied cover not being insured and/or cargo claims being brought against the owners by the charterers and/or cargo interests. At its worst, an owner may be unable to limit their liability under the Convention on Limitation of Liability for Maritime Claims 1976 (the LLMC Convention 1976). Under Article 4 of the LLMC, if an act or omission by a person seeking to limit their liability was "... committed with the intent to cause such loss or recklessly and with the knowledge that such loss would probably result" it is open to the insurers to argue that the owners have waived their rights to limit their liability - see The Atlantik Confidence [2016] EWHC 2412 (Admlty).[28]

The purpose of the ISM code is to provide an international standard for the safe management and operation of ships and for pollution prevention. Cyber security must be properly documented within a vessels' safety management system which will include carrying a valid Document of Compliance on board. Lack of documentation in itself does not render a vessel unseaworthy, especially where the documents are in the nature of certificates or similar (see The Derby [1985] 2 Lloyd's Rep. 325). However, the requirements of best management practice and the ISM code require there to be detailed written systems and procedures in place for management and navigation of a vessel, including shipboard operations and response to emergencies. In the absence of such procedures, this may go to both issues of unseaworthiness and due diligence. Regardless of competence of the crew (and incompetence in terms of lack of training or familiarity may overlap with other unseaworthiness in terms of lack of documentation) a vessel without a proper "instruction manual" is unseaworthy.

28 HFW (Oct, 2016) Atlantik Confidence - Cargo Insurers "Break Limits" in Unprecedented Judgement. Retrieved from https://www.hfw.com/ATLANTIK-CONFIDENCE-unprecedented-judgment-october-2016

Where the unseaworthiness is due to incompetence of mariners (existing at the beginning of the voyage) the due diligence is usually that of shore side personnel including owners, managers, recruitment agents and the like responsible for recruitment and training of officers and crew.

In the event that a cyber attack were to cause a vessel to ground or collide with another ship, the burden of proof is on the claimant to show that the vessel was unseaworthy and that the unseaworthiness caused the incident. If that burden is discharged, the burden passes to owners to prove that they and those for whom they are responsible exercised due diligence to make the ship seaworthy in the relevant respects and that the incident occurred despite the exercise of due diligence.

One of the ways in which the owners or managers can evidence that due diligence had been exercised would be to show that correct company procedures in advising the master and officers on the best practice for ensuring that the vessel was cyber resilient were in place and had been followed. In other words, owners need to show that they complied with the ISM code, and provided the vessel with a sufficient Safety Management System (SMS), and that an adequate "paper trail" of the same could be shown. Regulation 12 of the ISM code requires ship owners to carry out internal safety audits and to periodically evaluate the effectiveness of the SMS. How an owner chooses how to do this is up to them but in an unreported decision, the tribunal made it clear that an owner who pays "lip service" to the ISM code and turns a blind eye to "box ticking" on board his vessel, no matter how unwittingly, is likely to have an adverse decision made against him in relation to his vessels seaworthiness.

Where the unseaworthiness is due to incompetence of mariners (existing at the beginning of the voyage) the due diligence is usually that of shore side personnel including owners, managers, recruitment agents and the like responsible for recruitment and training of officers and crew.

Monitoring and management of mariners is very much part of the job of the master and senior officers, and even if competent themselves they may be negligent (in due diligence terms) in failing:

1. To spot incompetence, negligent or poor practices of others, and/or
2. To ensure compliance with correct systems and procedures.

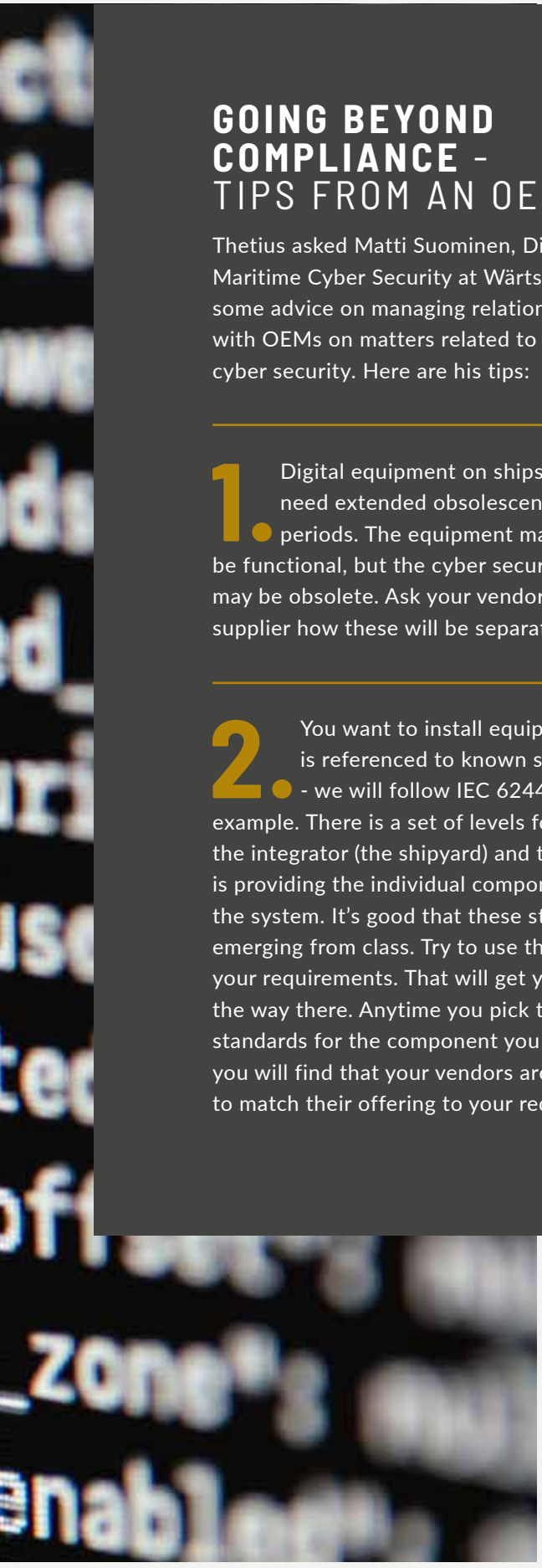
Such failing will only be relevant if it is a habitual or systemic one which can be said to exist at the beginning of the voyage. Evidence of failing (or especially multiple failings) on a particular voyage in question may be evidence of a systemic problem. It is for this reason that it is now a necessary requirement for an owner seeking to prove due diligence to be able to demonstrate that all the written procedures and systems are adequate and that the shore side personnel were diligent.

Installing systems in order to prevent cyber-attacks and developing risk avoidance strategies will go some way to defending unseaworthiness claims in the future. The law requires owners to take full responsibility for the effectiveness, safety and security of their vessels and vessel systems. In doing so, there is a good argument that this could be extended to assuming responsibility for vulnerabilities in the supply chain.

Whilst the Master and crew bear a significant responsibility for the seaworthiness of the ship, with the shift in technology it is probably the fleet technical managers and the safety teams who are best placed to facilitate the right relationships with OEMs as part of their day to day activities interacting, collaborating and setting standards to ensure that the safety standards prescribed in the on board SMS are maintained.

Thetius interviewed Wärtsilä to help understand what a good relationship could look like between technical teams and OEMs.

Installing systems in order to prevent cyber-attacks and developing risk avoidance strategies will go some way to defending unseaworthiness claims in the future.



GOING BEYOND COMPLIANCE - TIPS FROM AN OEM

Thetius asked Matti Suominen, Director of Maritime Cyber Security at Wärtsilä, for some advice on managing relationships with OEMs on matters related to cyber security. Here are his tips:

1. Digital equipment on ships will need extended obsolescence periods. The equipment may be functional, but the cyber security may be obsolete. Ask your vendor or supplier how these will be separated.

2. You want to install equipment which is referenced to known standards - we will follow IEC 62443, for example. There is a set of levels for the user, the integrator (the shipyard) and the OEM who is providing the individual component parts for the system. It's good that these standards are emerging from class. Try to use them and align your requirements. That will get you most of the way there. Anytime you pick the common standards for the component you are buying, you will find that your vendors are better able to match their offering to your requirements.

3. Consider your expectations for the way you expect the cyber risk to be split. The majority of ship owners and operators want highly secure equipment to a high standard of cyber notation in place. But some don't realise that their vessel needs to bring a number of things to bear first to support these standards. It may need the right power and monitoring capability at the site of installation for example.

4. OEMs can integrate with other solutions, but are not selling an ongoing cyber security service. For example, an engine can contribute data, but it cannot become a cyber risk monitoring system for the whole ship. Be aware of what you need to deliver to achieve your goals.

5. It is important to acknowledge that an effective cyber security strategy comes from both one-off actions and continuous maintenance of security. An OEM should deliver the one-off actions, but who takes responsibility for ongoing security should be agreed clearly between the ship owner and OEM.

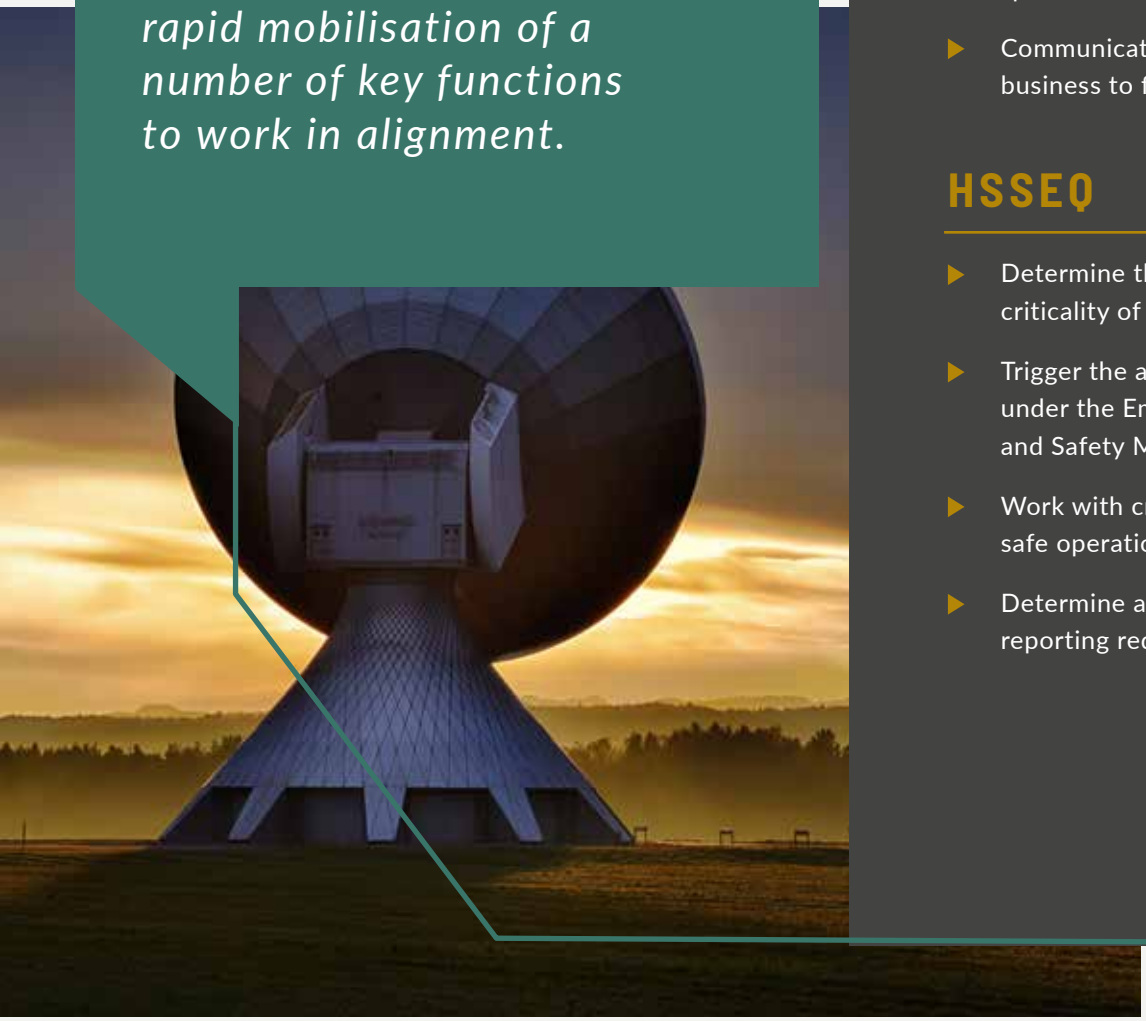
The majority of ship owners and operators want highly secure equipment to a high standard of cyber notation in place.

THE NEED FOR CROSS-FUNCTIONAL COHESION

TYPICAL SHORE-BASED FUNCTIONS THAT ARE INVOLVED IN A MAJOR MARITIME CYBER INCIDENT

A major cyber incident has far reaching implications. Surviving such a cyber emergency crisis requires rapid mobilisation of a number of key functions to work in alignment. Preparation through regular exercises strengthens an organisation's ability to respond effectively during a crisis.

A major cyber incident has far reaching implications. Surviving such a cyber emergency crisis requires rapid mobilisation of a number of key functions to work in alignment.



FUNCTIONS AND THEIR TYPICAL ACTIONS

IT

- Lead technical actions and communication.
- Validate that the cyber incident is real (not always obvious!).
- Contain the problem, investigate the spread of the incident to other systems and minimise the impact.
- Determine whether it is a single vessel incident or a breach that has spread across multiple vessels.
- Communicate effectively to the business to facilitate decision-making.

HSSEQ

- Determine the level of safety criticality of the incident.
- Trigger the appropriate procedures under the Emergency Response Manual and Safety Management System.
- Work with crew to confirm safe operations.
- Determine and execute on reporting requirements.

INSURANCE / CLAIMS

- Determine any consequential liabilities as a result of the incident.
- Determine what coverage is in place (e.g., P&I, Defence, Strike & Delay (S&D), War Risks) and any cover limitations.
- Determine whether to notify and consult the insurers, and what level of support insurers can provide.

TECHNICAL MANAGEMENT

- Liaise with HSSEQ to provide technical support and determine the level of safety criticality of the incident.
- Work with OEMs on mitigations, where relevant.

FINANCIAL

- Support decision-making around any ransom demands and related administration.

LEGAL

- Undertake investigation into regulatory compliance and disclosure requirements to regulators (and in which jurisdictions), customers, counterparties, shareholders and others and time frame for doing so and penalties for failure to comply.
- Review contracts and charter party agreements to check the allocation of risk and responsibility and any notice provisions that need to be complied with.
- In the event of a cyber security breach, assess the legal implications of making a ransom payment and whether this may breach any sanctions obligations.
- Identify contracts affected by breach.
- Where there is a loss of personal data, consider whether it is necessary to notify your Data Protection Officer (DPO).

CRISIS COMMUNICATIONS

- Establish leadership, roles and protocols for internal and external communications.
- Assess likely stakeholder impact.
- Develop and align key messages.

FLEET MANAGEMENT / LEADERSHIP TEAM

- Take ultimate ownership of key crisis actions.
- Work with commercial managers to determine whether and how to notify charterers.
- Work with the management team to make decisions around how to respond to any ransom demands.

Blending skills across all departments, not just fleet management and IT, can provide a more effective strategy to cyber risk management. This can be done by implementing cross-functional crisis teams. This approach moves beyond basic compliance and enables cyber threats to be evaluated and mitigated against more effectively.

Max Bobys, Practice Director at Hudson Cyber confirmed to Thetius that this is, "One of the most effective strategies that shipping companies of any size should consider."

A matrix maturity model approach that covers the different functional areas of the business enables each individual in that group to have an area of responsibility that they have to report on, track, and implement against, according to Mr Bobys.

Ultimately, this approach enables the group to secure the attention of the board and access C-Suite guidance. "Depending on the size of the company, we like to see groups from six to 12 people. What you do is take the responsibility out of the IT people and bring it into the group as part of a dialogue across the organisation. It's a very effective way of getting buy-in and consensus," he explained.

Interestingly, many shipping companies already have a cross-functional crisis team process in place for physical crises. It's a standard safety management procedure. Physical security is more intuitive and tangible physical threats can be visualised, unlike cyber threats. In the majority of cases, IT isn't yet considered a critical part of that cross-functional team. This is largely due to the fact that the crisis team hasn't envisaged the need to cover cyber attack scenarios, and in physical incident scenarios, IT is not necessarily critical.

"What is challenging ship owners is that cyber threats represent a risk to their business which often won't present itself in a readily discernible or understandable context," explained Mr Bobys.

CONNECTIVITY -A DOUBLE-EDGED SWORD?

Changes to the Maritime Labour Convention in 2021 placed internet access higher on the list of humanitarian requirements for seafarers, but the labour force itself will to a large extent force crew connectivity to expand at sea. In 2022, Thetius gathered opinions from over 200 seafarers about digital connectivity and the future of the seafaring trade. The results showed that 88% of seafarers believe that digitalisation will result in major new ways of operating vessel fleets within five years. More surprisingly, more than 1 in 3 seafarers chose access to digital technology as the most important factor when considering working for a new employer. These respondents placed a higher priority on connectivity than they did on pay, conditions, or shore leave.[29]

29 Thetius Inmarsat (2022) Seafarers in the Digital Age. Available at https://thetius.com/free-report-seafarers-in-the-digital-age/

"I think there will be a number of operators who are not ready for the challenges that come with high performance connectivity on their ships."

According to its Chief Marketing Officer Ghani Belhoul, Marlink estimates that at the end of 2022 there were upward of 37,000 vessels at sea equipped with very-small-aperture terminal (VSAT) connectivity. Now, with other forms of high performance connectivity rising rapidly such as coastal 5G and Low Earth Orbit (LEO) satellite networks, high capacity data exchange pathways are proliferating rapidly across the merchant sector and maritime transport.[30] Thetius' 2023 survey found that 43% of respondents said their company is planning to roll out LEO satellite communications within the next 12 months.

This level of connectivity makes cloud services at sea a very real possibility. But LEO networks in particular hold the potential to increase the number of backdoor vulnerabilities and expand infiltration opportunities. The 2023 survey showed that 45% of respondents believe LEO will increase cyber risks.

This means that ship owners and operators will need to consider additional budget for security and resources as part of their LEO installation plans. Ignoring the intersection that lies between cyber security and advancing satcoms will open up an organisation to avoidable risks. This will require further investment, additional resources and collaboration to ensure a sufficient cyber protection plan is in place.

We must also not forget the additional training that crew will require with increased connectivity onboard. While the potential exploitation of vulnerabilities of onboard systems is one challenge, another one is the fresh opportunity for online fraud of crew. Seafarers are also the victims of cyber scams and phishing emails are one of the biggest threats they face. Crew will not only require further training to operate new systems, but also in managing the possibility of new threats which if they become caught up in can have severe consequences on their mental health and wellbeing.

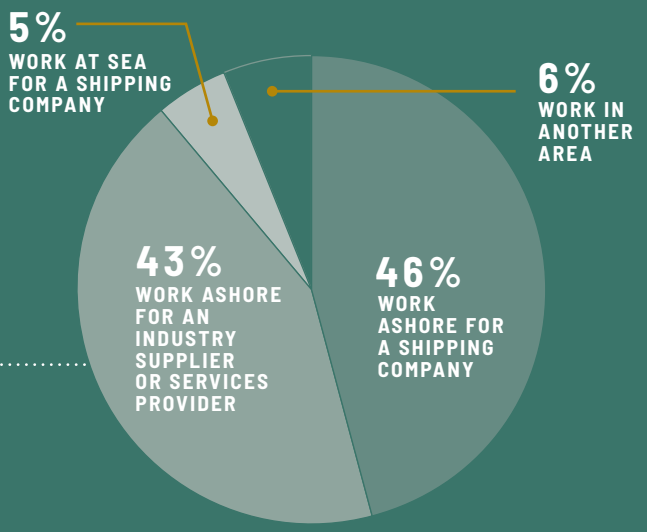
"High speed connectivity at sea is, and will continue to be, a game changer. Personally, I'm looking forward to internet connectivity no longer being a factor at sea, in the same way that high speed connectivity is guaranteed in a modern office ashore. But from a cyber security perspective, there are pros and cons to this. There will be more opportunities for threat actors to gain access and potentially damage could occur much quicker," a fleet IT director from a container shipping operator told Thetius.

When asked about the impact of this on the sector more broadly, he added, "I think there will be a number of operators who are not ready for the challenges that come with high performance connectivity on their ships. I believe we are as prepared as we can be, because we have taken a 'mobile office' approach for a number of years now. While we already have very high speed connectivity on some of our ships, access and user controls remain very strict."

30 From a Thetius interview conducted in June 2023.

Thetius

SURVEY RESULTS



RESPONSE AND MANAGEMENT

71% *believe that their organisation has a cyber emergency response plan that is regularly tested.*

79% *agree that senior leaders in their organisation have a clear understanding of cyber risk management.*

THE MAJORITY

(80%) believe that they understand what actions would be required of them during a cyber security incident.

64% *of respondents said their organisation has cyber risk management procedures in place for dealing with third party organisations such as suppliers.*

63% *said their organisation has cyber risk management procedures in place for dealing with customers or trade partners.*

INVESTMENT

A SIGNIFICANT PROPORTION

of respondents (44%) said they have no idea about how much their organisation invests in cyber security management each year.

33% **< US $100K**

33% spend less than US $100K per year on cyber security management.

3% **> US $10 MILLION**

3% said they invest more than US $10 million.

27% of respondents said that up to...

25% *of spending on cyber security would go towards onboard systems.*

COST OF ATTACKS AND RANSOM PAYMENTS

US$550K

Cyber attacks have cost organisations on average US $550K over the last three years.

US$3.2m

The average cost of a ransom payment is US $3.2m.

INSURANCE

1 in 4 believe that their organisation does not have an insurance plan in place to cover cyber attacks.

37%

said that their insurance policy did not cover the claim they made following a cyber breach.

CHALLENGES IN UNDERSTANDING CYBER RISK AND BENCHMARKING BEST PRACTICE

> ***One of the biggest challenges for stakeholders is that there is no practical way of benchmarking cyber hygiene with comparable organisations.***

41% *of respondents felt that this is currently a major challenge for their organisation.*

33%

felt that one of the biggest challenges in improving cyber risk management is understanding the level of risk.

30%

said that it was difficult to understand best practice.

CONNECTING TRENDS CHARTING PROGRESS SINCE THE GREAT DISCONNECT REPORT

+200%

In fact, we've seen a 200% increase in the cost of cyber attacks to organisations, and a 357% increase in the demand for ransom payments.

COST OF CYBER ATTACKS UP BY 200%, DEMAND FOR RANSOM UP BY 357%. WHAT ELSE HAS CHANGED?

Back in 2022 when Thetius, CyberOwl, and HFW carried out a similar analysis of the maritime cyber security landscape, 36% of respondents believed that their organisation had been the victim of an attack. In the 2023 survey, this figure remained much the same (35%). But what's most interesting to note is that the cost of attacks and demand for ransom payments have skyrocketed.

In fact, we've seen a 200% increase in the cost of cyber attacks to organisations, and a 357% increase in the demand for ransom payments.

Respondents reported that over the last three years, their organisations have spent around US $550K on managing and mitigating cyber attacks. These costs are largely driven by the price of cyber security, IT and other external advisors, business interruptions and delays, and the cost of replacing or restoring systems. Other costs include the payment of ransom, loss of business, and being tricked into transferring funds.

In 2022, respondents noted that cyber security incidents were costing their organisations around US $182K. Just 18 months later and we're seeing a substantial increase in the overall cost of cyber attacks to organisations operating in the maritime sphere.

The 2023 survey shows that the average price paid for ransom has remained persistently high. In 2022, the average price paid was US $3.1m and in 2023 it is US $3.2m. Most importantly is the significant increase in demand for ransom payments. In 2022, only 3% of respondents said they had paid a ransom following a cyber attack, but this year, nearly 14% admitted to doing so. This is a whopping 357% increase in just over a year.

The rise in ransom payments is not limited to the maritime sector. Cyber insurance firm Coalition reported that ransomware claims increased by 27% during the first half of 2023.[31] While in some cases,

31 TechTarget (Sep, 2023) Cyber insurance report shows surge in ransomware claims. Retrieved from https://www.techtarget.com/searchsecurity/news/366552773/Cyber-insurance-report-shows-surge-in-ransomware-claims

Just 18 months later and we're seeing a substantial increase in the overall cost of cyber attacks to organisations operating in the maritime sphere.

increased ransomware activity can be tied to Russia's invasion of Ukraine, ultimately ransomware operations are scalable and easy money makers for cyber criminals. The increase in ransom payments is not a surprise, but managing risk is an issue that needs addressing now.

In 2022, Thetius reported that 24% of industry professionals thought that their organisation did not have an insurance policy in place for cyber attacks, while 42% didn't know. Ship operators were found to be unnecessarily exposing themselves to cyber risks by not understanding their insurance policies and its limitations. It seems that 18 months on, little has changed.

A large majority of this year's respondents (42%) said that they are unclear about what is covered by their organisation's cyber risk policy, while 25% of respondents thought their organisation did not have a cyber risk insurance policy in place.

Moreover, 37% said that their insurance policy did not cover the claim they made following a cyber attack. A further 18% declined to comment or didn't know, indicating that even where an insurance policy is in place, securing a payout is not always possible.

As we've explored in this report, understanding and securing insurance for cyber crime is far from simple. Cover applications are rejected because the cyber security management system in place doesn't meet certain requirements.

37%

said that their insurance policy did not cover the claim they made following a cyber attack.

Alternatively, cyber insurance policies exclude so many areas that in the event of an attack and subsequent claim, no compensation is possible. Our 2023 research shows that little has changed when it comes to understanding insurance around cyber security and there is work to be done here.

In terms of preparation and response, this has remained largely the same since the previous survey. In 2022, 73% of respondents said they believed that their organisation had a cyber emergency response plan that was regularly tested. In 2023, this figure remained relatively similar with 71% believing their organisation has a response plan that is regularly tested.

Despite these rising figures, there is also evidence of progression. In 2022, we found that 54% of shipping companies admitted to spending less than US $100K on cyber security management, whereas in 2023 only 33% of shipping companies said they spend less than US $100K. This indicates that there is an increase in the number of organisations digging deeper into their wallets to combat cyber threats.

SUMMARY AND RECOMMENDATIONS

While the shipping industry is maturing and digitalisation is increasing, so too is the level of threat. This latest research conducted by Thetius, CyberOwl, and HFW suggests that the cost of cyber attacks is on the rise and the demand for ransom payments is skyrocketing - it's up 357% since a similar survey was conducted in 2022.

In 2021 and early 2022, Thetius explored the status of the maritime threat landscape and identified a huge disconnect between the perceived and actual readiness to respond to an attack. There is perhaps a heightened awareness around cyber security today, with 80% of survey respondents believing that they understand what actions would be required of them during a cyber security incident. Companies are also ploughing more capital into cyber protection tools. In 2022, 54% of shipping companies spent less than US $100K on cyber security management. The 2023 survey revealed that now only 33% spend less than that. Larger players are moving at a faster pace as they are exposed to vulnerabilities and it has dawned upon them the potential for catastrophe if they are the successful target of a cyber criminal.

But 18 months later, the deployment of advanced digital technologies and higher levels of connectivity thanks to the addition of LEO satellites are catalysing the emergence of new threats. Vulnerabilities are infiltrating different levels of the organisational structure, bringing new demands and requiring some difficult decisions to be made. Risk management teams, IT and cyber management teams, and fleet technical and safety management teams must consider, understand, and manage cyber security threats in a very specific way. In order to do so, maritime professionals require upskilling. Blending skills across all departments, which can be achieved with a cross-functional crisis team, can be useful in evaluating and mitigating cyber threats more effectively. However, in the majority of cases, IT isn't yet considered a critical part of the cross-functional team.

42% of respondents said that they are unclear about what is covered by their organisation's cyber risk policy

Making it further difficult to navigate the maritime cyber security environment, is the uncertainty around cyber insurance. 42% of respondents said that they are unclear about what is covered by their organisation's cyber risk policy, while 25% thought their organisation did not have a cyber risk insurance policy in place. Cover applications are rejected because the cyber security management system in place doesn't meet certain criteria. This is a major concern that needs to be addressed but will require collaboration and communication across the industry.

RECOMMENDATIONS:

1. Understanding how responsibilities are evolving for key roles is critical. These roles are changing as a result of increased connectivity, digitalisation and the consequential cyber risks, and there are increasing pressures and demands on people. Not only do people require the skills to operate advanced and complex technologies, but they also need the right cyber security knowledge to reduce the risk of opening up systems to vulnerabilities. Blending skills across all departments is helpful and this can be done via cross-functional teams.

Understanding how responsibilities are evolving for key roles is critical.

2. Make deliberate and holistic decisions on investments in cyber risk management. This requires a coherent security programme, led by an authority that understands the risks. Making decisions on point-based solutions may result in high costs, but low effectiveness. There are longer term consequences to decisions. Developing capabilities in-house vs leveraging the expertise and scale of outsourced providers needs to be considered carefully. So does the choice of bundling vs disaggregating cyber security from other functions.

Make deliberate and holistic decisions on investments in cyber risk management.

3. When assessing the installation of advanced satellite communications systems such as LEO, additional cyber risks must be considered in the budget. 43% of respondents said that their organisation is planning to roll out LEO within the next 12 months and nearly half agreed that it would increase cyber risks. Greater cyber protection will be required but this will come at an additional financial cost.

When assessing the installation of advanced satellite communications systems such as LEO, additional cyber risks must be considered in the budget.

4. Secure the right relationships with OEMs. Ships are being continuously upgraded with digital technologies and OEMs are held to account by technical teams. But it's complex and it's important to acknowledge that an effective cyber security strategy comes from both one-off actions and continuous maintenance of security. OEMs also need to develop software to standards which are understood by industry to avoid unnecessary confusion.

Secure the right relationships with OEMs.

5. Insurance needs to be right. While having it in the first place is a start, not having a clear understanding of how and what protection it actually provides is a major but all too common issue seen today.

Insurance needs to be right.

6. Check your contracts. Assigning risk and responsibility pre-incident in a contract is one of the better ways to mitigate any exposure the parties may have following a cyber security breach. If the contract is silent and no provision is made for cyber security, consider if it is necessary to incorporate an appropriately drafted cyber security clause.

Check your contracts. Assigning risk and responsibility pre-incident in a contract is one of the better ways to mitigate any exposure the parties may have following a cyber security breach.

> *"Blending skills across all departments, which can be achieved with a cross-functional crisis team, can be useful in evaluating and mitigating cyber threats more effectively."*

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 Dan Ng and Sara Fortes for contributing so much expertise and so many ideas to this project.

To all of the team at HFW including Tom Walters, Henry Clark, and 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. 12 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 146 responses. 45% of responses were from members of staff at shipping companies, 44% of responses were from members of staff at industry suppliers or service providers, 5% were from seafarers, and 6% of responses were from other areas.

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

A - H

A

Allianz Global (2022) Cyber: The changing threat landscape. Retrieved from https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/agcs-cyber-risk-trends-2022.pdf

Akpan, F.; Bendiab, G.; Shiaeles, S.; Karamperidis, S.; Michaloliakos, M. Cyber security Challenges in the Maritime Sector. Network 2022, 2, 123-138. https://doi.org/10.3390/network2010009

Atlantic Council (4th October 2021). Introduction: Cooperation on maritime cyber security. Retrieved from https://www.atlanticcouncil.org/in-depth-research-reports/report/cooperation-on-maritime-cybersecurity-introduction/

B

Beckstrom, Rod, U.S. Department of Homeland Security (2009) The Economics of Networks and Cyber Security. (p.7) Retrieved from https://www.researchgate.net/publication/259254523_Economics_Of_Networks_-_Rod_Beckstrom_National_Cybersecurity_Cente

D

Digital Ship. Getting Shipboard Cyber security Right. 2021. Available at https://www.youtube.com/watch?v=4e6UQBdv6wU

DNV (2023) Maritime Cyber Priority 2023. Retrieved from https://www.dnv.com/cybersecurity/cyber-insights/maritime-cyber-priority-2023.html?gad=1&gclid=Cj0KCQj woeem BhCfARIsADR2QCvUogGkYheJKTF_T9TyNV93e672NJnu5B5F6eE4y4yhnf-ztwN75zoaAl33EALw_wcB

E

Esentire, Cyber security Ventures (2022) Official Cybercrime Report. Retrieved from https://s3.ca-central-1.amazonaws.com/esentire-dot-com-assets/assets/resourcefiles/2022-Official-Cybercrime-Report.pdf

F

Forbes (Nov, 2018) Protecting Your Reputation From Cyberattacks Isn't Impossible If You Do These 3 Things. retrieved from https://www.forbes.com/sites/ryanerskine/2018/11/28/protecting-your-reputation-from-cyberattacks-isnt-impossible-if-you-do-these-3-things/?sh=3c5234624a66

G

Gopal, D et al. (25 January 2023) Predicts 2023: Cyber security Industry Focuses on the Human Deal. Gartner. Retrieved from https://www.gartner.com/doc/reprints?id=1-2D7XIUC3&ct=230413&st=sb

Gov.uk (19 April 2023) Official Statistics: Cyber security breaches survey 2023. Retrieved from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023

H

HFW (Oct, 2016) Atlantik Confidence - Cargo Insurers "Break Limits" in Unprecedented Judgement. Retrieved from https://www.hfw.com/ATLANTIK-CONFIDENCE-unprecedented-judgment-october-2016

I

IBM (2023) Cost of a Data Breach Report 2023 on the Mean Time To Contain (MTTC) breaches on on-premises systems, relevant for most vessel systems and applications – figure 36 or page 45. Retrieved from https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf

IBM (2023) Cost of a Data Breach Report 2023. Retrieved from https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf

Inmarsat, Thetius (2021) A Changed World. Retrieved from https://thetius.com/changed-world/

International Association of Insurance Supervisors (April 2023) Global Insurance Market Report (GIMAR) Special Topic Edition for Cyber. Retrieved from https://www.iaisweb.org/uploads/2023/04/GIMAR-2023-special-topic-edition-on-cyber.pdf

REFERENCES

L - Z

L

Law Society, The (21 July 2023) Seven in 10 firms don't have cyber insurance. Retrieved from https://www.lawsociety.org.uk/contact-or-visit-us/press-office/press-releases/seven-in-10-firms-dont-have-cyber-insurance

Leisterer, Hannfried, Dr. Alexander von Humboldt Institut Für Internet und Gesellschaft (February 03, 2014). Law, Cyber security and Critical Information Infrastructure Protection. Retrieved from https://www.hiig.de/en/law-cyber-security-and-critical-information-infrastructure-protection/

M

Maritime London (Mar, 2021) Meeting the cyber threat challenge in the maritime industry – protection beyond regulation. Retrieved from https://www.maritimelondon.com/news/meeting-the-cyber-threat-challenge-in-the-maritime-industry-protection-beyond-regulation

Maritime Executive, The (2021) The IMO 2021 Cyber Guidelines and the Need to Secure Seaports. Retrieved from https://maritime-executive.com/editorials/the-imo-2021-cyber-guidelines-and-the-need-to-secure-seaports

Mitre Corporation (2022) 11 Strategies of a world-class cyber security operations centre. Retrieved from https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

O

OECD. (2019a). Global value chains and the shipbuilding industry, OECD Science, Technology and Industry Working Papers. https://dx.doi.org/10.1787/7e94709a-en

OCIMF Tanker Management and Self-Assessment 3, published April 2017, retrieved from https://www.ocimf.org/es/document-libary/175-tmsa3-faqs/file

P

Palo Alto Networks (Jun, 2021) The True Cost of Cyber security Incidents: The Problem. Retrived from https://www.paloaltonetworks.com/blog/2021/06/the-cost-of-cybersecurity-incidents-the-problem/

S

S&P Global Market Intelligence (20 July 2023) Cyber insurance market poised for growth as hard market eases. Retrieved from https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/cyber-insurance-market-poised-for-growth-as-hard-market-eases-76602312

T

TechTarget (Sep, 2023) Cyber insurance report shows surge in ransomware claims. Retrieved from https://www.techtarget.com/searchsecurity/news/366552773/Cyber-insurance-report-shows-surge-in-ransomware-claims

Thetius, HFW, CyberOwl (2022) Global industry report: the great disconnect. Available at https://cyberowl.io/resources/global-maritime-industry-report-the-great-disconnect/

Thetius Inmarsat (2022) Seafarers in the Digital Age. Available at https://thetius.com/free-report-seafarers-in-the-digital-age/

U

UK Government (April, 2023) Cyber security breaches survey 2023. Retrieved from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023

UK Home Office (January 2018) Understanding the costs of cyber crime. A report of key findings from the Costs of Cyber Crime Working Group. Retrieved from https://www.gov.uk/government/publications/understanding-the-costs-of-cyber-crime

V

Verizon (2023) Data Breach Investigations Report. Retrieved from https://www.verizon.com/business/resources/reports/dbir/2023/master-guide/

LEARN MORE

If you would like to learn more about the findings in this report or maritime cyber security in general, please get in touch.

Nick Chubb

Founder and Managing Director, Thetius
nick@thetius.com

Daniel Ng

CEO, CyberOwl
daniel.ng@cyberowl.io

Tom Walters

Partner, HFW
tom.walters@hfw.com

Thetius
CYBEROWL
HFW