inmarsat
RESEARCH PROGRAMME

BEYOND COMPLIANCE
CYBER RISK MANAGEMENT AFTER IMO 2021

BEYOND COMPLIANCE CYBER RISK MANAGEMENT AFTER IMO 2021

CONTENTS

FOREWORD

BEN PALMER OBE

PRESIDENT,
INMARSAT
MARITIME

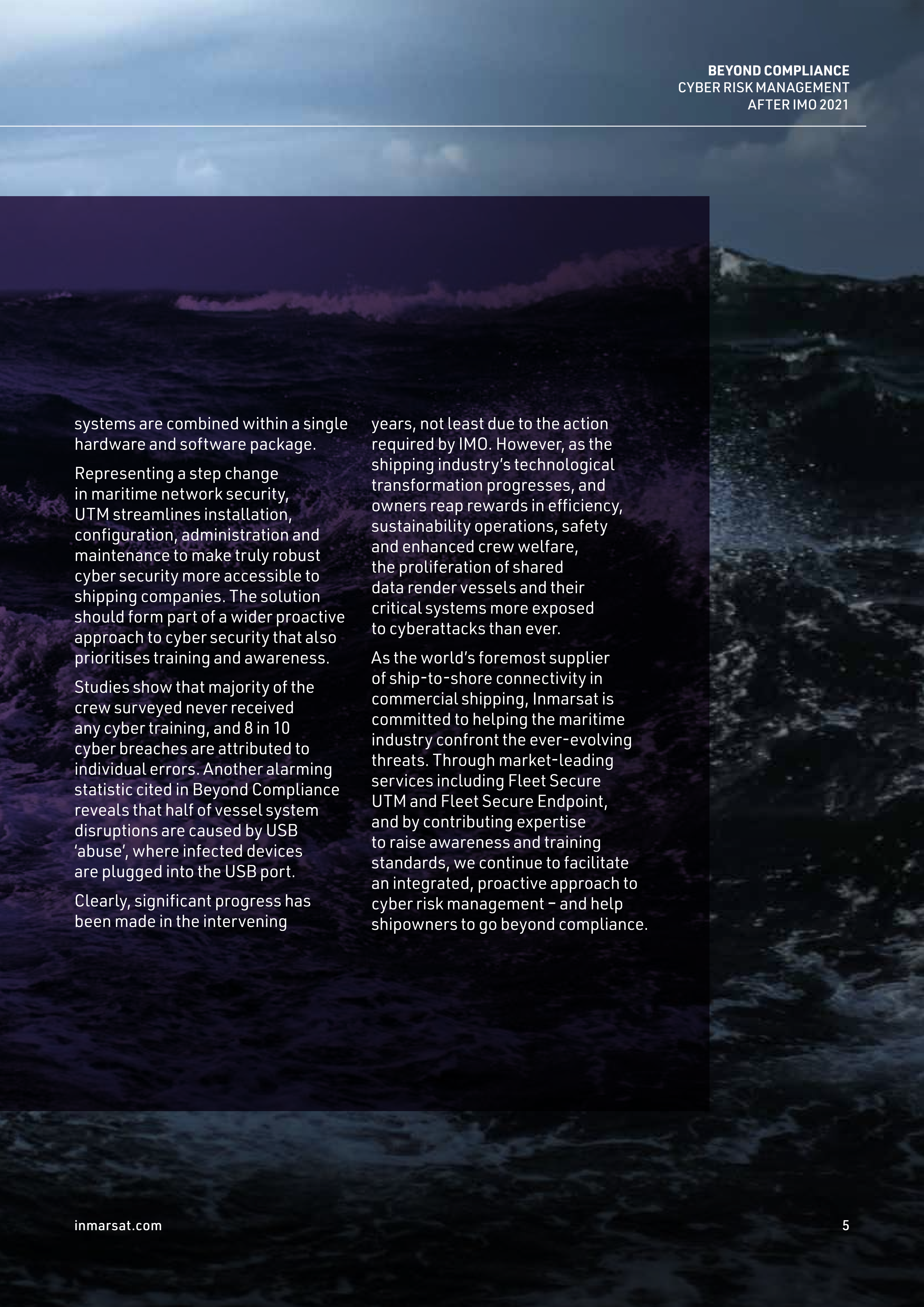
Cyber attacks are on the rise. Of nearly 200 maritime businesses surveyed earlier this year, almost half reported having been subject to a cyber breach since 2019. The IMO's 2021 cyber risk management code is helping shipowners to tackle this escalating threat, but there is more to cyber security than regulatory compliance.

In a report published earlier this year by Thetius, 3% of surveyed shipowners that had fallen victim to a cyber attack in the last three years reported having ultimately paid the perpetrator – at an average cost of US$3.1 million. Even where a ransom was not paid, the cost of combatting the threat averaged US$1.8 million.

Although the International Maritime Organization's (IMO) 2021 cyber risk management code establishes a much-needed foundation for cyber resilience, onboard technology continues to evolve, bringing with it new digital threats to shipping companies as they seek to match the pace of change. Against this background, the enclosed report, Beyond Compliance – Cyber Risk Management After IMO 2021, offers guidance on how to elevate cyber security standards above the IMO's regulatory framework.

Published as part of the Inmarsat Research Programme, Beyond Compliance examines the impact of the IMO 2021 cyber risk management code, explores the evolution of maritime cyber threats and explains how shipowners can respond to these risks.

Among the solutions highlighted in the report is unified threat management (UTM), an infrastructure-based approach whereby network security solutions including firewalls, anti-virus programs, content filters and intrusion prevention and detection



systems are combined within a single hardware and software package.

Representing a step change in maritime network security, UTM streamlines installation, configuration, administration and maintenance to make truly robust cyber security more accessible to shipping companies. The solution should form part of a wider proactive approach to cyber security that also prioritises training and awareness.

Studies show that majority of the crew surveyed never received any cyber training, and 8 in 10 cyber breaches are attributed to individual errors. Another alarming statistic cited in Beyond Compliance reveals that half of vessel system disruptions are caused by USB 'abuse', where infected devices are plugged into the USB port.

Clearly, significant progress has been made in the intervening years, not least due to the action required by IMO. However, as the shipping industry's technological transformation progresses, and owners reap rewards in efficiency, sustainability operations, safety and enhanced crew welfare, the proliferation of shared data render vessels and their critical systems more exposed to cyberattacks than ever.

As the world's foremost supplier of ship-to-shore connectivity in commercial shipping, Inmarsat is committed to helping the maritime industry confront the ever-evolving threats. Through market-leading services including Fleet Secure UTM and Fleet Secure Endpoint, and by contributing expertise to raise awareness and training standards, we continue to facilitate an integrated, proactive approach to cyber risk management – and help shipowners to go beyond compliance.

INTRODUCTION

By adopting new provisions into the ISM Code that, for the first time, embedded cyber risk management into safety management systems (SMS) for merchant ships, the IMO provided a clear (albeit high-level) anchor point for ship operators to benchmark their vulnerability to cyber threats. The rapid rise in cyber crime and attacks in the years leading up to its release had precipitated the need for leadership and direction setting from the highest level. Placing cyber risk management into the ISM code raised the floor for maritime operators and in particular gave smaller and less well resourced shipping companies a framework for building resilience to attacks.

It also catalysed other international bodies and expert organisations into action and now guidelines from BIMCO, the US National Institute of Standards and Technology (NIST), and others, form pillars of best practice for IT managers and cyber security teams to build their plans around.

Developments in connectivity and the transfer of data in greater volumes between ship and shore continue to bring significant gains for fleet management efficiency and crew welfare, but they also increase the vulnerability of critical systems onboard vessels to cyber attacks. An enduring feature of cyber threats is their ability to adapt and evolve, with new methods of attack finding new pathways of infection.

Earlier this year, Thetius surveyed nearly 200 maritime businesses on their experience of cyber attacks. 44% reported that their organisation has been the subject of a cyber attack in the last three years. Of those, 3% resulted in a ransom being paid by the victim to the attacker, at an average cost of US$3.1million. Even where a direct ransom wasn't paid, the costs to shipping arising from cyber threats and the personnel, systems, and infrastructure required to combat them, averaged US$1.8 million per year.[1]

In this report, we examine the ripple effects of IMO 2021 and the cyber risk management code and take a look at how shipping companies have raised standards of cyber security to compliance - and beyond. We begin by discussing how threats to shipping have evolved before exploring some of the emerging trends in management and response. We unpack Unified Threat Management (UTM) and tour some of the tools that are available to help maritime IT teams keep their networks and digital assets secure.

What is clear is that, while the IMO has provided a framework for basic threat resilience, there is more to combating cyber threats than compliance alone. New digital capabilities can lead to new digital threats to maritime businesses who are unprepared. Cyber security is an ever-evolving field, as is the case in maritime innovation. Keeping pace with developments on both sides is critical to building the wall high enough and thick enough to protect shipping from bad actors.

[1] Chubb, N. Finn P. Ng, D. (2022) The Great Disconnect - The State of Cyber Risk Management in the Maritime Industry. Thetius. P.18. available at thetius.com

CYBER RISK MANAGEMENT MAIN CYBER THREATS IN THE SHIPPING INDUSTRY

According to NIST's Computer Security Resource Center (CSRC) in the US, cyber risk management describes the process of 'identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders'.

NIST explains the process of identifying, assessing and mitigating the risks associated with the distributed but interconnected nature of IT and OT systems by monitoring events, processes and devices. This process covers a system's entire life cycle (design, development, distribution, deployment, acquisition, maintenance, and destruction), given that supply chain threats and vulnerabilities may, intentionally or unintentionally, compromise IT/OT at any stage.

Businesses most commonly experience the consequences of cyber threats as financial penalties, but this is not always the case. Perpetrators can include:
- Lone hackers
- Hacktivists
- Professional criminal organisations
- Advanced Persistent Threats (APTs)

While all of these can be considered 'bad actors', many attacks are automated and their sources are not always apparent. These attacks succeed by repeatedly probing for weaknesses in an organisation's networks and systems, often triggered by individual acts of carelessness by people with legitimate access to them. This is most commonly the result of connecting an infected peripheral device such as a USB stick or a crew member or employee opening a phishing email, which is a method used to steal sensitive information, such as account credentials or financial information, by pretending to be from a trustworthy source, such as an email or text from a friend or co-worker. Phishing emails entice users to click links that can install malware, giving hackers access to the organisation's technology environment.

SUPPLY CHAIN CYBER THREATS AND VULNERABILITIES

THREATS:
- Adversarial: e.g. insertion of counterfeits, tampering, theft, insertion of malicious software.
- Non-adversarial: e.g. natural/man-made disaster, poor quality products/services, poor practices.

VULNERABILITIES:
- Internal: e.g. information systems and components, organisational policy/processes.
- External: e.g. weaknesses to supply chain/within entities in supply chain, dependencies (power, communications, transportation, etc.).

In 2021, maritime security consultants, Waterways, conducted a penetration test across one carrier's fleet of 100

vessels. They sent 292 emails to the fleet nodes and tracked an open rate of 92%. **A link was contained in the email which was clicked by 90 of the recipient seafaring officers. 44 of them went on to access the website and enter in sensitive information.** While this email had been carefully designed to resemble a legitimate communication from head office, this is a tactic just as well understood by genuine threat actors.

Effective cyber risk management must consider multiple cyber assailants and diverse lines of attack - targeted and random. Continuous efforts are made by threat actors to update their strategies including malicious coding and vulnerabilities in hardware, software and even human behaviour.

In what still remains the most high profile shipping company attack in recent times, a piece of ransomware called 'NotPetya' found a point of entry into the Maersk logistics network via its container terminals business in 2017. The widely reported incident cost the container giant over $300m in systems renewal, with the group's IT team having to reinstall 4,000 servers, 45,000 PCs and 2,500 applications in 10 days.

However, Maersk is not alone. The list of high profile maritime businesses who have suffered similar attacks includes shipbroking powerhouse Clarksons, container operators CMA-CGM, COSCO, and MSC, and even the IMO themselves have had their networks compromised in recent years.

INDUSTRY PERSPECTIVE

EVERGAS

Evergas, a Danish petrochemical and natural liquid gas carrier can trace their roots back to 1883. With well over a century of operating experience, the company has learned to move with technology, stay dynamic, and take emerging threats seriously.

Their **IT Business Manager, Poul Rævdal**, joined the company in 2014 and has dedicated much of his time to building digital capability across the fleet,developing systems and processes that are resilient to digital threats. Poul told us, “Our fleet is all connected to the internet at various times and through various routes. From a network perspective, our ships have become a cluster of endpoints.”

The Evergas IT team manages their growing network of business, crew, and operational technology (OT) and is well aware of the threat that these increasingly interconnected shipping fleets create.

“We design and operate our network resilience framework around the BIMCO guidelines, TMSA3, IMO regulations and others, so that we take a blended approach,” Poul told us. ” We never compromise on safety and keep our business and crew network separate which ensures we have an uninterrupted connection to high-speed, always-on, business-critical bandwidth, with unlimited backup and 99.9% availability. We understand an attack on OT systems may endanger the safety of our vessels and crew, hence we need to be vigilant and prepared at all times.

So, which technological developments have Evergas implemented as a result of IMO 2021?

“I first began working with Inmarsat when we upgraded the communications equipment on eight ethylene tankers to Fleet Xpress. It was a natural progression for me from this to using network protection. We have a relatively small IT team, so it makes sense for us to unify the separate parts of our network security into one solution, dealing primarily with one supplier.”

Some IT managers are understandably nervous about implementing fundamental changes to their network security infrastructure. What was your experience of introducing unified threat management?

“Onboarding with Inmarsat Fleet Secure UTM was a great experience for us. The Inmarsat technical team gave us very detailed information that correlated how their UTM approach covers the requirements of the ISM code, advice from the various guidelines, and the four elements of the NIST approach - identify, detect, resolve, recover. This really helped us check off the details and ensure that the solution was comprehensive enough for our needs and our approach to network security.”

What impact IMO 2021 has had across the shipping industry in raising standards of cyber resilience?

“Regulations provide standards to base things on, but it is important from our perspective to go above and beyond the regulations. They are not always as strict or specific as they really should be in certain circumstances, but Bimco has produced a useful set of guidelines. For example, we physically separate the business network, crew network, and operational technology networks from each other and we also go beyond that with our unified threat management approach.”

Inevitably, new regulations and industry standards raise the possibility of enforcement and auditing. What has been the experience to date?

“We have not yet had a focussed ISM cyber security audit following 2021, other than aspects being covered as part of more broader surveys, but we are expecting it and getting ready for focussed cyber audits.”

A key issue for maritime IT managers is drawing together evidence for auditors that shows that fleet networks are being managed to at least minimum standards. For Poul, Inmarsat has created a powerful solution to this.

“As a UTM user, I go to the Fleet Secure Endpoint portal and I can access a system management overview, see all of the connected devices across the crew and business network, blocking and filtering statistics etc. It’s so nicely configured that you can access and download a comprehensive network report with one button click. The level of detail means that this is all an auditor is likely to require.”

> "It is important from our perspective to go above and beyond the regulations. We physically separate the business network, crew network, and operational technology networks from each other and we also go beyond that with our unified threat management approach."

SHIP-SPECIFIC THREATS AND VULNERABILITIES

Many of the incidents that make it to the public domain involve breaches of shorebased business networks and information technology (IT). This causes costly losses of company, customer, and supplier data, and threatens to undermine the company's reputation as a result.

However, ship fleets are becoming increasingly amalgamated into their operator's network infrastructure. Ships today have an interconnected, data-centric role in the global supply chain. As a result, they open up new pathways of infection and introduce 'operational technology' - or 'OT' - into the picture. OT describes the computer systems that play a functional, rather than simply informatic, role aboard the vessel. These could be ballast management computers, engine management systems, electronic chart display and information systems etc. While many are physically disconnected from the global communications network, some are not.

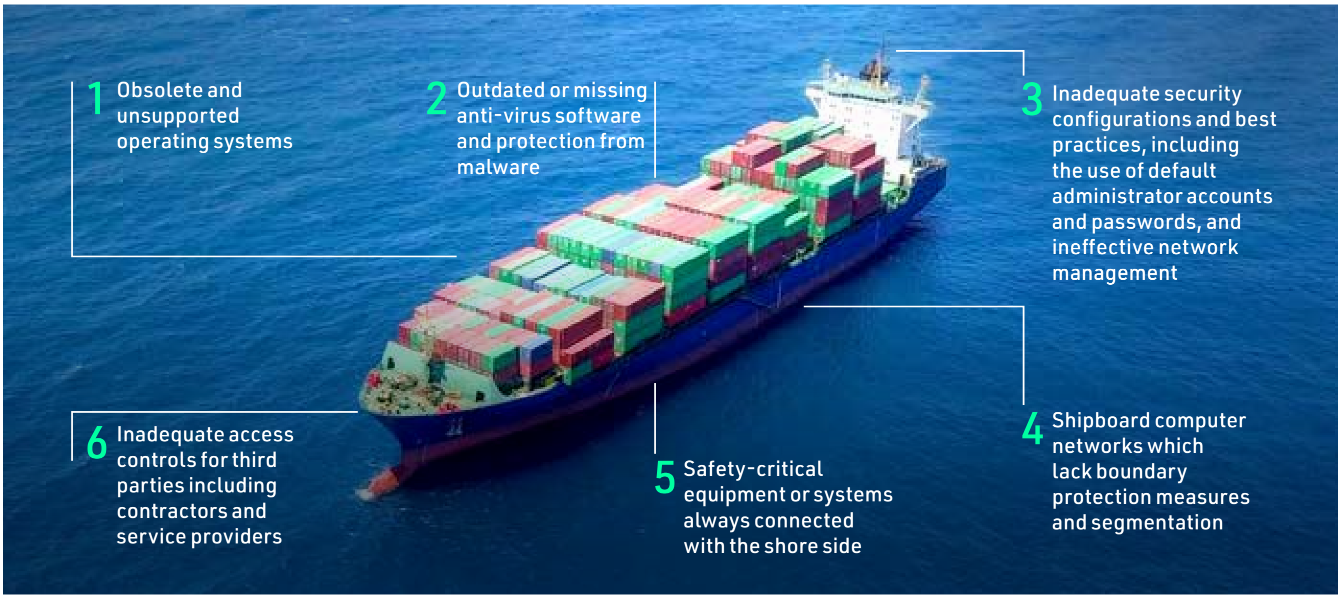
Cyber vulnerabilities on ships include:

- Obsolete and unsupported operating systems
- Outdated or missing anti-virus software and protection from malware
- Inadequate security configurations and best practices, including the use of default administrator accounts and passwords, and ineffective network management
- Shipboard computer networks which lack boundary protection measures and segmentation
- Safety-critical equipment or systems always connected with the shore side
- Inadequate access controls for third parties including contractors and service providers

Crew awareness of the prevailing threats while browsing the internet, checking email and interacting online and lack of training in responding to cyber threats.

Incidents can go under-reported too, even when operational technology is compromised with potentially catastrophic consequences. In one alleged incident, a ballast water management system was hijacked, resulting in an uncontrolled heeling of the vessel. Control was only returned to the crew after a ransom was paid, but the owner apparently preferred to leave the matter unreported over concerns that the ship would not be accepted for charter.

With more devices on board, more applications and media channels being used than ever before. According to an Inmarsat analysis of its more than 12,000 Fleet Xpress customer vessels, some ships are doubling their data usage every six months. The need for cyber resilience has therefore never been greater.


1 Obsolete and unsupported operating systems
2 Outdated or missing anti-virus software and protection from malware
3 Inadequate security configurations and best practices, including the use of default administrator accounts and passwords, and ineffective network management
6 Inadequate access controls for third parties including contractors and service providers
5 Safety-critical equipment or systems always connected with the shore side
4 Shipboard computer networks which lack boundary protection measures and segmentation

HARDWARE, SOFTWARE AND PERSONNEL

It is less likely for ships at sea to be the focus of targeted Denial Distribution of Service (DDOS) attacks, whose targets tend to be corporate or more transactional. However, malware and ransomware can be introduced easily enough to the unguarded ship network, via:

- Terminal hardware
- Software updates
- Misconfigured systems
- Inadequate integration
- Maintenance and design of cyber-related systems

In addition, ship networks are vulnerable to cyber threats arising from:

- Email, Phishing, social media scams, etc.
- USB memory stick as a source of malware
- Downloaded malware
- Connection with infected devices – cell phone, laptop, tablet
- Unauthorised use of bandwidth, exposing a lack of network segregation

These types of vulnerability relate to 'the human element', and specifically to weaknesses in cyber resilience as a result of shortcomings in procedures, training, and awareness among personnel.

Even setting aside the operational headaches, cost of system renewal, and the expenditure on training that a cyber breach can bring, ships that fall victim to a cyber attack can expect far-reaching implications, including:

- Claims against interruption to operations, e.g., a virus affecting onboard systems that causes costly delays in getting to port, potentially leading to cargo claims/charter party disputes and claims for compensation
- Loss of business-sensitive information could result in blackmail, with settlement no guarantee of closure
- Insurance cover: impact on premiums due to lack of cyber security measures
- Loss of reputation: corporate image tarnished by vulnerability to hackers
- Privacy impact: fined for failing to secure employee information

SYSTEMIC VULNERABILITIES

The IMO highlights the following ship systems as vulnerable to cyber attack:

1 Bridge systems
2 Cargo handling and management systems
3 Propulsion and machinery management and power control systems
4 Access control systems
5 Passenger servicing and management systems
6 Passenger facing public networks
7 Administrative and crew welfare systems
8 Communication systems

STANDARDS AND TECHNOLOGY

As we have established, IMO 2021 created a shift in the landscape for maritime cybersecurity. Regulatory compliance in the maritime industry is heavily driven by the nature of how the industry operates as an international market with stakeholders from all over the world. In order to ensure a level economic playing field for all these stakeholders, technical requirements do not tend to be highly advanced, favouring a yardstick approach over a more prescriptive one.[2] However, with the increasing threats faced by the industry and the vulnerabilities of the global maritime supply chain becoming more apparent, the industry's requirements for cyber risk management will only continue to evolve.

The International Association of Classification Societies (IACS) monitors the emerging cyber risk environment and acknowledges that the role of classification societies as advisors is becoming more prominent as the industry accelerates the uptake of digital technologies. So much so that the IACS is pushing for the improvement of onboard requirements for cyber systems on the global merchant fleet by focusing on concerns like updating software quality standards, developing cyber resilience, and successfully incorporating cyber risk management into the safety management systems of vessels under classed fleets. Through a process of cross industry collaboration, the IACS has developed several recommendations aimed at developing and maintaining the cyber integrity of ships. These recommendations primarily address the need for a more complete understanding of the interplay between onboard systems, the protection from events beyond software errors, the need for appropriate response and recovery in the event of the protection's failure, and the means for detection in order for the appropriate response to be put in place.[3]

In light of these growing threats and complexities, the IACS has also adopted new unified requirements focusing on the cyber resilience of vessels. The requirements, identified as UR E26 and UR E27, focus on providing minimum goal-based conditions for the cyber resilience of new ships and for the cyber security of onboard systems and equipment. UR E26 focuses on ensuring the secure integration of the operational technology (OT) and information technology (IT) equipment into the vessel's network during the design, construction, commissioning, and operational life of the ship. UR E27 focuses on ensuring that the integrity of the system is secured and hardened by third-party equipment suppliers. These new unified requirements will be applied to new ships contracted for construction on and after 1 January 2024, though they may be applied in the interim as non-mandatory guidance.[4]

Standards have been developed across many segments of the industry. In the tanker sector for example, standards in cybersecurity were incorporated into the OCIMF's Tanker Management and Self Assessment (TMSA) requirements as early as 2017. The addition of Element 13 of the TMSA 3 standards focuses on maritime security which includes the management and assessment of cyber systems.[5]

Looking at the increasing level of cyber risk in the global market, the standards for information security controls set forth by the International

[2] Meland, P.H., Bernsmed, K., Wille, E., Rødseth, Ø.J., & Nesheim, D.A. (2021). A Retrospective Analysis of Maritime Cyber Security Incidents. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation.

[3] Annual Review 2021, International Association of Classification Societies, extracted from https://iacs.org.uk/media/8965/iacs-ar-2021.pdf

[4] IACS adopts new requirements on cyber safety, published April 2022, extracted from https://iacs.org.uk/news/iacs-adopts-new-requirements-on-cyber-safety/

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

Organisation for Standardization (ISO) have also been revamped. Known as ISO 27002, the standard has extended to include new controls and new categorisations such as themes and attributes. With the IMO cyber risk management guidelines identified to be under the 'Cybersecurity Concepts' attribute.[6]

The focus on maritime cybersecurity has also created a surge in terms of technological developments, especially with the rapid pace of digitalisation in the maritime industry through technologies such as artificial intelligence, and data analytics. According to Gartner, one of the primary aims of cybercriminals is to hack through authenticated access points.[7] This approach allows them to blend in the normal environment. This risk requires investment in several cyber defence mechanisms such as improving identity infrastructure hygiene, introducing multifactor authentication and ensuring continuous monitoring. The Gartner report also highlights that the segmentation of networks helps in limiting the damage of undetected attacks, something that remains at the heart of cyber risk management guidelines. In the maritime context, this would be the segregation of IT, OT, IoT systems, and following recent amendments to the MLC; crew internet access networks.

As emerging technologies cut deeper into the operations and processes of the maritime world, new risks and dangers also emerge. For Port-IT, these emerging maritime threats are what drives development across their product line. The company was established in 2007 in response to growing demand for cyber security solutions that met the specific needs of shipping.

Over a decade later, the Fleet Secure Endpoint service they developed in partnership with Inmarsat Maritime has made a considerable impact, winning the 2019 Safety at Sea 'Best Security Solution' award, going on to become a market leading security package as part of the Inmarsat Fleet Secure UTM system.

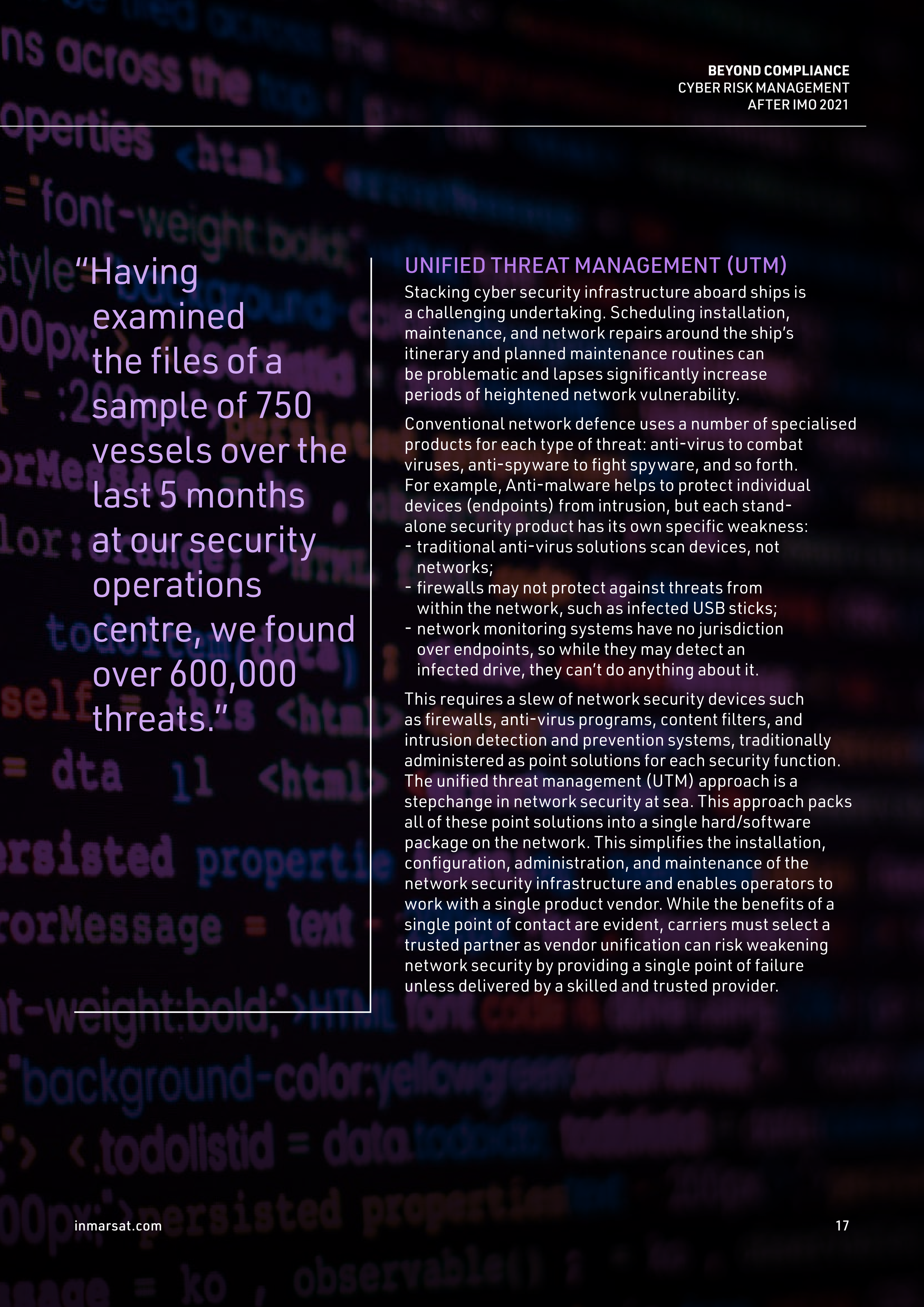
From anti-virus to integrated network security products, the company tailors their approach specifically to the maritime cyber threat environment. Speaking on a webinar in 2021[8], Port-IT CEO Youri Hart provided some startling statistics. He said, "having examined the files of a sample of 750 vessels over the last 5 months at our security operations centre, we found over 600,000 threats - and that is a lot. Among those threats, we found 1391 unique viruses - that means that each vessel had an average close to 2 unique virus infections. Interestingly, we also saw a difference in the most common viruses detected between these ships and shore-based networks. In the 'real world' ashore at that time, the most common threat detected was Inc.Attack.Generic, which was trying to exploit Windows vulnerabilities. But on the ships, the most common virus detected was Win/Madang.a. This is a virus that is already 15 years old and was being introduced by crew using USB drives."

Hart continues to note that, **"Ransomware is an issue for the maritime industry. While ransomware only made up 0.7% of our total detection of file code that we saw, this equates to 42% of vessels being hit by a ransomware attack. Luckily, these ships were protected by the solutions they had in place, but it is clear that this remains a serious threat."**

[6] ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection - Information Security Controls, extracted from https://www.iso.org/standard/75652.html

[7] How to Respond to a Supply Chain Attack, Gartner, published January 2021, extracted from https://www.gartner.com/smarterwithgartner/how-to-respond-to-a-supply-chain-attack

[8] Digital Ship. Getting Shipboard Cybersecurity Right. 2021. Available at https://www.youtube.com/watch?v=4e6UQBdv6wU



> "Having examined the files of a sample of 750 vessels over the last 5 months at our security operations centre, we found over 600,000 threats."

UNIFIED THREAT MANAGEMENT (UTM)

Stacking cyber security infrastructure aboard ships is a challenging undertaking. Scheduling installation, maintenance, and network repairs around the ship's itinerary and planned maintenance routines can be problematic and lapses significantly increase periods of heightened network vulnerability.

Conventional network defence uses a number of specialised products for each type of threat: anti-virus to combat viruses, anti-spyware to fight spyware, and so forth. For example, Anti-malware helps to protect individual devices (endpoints) from intrusion, but each stand-alone security product has its own specific weakness:

- traditional anti-virus solutions scan devices, not networks;
- firewalls may not protect against threats from within the network, such as infected USB sticks;
- network monitoring systems have no jurisdiction over endpoints, so while they may detect an infected drive, they can't do anything about it.

This requires a slew of network security devices such as firewalls, anti-virus programs, content filters, and intrusion detection and prevention systems, traditionally administered as point solutions for each security function. The unified threat management (UTM) approach is a stepchange in network security at sea. This approach packs all of these point solutions into a single hard/software package on the network. This simplifies the installation, configuration, administration, and maintenance of the network security infrastructure and enables operators to work with a single product vendor. While the benefits of a single point of contact are evident, carriers must select a trusted partner as vendor unification can risk weakening network security by providing a single point of failure unless delivered by a skilled and trusted provider.

PRODUCT FOCUS

WHAT IS INMARSAT FLEET SECURE UTM?

As we have seen, using point solutions to defend individual threat types becomes difficult to manage in the maritime context. As the complexity increases, so do the opportunities for error. Attackers only need to be successful once; defenders must succeed every time. This is where Fleet Secure Unified Threat Management (UTM) shines.

With Fleet Secure UTM, operators no longer need to juggle products from multiple vendors to secure their networks. UTM combines multiple security features into a single device or software package, simplifying system defence and reducing CAPEX and OPEX in the process. Integrating network security functions simplifies both management and compliance.

Fleet Secure UTM is a comprehensive package of network security tools designed to help shipping companies comply with the IMO 2021 cyber security requirements in one simple step. It continuously inspects, detects, and protects connected vessel networks in line with the NIST cybersecurity framework - identify, protect, detect, respond and recover.

Via a user-friendly online portal, all Inmarsat Fleet Secure UTM users get comprehensive:

- asset management;
- automatic detection of new devices on the network;
- alerting;
- remote 24/7 expert monitoring at the Security Operations Centre; and
- reporting.

These benefits facilitate compliance with the IMO 2021 cyber security risk management regulations and instantly put clients at an advantage. But in today's cyber environment, compliance with regulations isn't enough in isolation. For companies going beyond compliance, Fleet Secure UTM can integrate continuous:

- gateway anti-virus software to monitor, identify and block any trace of infection;
- intrusion detection and prevention;
- advanced ransomware detection;
- web-content filtering to block malicious traffic; and
- application control.

WHAT IS FLEET SECURE ENDPOINT?

Fleet Secure UTM works at the network level, controlling the gateway. At the opposite end, Inmarsat's Fleet Secure Endpoint is an advanced anti-malware system that targets endpoints from a network-centric perspective. Endpoint protection is critical to ensuring layered protection—firewalls, company policies, and network security devices are not enough.

Fleet Secure Endpoint detects and supports all fixed and mobile devices and operating systems on board. As well as ransomware protection, it includes:

- regularly updated anti-virus, anti-malware and anti-phishing protection;
- network monitoring for potentially malicious devices;
- system status information, risk assessments, and recovery procedures;
- asset management and inventory for all connected devices;
- 24/7 Security Operations Centre monitoring and support;
- automatic logging of all actions taken by support staff;
- a detailed dashboard showing recent security alerts; and
- scheduled risk assessments

FLEET SECURE ENDPOINT FEATURES AND BENEFITS

Fleet Secure Endpoint offers continuous protection of all online endpoints on the vessel's network with web content filtering blocking malicious traffic whether it's incoming or outgoing. Every single potential vulnerability across the vast network of the vessel can be defended from threat regardless of origin. Whether from a computer, crew laptop, USB or onboard sensor, Fleet Secure Endpoint will automatically monitor, identify and block any trace of infection. Lightweight software on end-user machines handles updates and reports system status to the server. It provides multi-layered security by integrating anti-virus, anti-phishing, anti-spyware, botnet protection, and more.

Fleet Secure Endpoint includes advanced remote network endpoint monitoring to provide enhanced network oversight. In-house IT teams can remotely monitor all security events, set up alerts and remotely roll-out configuration updates.

At the Security Operations Centre, a team of trained cyber security experts and experienced marine engineers provide 24/7 support. Above all, Fleet Secure Endpoint is designed explicitly for a maritime environment . For vessels with low bandwidth, lower-data options for Fleet Secure Endpoint are available on request.

HOW CAN FLEET SECURE HELP WITH IMO 2021 COMPLIANCE?

There are 5 stages to IMO 2021:

1 Identify key roles and systems/assets

Shipping companies must establish their own usage and access policies to IT and OT networks onboard and identify critical tasks. Inmarsat can consult with Fleet Secure customers and help them build robust policies that work with the powerful capabilities of Fleet Secure. The system tracks and monitors all connected devices and provides a breakdown of software and operating systems installed including version numbers. Inmarsat can also provide cyber security assessment reports and penetration testing.

2 Protect critical infrastructure services

Fleet Secure provides the ability to identify risks to ships, personnel, and the environment and helps carriers establish the appropriate safeguards such as a secure network architecture. From establishing LAN, VLAN split, and network segregation and isolation, to providing firewall, blocking, DDoS, IP, and Port Filtering infrastructure, Fleet Secure UTM represents a total solution.

3 Detect cyber events

Intrusion detection and prevention is embedded into the Fleet Secure solution and the system monitors for IT Policy violations and Security Information and Event Management (SIEM).

4 Resolve cyber events

Blacklist, whitelisting, blocking, and preventing recurrences is a vital part of managing cyber risk. Fleet Secure UTM manages all of these as well as providing a framework for authorising remote access if required.

5 Recover from cyber events

Fleet Secure UTM provides a powerful logging and reporting functionality. This ensures effective cyber forensics are available following intrusion and hijacking attempts.

PUTTING CYBER RISK MANAGEMENT COMPLIANCE INTO PRACTICE

Managing cyber risk onboard ships is considered a natural extension of current operational risk management practices incorporated into existing Safety Management Systems within the existing ISM Code.

The relevant MSC.428(98) - Maritime cyber risk management in safety management systems resolution therefore:

- Affirms that an approved safety management system should consider cyber risk management in accordance with the objectives and functional requirements of the ISM Code.
- Encourages administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

RESPONDING TO CYBER ATTACKS

The Cyber Security Plan should, at minimum, include:

- A process for initial incident triage
- Steps to quarantine all electronic traffic to and from ship or fleet. Procedures for alerting and requesting communication vendors to check traffic
- Procedures for keeping corporate IT security department abreast of the situation
- Procedures to secure/ establish backup communications to the affected vessel(s)
- Steps to stabilize and isolate the infected system to guard against further spread
- Steps for gathering Intelligence and evidence from affected systems
- Procedures for executing recovery of critical systems remotely
- Arrangements for completely replacing the ICT system at the next safe port after a cyber event

RECOVERY FROM CYBER ATTACKS

Workaround plans are required to take account of possible failures in critical shipboard systems, with the processes described in a vessel's emergency manuals so that the Captain can respond without the need to ask for help from/wait for shore-based colleagues. These plans should provide the Captain with instructions and/or a checklist on what to do. In the case of cyber resilience, workarounds plans might include:

- Actions to restore crashed/ failed email clients or degraded/failed ship-shore communication links; use backup FleetBroadband for email/voice until recovery
- Actions to work around/ recover failed PCs
- Usage of citadel telephone to send telex; testing of backup email ID from ship-to-shore and from shore-to-ship
- Fall back to paper charts in case of compromised ECDIS

In all cases, the Fleet ICT Manual inserted into the Ship's SMS/ISM Code documentation should provide full guidance and document the Cyber Security Plan for all critical on-ship systems.

TRAINING FOR CYBER ATTACKS

As the Plan is part of the Vessel's ISM it is also essential to periodically carry out drills to test any issues, train the crew, HSSE (Health, Safety, Security & Environment) team and any other stakeholders on how to respond to a cyber incident onboard ship, and encourage a culture of continual improvement. This means ship owners and managers should give cyber security drills the same weight as they give any regular Incident Management Drill – whether for grounding, ship fire or collision.

Under the new regime, cyber drills should be conducted across the fleet at least once a year to test response procedures and assess crew preparedness, procedures during a cyber incident onboard. It is essential that the Ship Manager's Incident Commander takes charge and demonstrates effective leadership in these exercises to ensure the security of the ship, its crew and cargo, while allowing the Fleet IT team to concentrate on securing the ICT infrastructure and resolving the cyber issues. In addition, regular anti-phishing campaigns and penetration testing using simulated malicious emails can maintain high-levels of crew vigilance and test onboard systems and processes.

Penetration testing by professional 'white-hat' hackers should also take place to identify technical weaknesses.

A PATHWAY TO COMPLIANCE

As the leading supplier of ship-to-shore connectivity in commercial shipping, Inmarsat is also a stakeholder where the development of industry best practices are concerned, both as a service provider and as custodian of a global network that is secure across all touchpoints. In fact, its secure, encrypted network uses military-grade satellites, is fully approved by the highest standards of the IMO and is fully audited by the stringent standards of International Mobile Satellite Organization (IMSO).

Based on its experience of offering a secure communication platform from the onshore office to the maritime terminals onboard ship, Inmarsat has developed security services designed to uphold cyber resilience at sea. These are most effective with Inmarsat's high-speed service Fleet Xpress and include:

Fleet Secure Endpoint – a powerful multi-layered endpoint security solution for remote monitoring of onboard computers

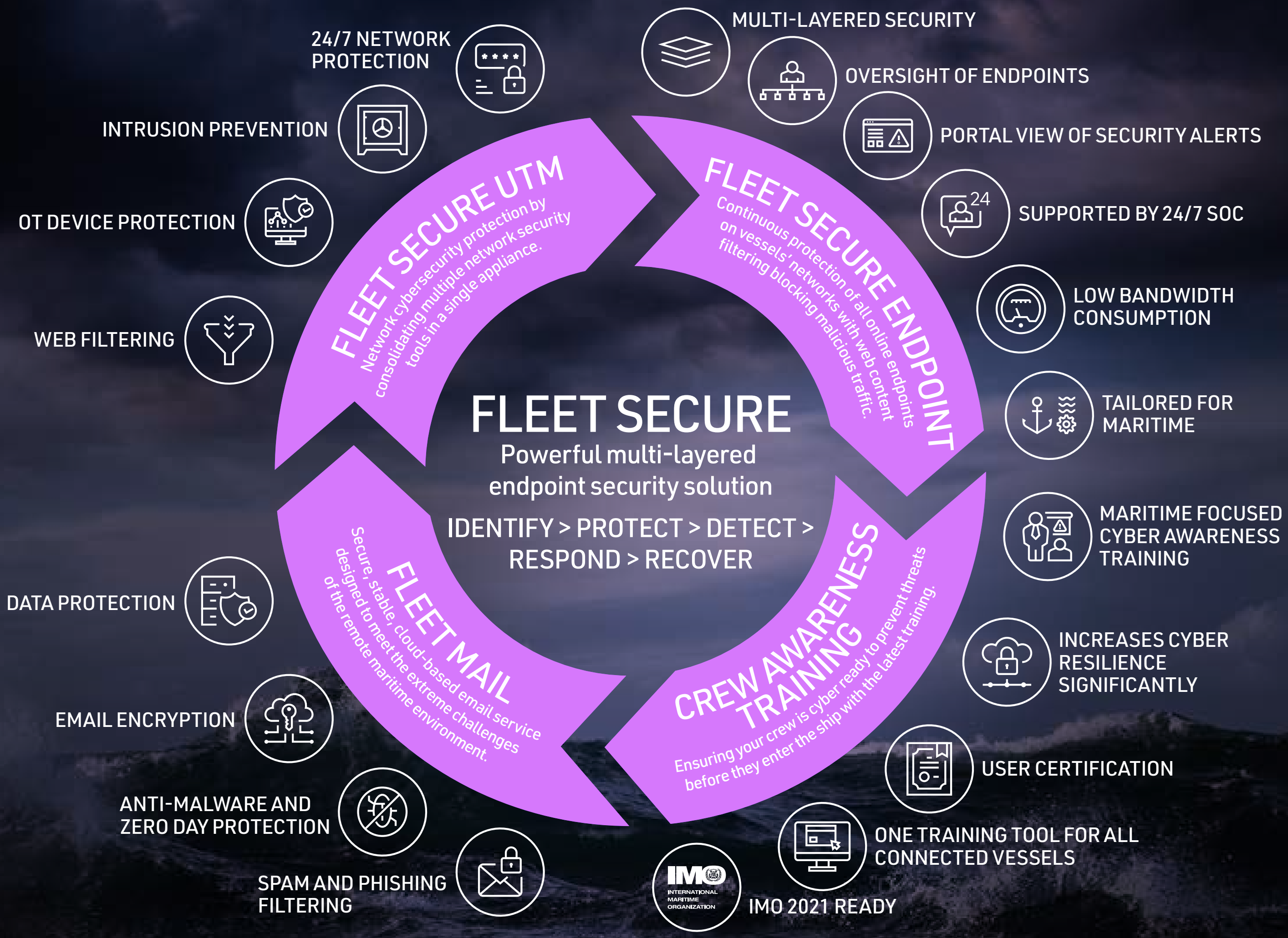
Fleet Secure Unified Threat Management – a powerful multi-layered anti-virus solution, to remove infections and threats on any onboard network

Fleet Secure Cyber Awareness – a mobile training app for crew to gain up-to-date cyber security knowledge

Fleet Mail – optimised for use at sea, delivering a stable, secure service for reliable and continuous access to emails, even if the network temporarily goes offline.

The following section of this report offers guidance covering Fleet Secure Endpoint, with a specific focus on the digital tool's potential to offer direct support to ship operators/owners seeking to implement IMO 2021-ready cyber security SMS.

While not representing compliance itself, Fleet Secure Endpoint implementation provides endpoint protection on vessels based on IMO's 'identify, detect, protect, respond, recover' pillars for cyber security planning. In offering a fully IMO-compliant reporting solution, it also supports operators/owners to achieve compliance at every stage in an orderly and straightforward manner.



FLEET SECURE

Powerful multi-layered endpoint security solution

IDENTIFY > PROTECT > DETECT > RESPOND > RECOVER

FLEET SECURE UTM
Network cybersecurity protection by consolidating multiple network security tools in a single appliance.

FLEET SECURE ENDPOINT
Continuous protection of all online endpoints on vessels' networks with web content filtering blocking malicious traffic.

CREW AWARENESS TRAINING
Ensuring your crew is cyber ready to prevent threats before they enter the ship with the latest training.

FLEET MAIL
Secure, stable, cloud-based email service designed to meet the extreme challenges of the remote maritime environment.

24/7 NETWORK PROTECTION

INTRUSION PREVENTION

OT DEVICE PROTECTION

WEB FILTERING

MULTI-LAYERED SECURITY

OVERSIGHT OF ENDPOINTS

PORTAL VIEW OF SECURITY ALERTS

SUPPORTED BY 24/7 SOC

LOW BANDWIDTH CONSUMPTION

TAILORED FOR MARITIME

MARITIME FOCUSED CYBER AWARENESS TRAINING

INCREASES CYBER RESILIENCE SIGNIFICANTLY

USER CERTIFICATION

ONE TRAINING TOOL FOR ALL CONNECTED VESSELS

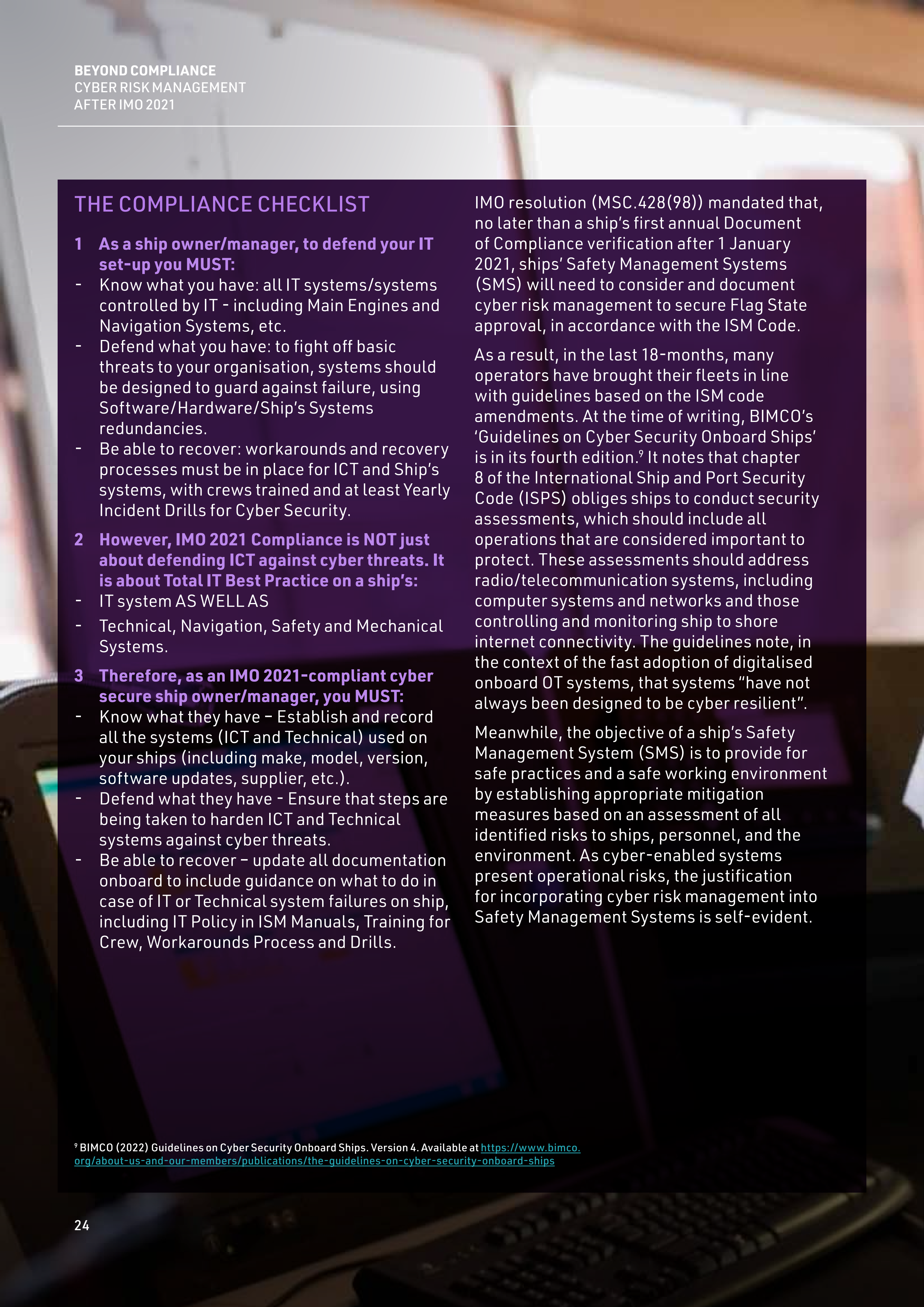
IMO 2021 READY

DATA PROTECTION

EMAIL ENCRYPTION

ANTI-MALWARE AND ZERO DAY PROTECTION

SPAM AND PHISHING FILTERING



THE COMPLIANCE CHECKLIST

1 **As a ship owner/manager, to defend your IT set-up you MUST:**

- Know what you have: all IT systems/systems controlled by IT - including Main Engines and Navigation Systems, etc.
- Defend what you have: to fight off basic threats to your organisation, systems should be designed to guard against failure, using Software/Hardware/Ship's Systems redundancies.
- Be able to recover: workarounds and recovery processes must be in place for ICT and Ship's systems, with crews trained and at least Yearly Incident Drills for Cyber Security.

2 **However, IMO 2021 Compliance is NOT just about defending ICT against cyber threats. It is about Total IT Best Practice on a ship's:**

- IT system AS WELL AS
- Technical, Navigation, Safety and Mechanical Systems.

3 **Therefore, as an IMO 2021-compliant cyber secure ship owner/manager, you MUST:**

- Know what they have – Establish and record all the systems (ICT and Technical) used on your ships (including make, model, version, software updates, supplier, etc.).
- Defend what they have - Ensure that steps are being taken to harden ICT and Technical systems against cyber threats.
- Be able to recover – update all documentation onboard to include guidance on what to do in case of IT or Technical system failures on ship, including IT Policy in ISM Manuals, Training for Crew, Workarounds Process and Drills.

IMO resolution (MSC.428(98)) mandated that, no later than a ship's first annual Document of Compliance verification after 1 January 2021, ships' Safety Management Systems (SMS) will need to consider and document cyber risk management to secure Flag State approval, in accordance with the ISM Code.

As a result, in the last 18-months, many operators have brought their fleets in line with guidelines based on the ISM code amendments. At the time of writing, BIMCO's 'Guidelines on Cyber Security Onboard Ships' is in its fourth edition.[9] It notes that chapter 8 of the International Ship and Port Security Code (ISPS) obliges ships to conduct security assessments, which should include all operations that are considered important to protect. These assessments should address radio/telecommunication systems, including computer systems and networks and those controlling and monitoring ship to shore internet connectivity. The guidelines note, in the context of the fast adoption of digitalised onboard OT systems, that systems "have not always been designed to be cyber resilient".

Meanwhile, the objective of a ship's Safety Management System (SMS) is to provide for safe practices and a safe working environment by establishing appropriate mitigation measures based on an assessment of all identified risks to ships, personnel, and the environment. As cyber-enabled systems present operational risks, the justification for incorporating cyber risk management into Safety Management Systems is self-evident.

[9] BIMCO (2022) Guidelines on Cyber Security Onboard Ships. Version 4. Available at https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

CYBER RISK MANAGEMENT AUDITS

To verify that companies have adequately and appropriately implemented and incorporated appropriate cyber risk mitigation into their SMS, internal and external audits are given a mandate in accordance with the ISM Code. Routine examinations verify that a management system includes cyber risk management with a cursory review of the system's documentation. In preparing this report, Thetius did not interview an operator that had received an audit specifically examining cyber risk management compliance, although many are being asked for some evidence as part of a wider survey.

Vessels must be able to demonstrate to Port State Control or any other recognized authority that the ship, its systems and its crew are prepared for cyber risks and what to do about them in the same way that they would need to document any other safety issue.

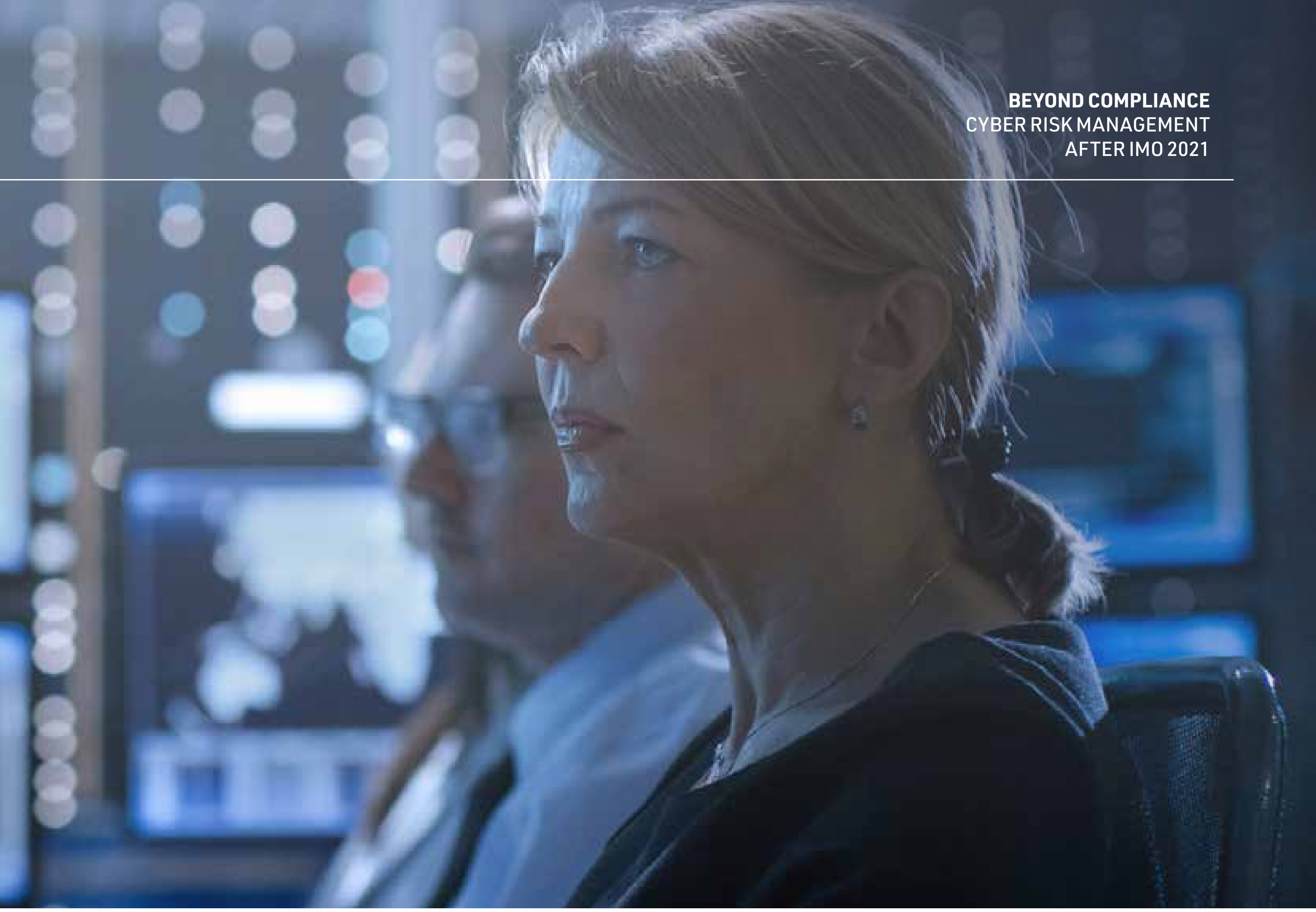
Therefore, prepared answers are needed to the questions:

- What assets do we have (kind of hardware/software and what is connected to the network)?
- What would we do if they do not work?
- How are assets protected?
- What would we do if they were compromised?
- Who has control ashore and onboard?

As well as being able to liaise with or identify the person responsible for cyber security on the ship, the Port State/Flag State/RO auditor should be able to check that the Safety Management System documents this and shows that the ship's owner or manager:

1 Has identified the systems on-board and outlined the relevant cyber risks
2 Has the ability to detect breaches in cyber security onboard
3 Has measures in place to protect systems and software onboard
4 Has response measures in place to deal with a cyber attack, specifically related to system redundancy, training and workaround plans

The IMO resolution on cyber risk - MSC.428(98) – references MSC-FAL.1/Circ.3 on Guidelines on maritime



cyber risk management offer an introduction to cyber threats in the maritime domain covering:

- IT and OT systems
- Intentional and unintentional threats
- Identify – Protect – Detect – Respond – Recover
- International best practices – ISO and EN standards

This is all-encompassing, and the modular concept of the ISM Code is flexible enough to offer a framework for continuous improvement that can accommodate cyber security in a company's SMS. Even so, individual companies will clearly vary in terms of systems, personnel, procedures and preparedness. The risks to a specific ship will also be unique and dependent upon the specific integration of cyber systems aboard. It is nonetheless up to ship owners and operators to assess their cyber risks and to implement appropriate mitigating measures: each 'Document of Compliance' or 'DoC' holder must consider their own cyber risks and implement necessary measures in their SMS.

It is important to add that ISM does not prescribe a calendar schedule for assessing new risks, instead advising that they are accommodated as soon as possible. For this reason, the SMS should continue to be considered by owners as a 'live' document that is regularly updated and improved as risks evolve.

The general situation still resembles a settling-in period for most maritime jurisdictions, but operators must be prepared for targeted cyber security audits at any time. Achieving and documenting compliance relies on ship owners and ships having had their IT, operating technology systems, procedures and crew training risk-assessed to demonstrate that they are prepared for cyber attacks and the actions that will be taken should systems be compromised. This would include producing a comprehensive status report of the operators business network, operational technology network, and employee access network. IT managers are advised to consider this when selecting cyber security partners and this report is generated automatically and to a high level of detail Inmarsat's Fleet Secure portfolio.

Systems Inventory

Developing a process to identify, protect against, detect, respond to and recover from cyber attacks is no box-ticking exercise: in the first instance, the ship owner/manager must be prepared to report an inventory of all critical hardware and software systems onboard each of its ships, listing the:

- IoT Systems
- Navigation
- Engine Control
- Cargo Control
- DP, Gas, Firefighting, etc.
- ICT – Business Computer System
- ICT – Crew Systems

This list needs to include:

Hardware

- Record make, model, version, function on all your hardware
- Individual hardware (and IP address) and patch panel, power
- Take note of possible attack surface/connection point among your hardware and work to secure them (USB, Ethernet, exposed wiring)

Software

- Record make and version of the applications used on ship across all hardware. Firmware and software application versions, patch levels, malware protection

Existing documentation should be used as much as possible - especially technical and engineering details.

In terms of response and recovery, it is also the owner/manager's responsibility to formalise solutions that address security gaps, so that the ship can continue to operate in the event of a cyber attack or its aftermath, or at least the risks can be mitigated. It should be evident that workaround plans for critical systems and processes are incorporated into the network and system design and described for Captains in a vessel's emergency manuals. These plans should include instructions and/or checklist in the event of critical system failure, due to cyber incident or unplanned system breakdown without a need to request and wait for help from the shore office. The responsibility for verifying these steps when the ship's DoC is due for renewal also falls to the ship's owner/manager.

Risk Assessment Scope

The goal of the assessment of a ship's network and its systems and devices is to identify any vulnerabilities that could compromise or result in either loss of confidentiality, loss of integrity or result in a loss of operation of the equipment, system, network, or even the ship. As explained elsewhere, these vulnerabilities and weaknesses broadly fall into one of the following categories:

1. Technical such as software defects or outdated or unpatched systems
2. Design such as access management, unmanaged network interconnections
3. Implementation errors for example misconfigured firewalls
4. Procedural or other user errors

Responsibilities

IMO 2021 requirements do not cover servers or staff onshore but they clearly have a major impact on fleet management. For example, the individual managing the Fleet IT policy and documentation (usually, the 'Fleet ICT Manager') would also normally be responsible for the owner/manager ISM documentation system for ships, for example. Critically, under IMO 2021, at a minimum a ship's SMS identifies the party ashore and onboard taking responsibility for cyber security (ICT Manager, Chief Security Officer, or any other). In broad terms, that individual will take responsibility for:

- Having an understanding of the extent of cyber risks
- Managing crew awareness of and preparedness for threats to the vessel's systems
- Steps to secure ship systems to minimise the impact if a threat is actualised

In line with the ISO27001 standard, IMO 2021 also states that the owner's risk assessment should be auditable for the following attributes:

- The hardware installed
- The software in use
- Details of what is connected to the network
- How the above is protected

In best practice organisations, fleet ICT Managers work with the crewing department to ensure that the crew understands the importance of cyber security and have been trained either in the classroom or online. A record of the crew's performance in these training exercises should be kept on file by the HR/Crewing department and made available to audit inspectors.

120243
209.1
2046
288
0.0
0.0
288
100
100
Heading
209.1
Rate Of Turn
303
Pilot Card
Auto Pilot
Signals
Gyro
Heading
Mode1

RELATED CYBER SECURITY GUIDELINES

RELATED GUIDELINES

IMO's GUIDELINES ON MARITIME CYBER RISK MANAGEMENT refer to three specific guidelines as having been developed to help shipping get 'cyber ready':

1 Guidelines on Cyber Security Onboard Ships – BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, OCIMF, IUMI and WORLD SHIPPING COUNCIL.

Guidance to ship owners and operators on procedures and actions to maintain the security of cyber systems in the company and onboard ships; designed to help owners understand, and manage:

- Limitation and control of network ports, protocols and services
- Configuring network devices such as firewalls, routers and switches
- Secure configuration of hardware and software
- Protecting web browsing and email
- Satellite and radio communications
- Defences against malware
- Data recovery capability
- Wireless Access control
- Password protection
- Application software security (patch management)
- Secure network design
- Physical security
- Boundary defence

The Guidelines also includes procedural controls for crew, including training and awareness, software maintenance and upgrades, and anti-virus updates. However, the Guidelines are not a basis for external auditing of a company's/ship's approach to cyber risk management.

2 NIST framework

Published in 2014 by the US National Institute of Standards and Technology, the NIST CSF guide focuses on the same five functional elements presented by the IMO for risk management - Identify, Protect, Detect, Respond, Recover, to assist organisations in:

- Describing their current cyber security posture
- Describing their target state for cyber security
- Identifying/prioritising opportunities for improvement within a repeatable process
- Assessing progress toward the target state
- Communicating among internal and external stakeholders about cyber security risk

The NIST framework includes usable profile templates for use in risk assessment profiling at the individual vessel level. The resulting profile will help to identify and prioritise actions to align policy, business and technological approaches in order to manage and reduce risks.

Sample profiles are publicly available: http://mariners.coastguard.dodlive.mil/2018/01/12/1-12-2018-release-of-offshore-operations-and-passenger-vessel-cybersecurity-framework-profiles.

3 ISO27001

The ISO27001-Annex A of cyber security objectives is published currently as ISO 27002. Here, cyber security controls are not specifically focused on Critical Infrastructure Protection or on the Maritime Industry, but with appropriate focus on cyber risk they may be applied by any organisation.

ISO27001 is also the only information security management system standard that can be independently certified with a level of authority.

MOVING BEYOND COMPLIANCE

Over the 12 months between May 2020 and May 2021, cyber attacks targeting the maritime sector increased by 168% in the Asia-Pacific region alone.[10]

This figure reflects a more expansive global trend of cyber threats aimed at, or heavily impacting on the maritime industry. Aboard ships, in ports, or in company offices, the need to go above and beyond the compliance requirements for cyber risk management is growing rapidly as the industry advances the use of digital technologies and onboard information technology systems.

The guidelines on maritime cyber risk management published by the International Maritime Organization (IMO) have helped stakeholders address these threats. Alongside high-profile incidents affecting prominent carriers within the past few years and the increased visibility of the maritime supply chain as a key factor in global trade, the industry has become more aware of the scale and urgency of the risks. However, the nature of digital attacks is evolving due to advancements in computing technology and the increased prevalence of geopolitical conflicts occurring worldwide. This requires shipping companies and maritime organisations to take a more proactive approach toward cyber risk management.

As we have seen already, the IMO list five functional elements of a maritime cyber security plan[11]: identify, protect, detect, respond, recover.

In order to ensure the resilience of any organisation's digital infrastructure, settling for the standard should not be the only option and a continuous cycle of improvement should always be upheld. Similar to the development of technology products, the focus on addressing these maritime cyber threats will require a continuous loop of assessments and improvements as the profile of maritime cyber threats also evolves with the technological landscape on board ships and ashore.

Digitalisation brings both positive and negative aspects related to the evolving cyber risk landscape of the maritime industry. This requires that the adoption of digital technologies must be approached strategically. The integration of these technologies must also be configured according to the organisation's cyber security policies and procedures in order to minimise the potential attack surface for malicious parties.[12] Ship owners and ship managers must look at digital technologies as critical parts of their development, and every potential vulnerability must be assessed before they are ultimately integrated into the organisation's systems. In order to do this, ship owners and ship managers must understand the importance of segregating their business systems and their operational systems,[13] and preparing for the impact that these systems may receive if ever they fall vulnerable to cyber threats. Establishing these divisions are important and managing them is even more critical. In this day and age, technology gives companies a competitive advantage, but without proper management and execution, it may be their downfall.

The use of emerging technologies utilising deep learning and reinforcement learning algorithms can also potentially support the efforts of shipping companies aiming to go beyond the regulatory requirements and ensure that their networks are continuously monitored for malicious activity. The application of digital technologies such as artificial intelligence provides industry stakeholders an option for automated threat detection and can support organisations in containing potential threats to their businesses.[14]

Maintaining control over technology requires the decision makers within the organisation to focus

[10] Rising cyber exposure in Asia maritime shipping, Sabba Manyara, The Asset Publishing and Research Ltd, published January 2022, extracted from https://theasset.com/article/45794/rising-cyber-exposure-in-asia-maritime-shipping

[11] MSC-FAL.1/Circ.3, Guidelines on Maritime Cyber Risk Management, International Maritime Organization, published July 2017, extracted from https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

[12] Meland, P.H., Bernsmed, K., Wille, E., Rødseth, Ø.J., & Nesheim, D.A. (2021). A Retrospective Analysis of Maritime Cyber Security Incidents. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation.

[13] Report: Maritime Cyber Attacks Up by 400 Percent, The Maritime Executive, published June 2020, extracted from https://maritime-executive.com/article/report-maritime-cyberattacks-up-by-400-percent

[14] Caravel Group and DarkTrace, extracted from https://www.darktrace.com/en/resources/cs-caravel-group.pdf

on several key elements such as how people interact with it, how it supports the business, how we can measure its performance, and how the business can go on without it. Understanding our relationship with technology gives organisations a better grasp of where they are currently at and how they can proceed moving forward.

MANAGING SECURITY IN THE MARITIME SUPPLY CHAIN

Managing cyber security and ensuring cyber resilience in the maritime supply chain is a complex endeavour. The maritime industry has a very unique landscape compared to land-based sectors. Cyber security practices in the maritime industry are greatly affected by multiple factors such as the use of legacy systems for both ships and shore-based facilities, the intricacy of connectivity systems on board vessels which are often designed in vulnerable states due to organisations trying to cut costs, and it is the intricate design of these systems that also often create vulnerabilities and become attractive attack points for cybercriminals.

According to reports by the maritime cyber security solutions provider Naval Dome, cyber attacks on operational technology systems have increased by 900% from 2017 to 2020 with substantially more of these incidents becoming unreported.[15] This ends up creating a fragmented ecosystem in terms of threat intelligence and cyber security information. For the industry to develop its technology and operations against cyber threats, and to support organisations in making better decisions in their cyber security policies and procedures, the industry must focus on sharing information regarding cyber threats, incidents, and attempts. In March 2022, the US government passed new legislation that requires national organisations that provide critical infrastructure services to report all cyber incidents to the authorities.[16] This development should be seen by the industry as a precedent toward the collaborative goal of reducing cyber risks for the whole maritime community.

Beyond compliance, the successful implementation of cyber security practices and procedures relies upon their execution on the critical links of the maritime supply chain. The relationships of ship owners, managers, agents, vendors, external parties, and crew members play an important role in how organisations interact and manage these threats. The interfaces between these actors with technology are the areas where cyber security management should be emphasised.

Shipping companies should consider establishing channels of communication and dedicated groups within the organisation to focus on increasing the visibility of their digital assets and operations. Increasing the level of visibility on potential cyber risks also raises the level of awareness within the organisation. This form of engagement within each person supports the focus on the human element being a critical factor in managing the organisation's state of maritime cyber security. Through these channels, organisations should proactively test and improve their cyber security redundancies, continuity plans, and data recovery strategies.

Assessing the state of the organisation's cyber security capabilities through risk assessments, penetration testing, and having ethical hackers launch attacks on the organisation's digital infrastructure can be considered part of the process of cyber security maturity. It is only through continuous improvements and monitoring that any organisation can consider itself ready in the event of a cyber attack. No organisation is truly safe in terms of cyber risks, these cybercriminals will continue to develop new and complex methods for achieving their malicious objectives and it only makes that shipping companies should remain one step ahead.

[15] Maritime Cyber Attacks Increase by 900% in Three Years, Vanguard Media Ltd, published July 2020, extracted from https://www.vanguardngr.com/2020/07/maritime-cyber-attacks-increase-by-900-in-three-years/

[16] H.R.5440 - Cyber Incident Reporting for Critical Infrastructure Act of 2021, US Congress, published September 2021, extracted from https://www.congress.gov/bill/117th-congress/house-bill/5440

GEN-2

CREATING A CULTURE OF AWARENESS AND TRAINING AMONG THE ENTIRE ORGANISATION

Humans are recognised as the weakest link in a digital infrastructure network.[17] The key challenge in establishing safe and secure digital environments has always revolved around human factors. However, humans also present themselves as one of the best solutions in hindering cyber threats.

For an organisation to successfully navigate the digital transformation of the maritime industry would require every person in the whole organisation to have a certain level of digital literacy. This digital literacy is critical because it includes the understanding of how digital environments work and how to properly evaluate digital resources. The development of this form of literacy is a foundational aspect of increasing the cyber security awareness of any organisation.

Shipping companies must focus on applying this concept in building the cyber resilience of their organisation. Creating an environment where the sense of individual responsibility is highlighted plays an important role in how organisations create awareness. At the same time, establishing policies and procedures offer each person a better understanding of the organisation's direction and how they can potentially respond in a coordinated manner should an incident occur.

Conducting regular drills around cyber incident response should focus on ensuring that each team member is knowledgeable of their roles and responsibilities. The delivery of awareness campaigns on cyber security hygiene should also be done frequently to consistently gain the support of the whole organisation. The simulation of realistic digital attacks and practical cyber security response scenarios can also allow for better engagement from each individual and allows companies to identify areas where they can improve, such as in the responsible management of digital devices and network accounts. The opportunity to implement these activities can significantly raise the standard of how the organisation reacts to real life cyber attacks.

Communication will also play a significant role in how companies will ultimately survive these cyber attacks. It is important that there are procedures in place for organisations in creating transparent lines of communication to and from various stakeholders, and ensure that every action is documented to ensure efficient examination and investigation after the incident.

Cyber attacks are constantly evolving and becoming more devious in their workings and, while technical countermeasures will stop the vast majority of attempted attacks, they are intrinsically reactive in their operation. The remainder of the protection relies on staff vigilance, preparedness procedures, and understanding. Weak cyber security in any one of these areas may undermine robustness elsewhere.

Crew education is, therefore, an indispensable component in a well-rounded security strategy: a small investment in training and awareness can prove enormously valuable. Alarmingly, a study conducted in 2018 recorded close to 50% of vessels as having come under cyber attack and a large number of cyber breaches as resulting from individual errors also saw majority of crew reporting that they had never received any cyber training. Some estimates suggest that 50% of ship system disruptions are the result of USB 'abuse', where infected memory sticks or

[17] The human factor in cybersecurity, Security Magazine, published September 2021, extracted from https://www.securitymagazine.com/articles/96009-the-human-factor-in-cybersecurity

mobile devices (including second hand phones) are plugged into the port. Other common cyber weaknesses include easily guessed passwords and responsiveness to phishing.

In bringing Cyber Risk Management into the ISM Code, MSC 428 (98) follows the September 2019 edition of the Tanker Management Self-Assessment (TMSA) scheme and the latest Ship Inspection Report Programme (SIRE) questionnaire to include cyber awareness training in IMO guidelines mandatory requirements.

Users of Inmarsat's Fleet Secure portfolio can ensure their crew is cyber ready with the latest training even before they enter the ship. Developed by Marine Learning Alliance under the guidance of the University of Sunderland and the Institute of Marine Engineering Science and Technology, the Fleet Secure Cyber Awareness training programme contains everything crew needs to know to be aware of vulnerabilities and suspicious online behaviour with best practice guidance. The easy-to-use application-based training can be downloaded on any laptop, tablet or mobile device and used offline to eliminate the need for any additional bandwidth use.

CONTACT

For further information and questions, please contact the Inmarsat Maritime Security Services team
Maritime.Security@inmarsat.com

inmarsat.com

As described in the methodology section, the report is based on Inmarsat's internal GMDSS data which is correct to the best of its knowledge. The report also contains certain assumptions based on this data. These assumptions are made in good faith but are statements of opinion only. The report also contains opinions provided by third parties which may not reflect the views of Inmarsat.

While the information in this document has been prepared in good faith, no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability (howsoever arising) is or will be accepted by the Inmarsat group or any of its officers, employees or agents in relation to the adequacy, accuracy, completeness, reasonableness or fitness for purpose of the information in this document. All and any such responsibility and liability is expressly disclaimed and excluded to the maximum extent permitted by applicable law.