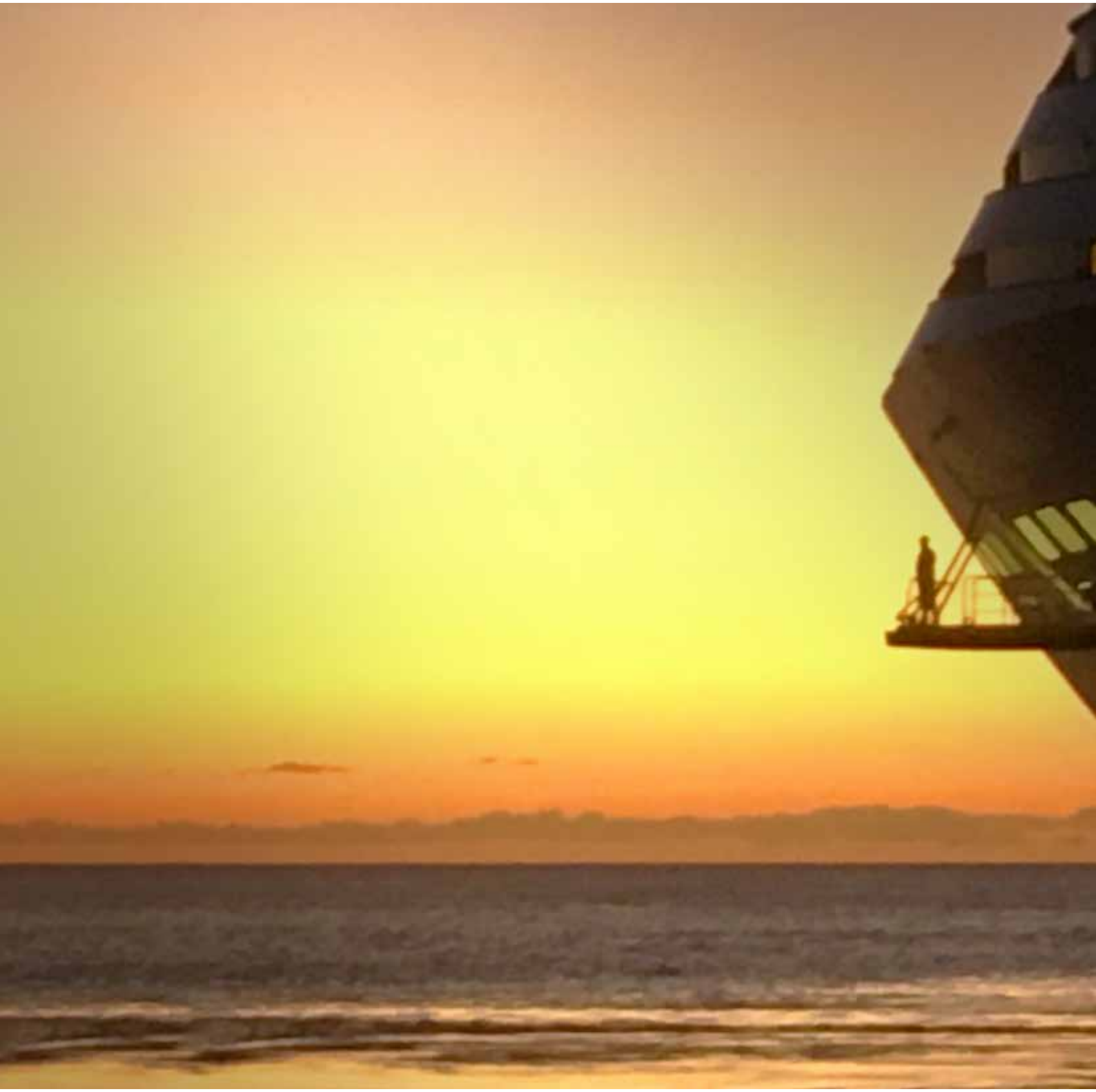
inmarsat
RESEARCH PROGRAMME

CYBER SECURITY

REQUIREMENTS FOR IMO 2021

WHITE PAPER

DECEMBER 2020



CYBER SECURITY
REQUIREMENTS FOR IMO 2021

CONTENTS

01 INTRODUCTION

Developments in connectivity and the transfer of data in greater volumes between ship and shore continue to bring significant gains for passenger experience, operations, fleet management efficiency and crew welfare, but they also increase the vulnerability of critical systems onboard vessels to cyber attacks.

A 2019 IHS Markit/BIMCO report* recorded 58% of respondents to a survey of stakeholders as confirming that cyber security guidelines had been incorporated into their company or fleet by 2018. The increase over the 37% giving this answer in 2017 explained a sharp drop in the number of maritime companies reporting themselves as victims of cyber attacks according to authors – 22% compared to 34%.

However, the enduring feature of cyber threats is their ability to adapt and evolve, with new lines of attack developed as barriers are put in place, and strategies to expose vulnerabilities constantly emerging. A June 2020 White Paper** from the British Ports Association and cyber risk management specialists Astaara suggests that reliance on remote working during the COVID-19 crisis coincided with a fourfold increase in maritime cyber attacks from February onwards, for example.

In fact, cyber security was ranked as the second-highest risk for shipping in 2019, behind natural disasters, according to a survey of over 2,500 risk managers conducted by Allianz.

Given that, according to IBM, companies take on average about 197 days to identify and 69 days to contain a cyber breach, it is clear that an attack on a vessel's critical systems could threaten the safety of a ship as well as the business of operating passenger cruise and ferry services. The fact that a 2019 Data Breach Investigations Report from Verizon indicates that nearly one-third of all data breaches involve phishing provides one indicator that, where cyber vulnerabilities exist, the 'human element' can badly expose them.

The U.S. Coast Guard has already advised ship owners that basic cyber security precautions should include: segmenting networks so that infections cannot spread easily; checking external hardware such as USB memory devices for viruses before connection to sensitive systems; and ensuring that each user on a network is properly defined, with individual passwords and permissions.

From 2021, the Convention for the Safety of Life at Sea that covers 99% of the world's commercial shipping will formalise the approach to cyber security permissible for ships at sea.

By International Maritime Organization (IMO) resolution, no later than a ship's first annual Document of Compliance audit after 1 January 2021, every Safety Management System must be documented as having included cyber risk management, in line with the International Safety Management Code.

The following report offers ship owners and managers guidance covering their responsibilities under the new IMO regime and explains how the cyber security solution Fleet Secure Endpoint provides a comprehensive tool to support them towards compliance.

* Safety at Sea and BIMCO cyber security white paper. Downloadable at: https://www.bimco.org/-/media/bimco/about-us-and-our-members/publications/ebooks/cyber-security-guidelines-2018.ashx

** Managing Ports' Cyber Risks: https://www.britishports.org.uk/system/files/documents/bpa_astaara_white_paper_0.pdf

02
CYBER RISK MANAGEMENT - THE THREAT TO SHIPS

One description of cyber risk management used by IMO sees it as "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".

The description draws on wording developed by the National Institute of Standards and Technology (NIST) of the US Department of Commerce for Cyber Supply Chain Risk Management (C-SCRM). In full, NIST explains C-SCRM as the process of identifying, assessing and mitigating the risks associated with the distributed and interconnected nature of data-centric information technology (IT) systems and the operational technology (OT) systems monitoring events, processes and devices. It is a process which 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, as perpetrators can include:

- **Terrorism**
- **Hacktivists groups**
- **Nation states**
- **Insider attacks**
- **Cyber criminals**

While all of the above involve 'bad actors', many attacks are also automated and their source is not immediately apparent: they succeed by repeated or multiple probing for weaknesses in an organisation's systems or by individual acts of carelessness by those having access to them. In addition, cyber security can be vulnerable where 'threats' are non-adversarial (e.g. software maintenance, or any activity involving connectivity for a third party onboard).

Effective cyber risk management must therefore consider not only multiple cyber assailants but: diverse lines of attack (targeted and random); continuous efforts by assailants to update strategies including malicious coding; and vulnerabilities in hardware, software and human behaviour.

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, organizational policy/processes.
- External: e.g. weaknesses to supply chain/ within entities in supply chain, dependencies (power, communications, transportation, etc.).

In 2017, NotPetya ransomware found a point of entry to the Maersk logistics network via its container terminals business. 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. Also reported, although in less detail, has been a suspected malware attack that brought the Mediterranean Shipping Company website and portal to a standstill in April 2020.

SHIP THREATS AND VULNERABILITIES

These incidents are in the public domain and involve the land-side systems managed by two of the most sophisticated shipping and logistics organisations in the world, both of which place a premium on public profile.

However, ships themselves increasingly play a fully connected data-centric role in the supply chain. In doing so, common cyber vulnerabilities can be found onboard existing ships, and on some new-build ships. These may 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

If these vulnerabilities are well-known, it is also widely recognised that incidents onboard are under-reported. Furthermore, a hallmark of successful cyber crime will be a lack of publicity. In fact, the full extent of the incidents affecting shipping is therefore hard to gauge. In one alleged incident, a ballast water management system cyber breach saw a ship heeled, with control only returned to the crew after a ransom was paid. However, the owner apparently preferred to leave the matter unreported, subsequently denying the whole episode over concerns that the ship would not be accepted for charter.

It is nonetheless fair to point out that – for the connected ship – the vulnerabilities listed above are not simply exposed to the same spread of cyber threats as land-based counterparts: they are also subject to the General Data Protection Regulation (GDPR). Effective in EU jurisdictions from 2018, GDPR requires businesses to demonstrate sufficient control and protection over the data they own - especially if they subsequently have a breach. Failure to comply can bring fines of up to 4 per cent of an organisation's global turnover or £17.5m, whichever is higher.

With more devices on board, and more applications and media channels being used than ever before, some ships are doubling their data usage every six months according to an Inmarsat analysis of its more than 10,000 Fleet Xpress customer vessels. The need for cyber resilience has therefore never been greater.

HARDWARE, SOFTWARE AND PERSONNEL

Understandably, the ship at sea is not itself likely to be the focus for 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 second types of vulnerability relate to 'the human element', and specifically to weaknesses in cyber resilience brought by shortcomings in procedures, training and awareness among personnel.

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

- Claims against interruption to operations, e.g., a virus affecting onboard systems 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 passenger and employee information

SYSTEMIC VULNERABILITIES

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

03
THE BASIS FOR IMO 2021

To be approved as IMO-compliant, after 1 January 2021 every ship's Safety Management System MUST include a Cyber Security Plan. However, some will be unfamiliar with the rationale driving 'IMO 2021'.

Regulators have aligned the provisions with International Safety Management Code (ISM Code) guidelines to ensure that companies and their employees, on ship and shore, observe the Convention of the Safety of Life at Sea (SOLAS). The ISM Code requires all identified risks to ships, personnel and the environment to be assessed and appropriate safeguards to be established.

IMO sees it as the responsibility of the ship owner/manager to "Identify, Protect, Detect, Respond [to] and Recover [from]" cyber attacks through the preparation of cyber security planning that can be audited as part of a ship's Safety Management System. These functional elements can be explained as:

- **Identify**: Develop the understanding to manage cyber security risk. Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.
- **Protect**: Safeguard to ensure delivery of critical infrastructure services. Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.
- **Detect**: Develop and implement activities necessary to detect and identify the occurrence of a cyber-event in a timely manner.
- **Respond**: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired in the event of a detected cyber security breach/cyber-event.
- **Recover**: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event. Maintain plans for resilience and to restore all that was impaired by the cyber security event.

Guidelines on Cyber Security Onboard Ships Version 2.0 were produced with input and support from a joint maritime industry working group whose members include BIMCO, Cruise Lines International Association (CLIA), International Chamber of Shipping (ICS), International Association of Dry Cargo Shipowners (INTERCARGO), International Association of Independent Tanker Owners (INTERTANKO), International Union of Maritime Insurance (IUMI) and Oil Companies International Marine Forum (OCIMF). These guidelines describe ship cyber security as "an inherent part of the safety and security culture necessary for the safe and efficient operation of the ship". The guidelines are addressed to senior management ashore and onboard personnel alike.

The following section offers guidance on what 'IMO 2021' means in practice for owners.

04
IMO 2021 IN PRACTICE

By IMO resolution (**MSC.428(98)**), no later than a ship's first annual Document of Compliance verification after 1 January 2021, any ship's Safety Management System (SMS) will need to take account of cyber risk management to secure Flag State approval, in accordance with the ISM Code.

The Cyber Security Onboard Ships Version 2.0 Guidelines note that chapter 8 of the International Ship and Port Security Code obliges ships to conduct security assessments, which should include all operations that are important to protect. They 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".

The objective of a ship's Safety Management System (SMS), meanwhile, 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.

To verify that companies have adequately and appropriately implemented and incorporated appropriate cyber risk mitigation into their SMS, internal and external audits are required in accordance with the ISM Code. Routine examinations would verify that a management system includes cyber risk management with a cursory review of the system's documentation.

Achieving and documenting compliance relies on ship owners and ships to 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.

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:

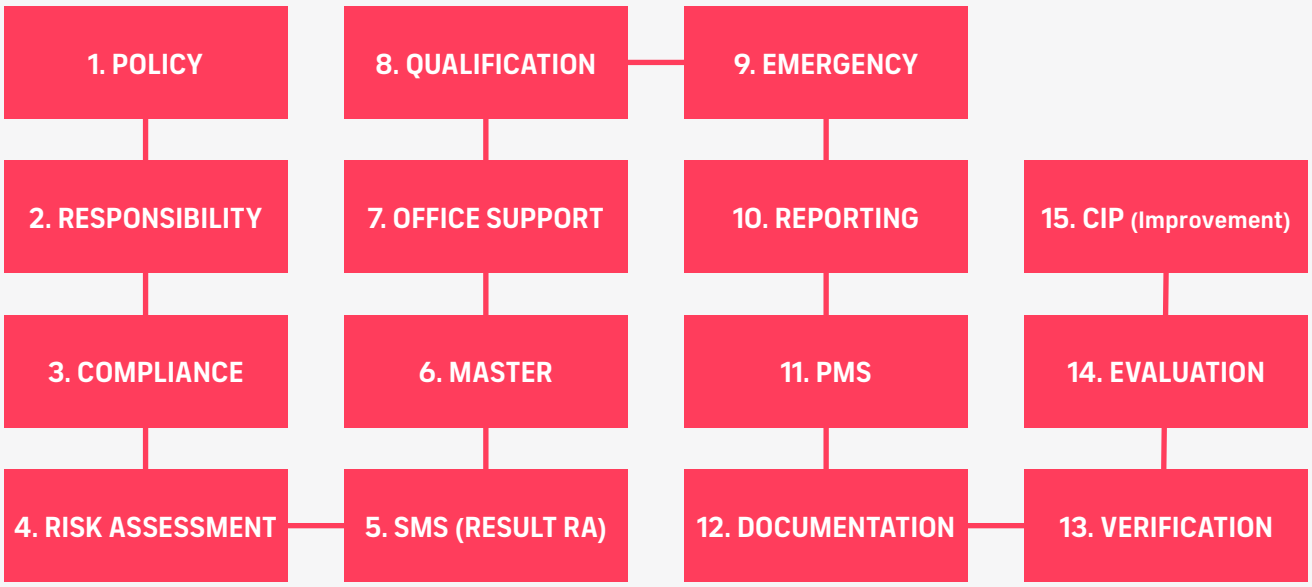
- IT and OT systems
- Intentional and unintentional threats
- Identify – Protect – Detect – Respond – Recover
- International best practices – ISO and EN standards

This is all-embracing, and the modular concept of the ISM Code is also 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' holder must consider their own cyber risks and implement necessary measures in their SMS.

ISM CODE CYBER SECURITY PROCESS (SOURCE: DEUTSCHE FLAGGE – ISM CYBER SECURITY 2018)



Incorporating cyber risk into the SMS can take several months, depending on the complexity of the systems onboard the vessel involved. Meeting the 2021 deadline, or the first inspection thereafter will require a combination of technical mitigations, revised (or new) procedures and staff/crew training to develop a practical and cost-effective route to compliance.

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 be considered by owners as a 'live' document that is regularly updated and improved as risks evolve.

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 establish 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 & Engineering details.

In terms of response and recovery, it is also the owner's/manager's responsibility to formalise the workarounds that address cyber security gaps, so that the ship can continue to operate in the event of a cyber attack or its aftermath, or risks can be mitigated. Workaround plans for critical systems and processes should be 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 Document of Compliance 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') will 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 will identify 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 minimize the impact if a threat is actualised

Given that, 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

The Fleet ICT Manager will need to work with the Head of Crewing to ensure that 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.

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
- 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.

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 organization.

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

05
IMO 2021 COMPLIANCE

Managing cyber risk onboard ship 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.

The owner/manager 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

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

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 ship network protection 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.

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 organization, 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.

06
FLEET SECURE ENDPOINT - AN INTRODUCTION

Inmarsat's objective is to deliver cyber resilient digital services and mission-critical communications to its global maritime customers. It does so by:

- Embedding threat-based risk management into Inmarsat systems, products and services
- Delivering operational resilience by identifying, managing and responding to cyber threats with people, process and technology capabilities
- Fostering a culture where Inmarsat people embrace security and where threat-based security measures are embedded in their day-to-day working
- Sustaining a demonstrable framework for effective, efficient, and adaptable threat-based cyber risk management

Day to day protection of Inmarsat's Information Systems infrastructure is the responsibility of the Security Operations Team. Inmarsat has instituted an in-house 24/7 Cyber Security Operations capability that collaborates actively with the cyber security intelligence community as well as Cyber Security, our partners and maritime customers to tackle cyber threats and manage incidents.

SECURITY AND ENDPOINTS

Security devices such as Unified Threat Management/Next Generation Firewall sit at the ship network level, where they detect and protect against attacks commonly made from shore to ship and vice versa. However, while network monitoring will display a detailed view of the vessel's IT infrastructure, it will not have any jurisdiction over the endpoint, meaning that endpoints such as business-essential PCs and crew laptops remain at risk.

Traditional anti-virus solutions were not really designed to prevent the sort of sophisticated and targeted malware that has become the mainstay of today's maritime cyber threat landscape. They were conceived around a machine-centric view of security and worked by scanning and quarantining suspicious files to prevent them from being launched and were not geared to offer protection against attacks launched on a machine from its host network.

Conventional AV software requires constant updates of new signature files to remain current. Having only one security feature to protect the endpoint will rely heavily rely on a signature set by one security vendor and, in many cases, individual security vendors will not catch 100% of malware. To maintain integrity, a full system scan would also be required after every update, which would often slow the machine's performance to a crawl and frustrate end-users.

If no or lower forms of security is installed on the endpoint, then it is at risk of infection even if the ship network is protected by a security device. For example, someone plugging a USB into the computer can infect it even without clicking anything. If a network security device is being used, then it may recognize the device is infected but cannot clean the infection.

With new variations of malware emerging almost daily, no single vendor was able to keep up and include all new signatures in their database. Cyber criminals preference for the latest iterations shows they know this and actively exploit the lag between new malware being detected, a signature being developed, and an update being issued and installed.

Inmarsat Fleet Secure Endpoint avoids many of these shortcomings as it was built from scratch with a network-centric view of security in mind but targets endpoints. Endpoint protection is a crucial step to ensuring layered protection and not just relying on firewalls, company policies, and network security devices to be the saving grace for security.

FLEET SECURE ENDPOINT ONBOARD

Fleet Secure Endpoint provides an extension of security to all endpoints on a vessel and delivers several security functions in a single managed service which protects everything from business essential PCs to crew laptops. Fleet Secure Endpoint can be applied to multiple Inmarsat maritime services – Fleet Xpress, FleetBroadband, and Fleet One.

Fleet Secure Endpoint scans the network for security issues and records its findings, providing an auditable trail covering alerts and network status. Its reach extends to any new devices joining the network. Whilst Fleet Secure Endpoint itself does not deliver IMO 2021 compliance, it provides the ship owner and ship manager with a cyber security solution that facilitates and supports compliance.

MORE THAN ANTI-VIRUS
Standard anti-virus is no longer adequate protection

	GENERIC ANTI-VIRUS (Bitdefender, Symantec, etc.)	ENDPOINT PROTECTION (ESET Protection)	FLEET SECURE ENDPOINT
Anti-Virus (Anti-Spyware, Anti-Phishing)	✓	✓	✓
Web control		✓	✓
Two-way firewall		✓	✓
Botnet protection		✓	✓
Ransomware prevention		✓	✓
Multi-engine scanning			✓
Network monitoring			✓
Asset inventory (software, hardware, driver, etc.)			✓
Endpoint health status alerting			✓
Endpoint threat alerting			✓

07
FLEET SECURE ENDPOINT AND FLEET XPRESS - SUPPORTING IMO 2021 COMPLIANCE

Fleet Secure has been designed to align with IMO's five pillars for cyber resilience, namely: identify; detect; protect; respond; and recover, while its reporting function has been developed with IMO compliance in mind. In addition, an ISO 27001 audit of Fleet Secure Endpoint conducted by DNV GL describes Fleet Secure Endpoint as a single product which can assist in achieving IMO 2021 compliance. Although Fleet Secure Endpoint works across all of Inmarsat's maritime services, to maximise protection and compliance Fleet Secure Endpoint should be used in conjunction with Fleet Xpress, which provides reliable high-speed internet access with the ability to separate crew and business traffic and make it easier to respond to and recover from attacks.

IDENTIFY

Fleet Secure highlights where errors and warnings have occurred in the vessel/fleet, which enables the designated security personnel to quickly ascertain potential weak spots that require further investigation. It does this using a powerful network scanning and monitoring module, called Teyla, that automatically detects devices on the local network and checks whether Fleet Secure Endpoint is installed. If not endpoints will be marked as 'rogue nodes' and alerts are raised as an alert. The designated security officer can either allow or deny network access privileges to that device.

This oversight means someone on the vessel is always aware of what is connected to their network. To aid network audits, on machines where installed, Fleet Secure Endpoint will also collect data on installed software, hardware and system configuration.

PROTECT

Fleet Secure Endpoint is built around ESET Endpoint Security, an award-winning enterprise-grade endpoint security product, and has special adaptations for use in a maritime setting. It not only detects and blocks files with known signatures from operating but monitors low-level system calls and actively analyses software for suspicious behaviour **in real time**.

- **Botnet protection** shuts down malicious connections to known botnets. Botnets hijack a machine without the owner's knowledge to carry out Distributed Denial of Service (DDOS) attacks. When activated, they consume processing power and cause spikes in bandwidth consumption.
- **Multi-engine scanning** broadens detection by using malware signature databases from multiple security vendors so that new fingerprints not known by all vendors are included during inspection.
- **Ransomware prevention** detects and prevents malicious encryption attempts before they have a chance to initiate and encrypt the device.
- **Two-way endpoint firewall** blocks malicious incoming and outgoing network traffic.
- **Anti-spyware** terminates malicious applications designed to steal sensitive information.
- **Anti-phishing** blocks connections to sites known to extract confidential user information.
- **Web control** allows the system administrator granular control over the websites users can visit.
- **Endpoint Threat alerting** sends an email notification to the system administrator listing recently detected threats on vessels.

RESPOND

Knowing how to react during and after a cyber-incident is critical to a well-rounded cyber security strategy. It is necessary to envisage a wide range of potential scenarios and plan the steps needed, to contain their impact on vessel operation and safety and secondly to restore impaired systems and recover data in a timely fashion.

Fleet Secure Endpoint can assist the response stage in several ways. In contrast to off-the-shelf products, the service is enhanced by round-the-clock monitoring by a dedicated team of IT experts based in the Inmarsat Security Operating Centre, who check security events or other signs of unusual network activity on a vessel as and when they occur. They are supported by marine engineers with extensive knowledge of different hardware and software systems found on modern vessels.

Via the portal, the ship owner's in-house IT team can roll out updates in real-time, quickly and remotely to all computers installed with Fleet Secure Endpoint in the wake of an incident, in order to prevent an attack spreading across the fleet and reduce exposure to similar attacks in the future.

Additionally, the shore-based portal retains a centralised log of all flagged security events and allows bespoke alerts to be created. For example, alerts can be set up to warn when a certain virus or class of virus is detected or certain software requires updating.

The **asset management** functionality incorporated into Fleet Secure Endpoint gives offers a clear overview to designated security personnel and IT staff of which devices are onboard and which devices have Fleet Secure Endpoint installed. It also provides detailed information on assets and the software environment available for responding to an incident and for analysis during the post-incident review.

- Alerting offers pro-active insight on what is happening on board and helps react to incidents
- Alerts can be created to E-mail the user when events happen on board, such as virus detections or outdated software
- A single agent handles all Fleet Secure Endpoint related activities and multiple software packages are not needed, saving system resources
- A 24/7 Security Operations Centre takes action when needed

RECOVERY

If an infection is detected onboard, Fleet Secure Endpoint will automatically detect the infection and respond by blocking it, removing it and finally reporting it. The built-in memory analysis will detect both known threats and new security vulnerabilities. If Fleet Secure Endpoint recognises a file to be malicious, it will be stored in a dedicated quarantine location on the device. Quarantined files are stored in a location that ensures the malicious file cannot infect the system.

Once a security incident has been brought under control and the immediate threat has been neutralised, attention shifts to restoring and reconnecting systems needed for normal vessel operation. Work also begins on investigating the exact cause of the incident and taking measures to prevent a recurrence or similar event from taking place elsewhere in the fleet.

REPORTING

Fleet Secure Endpoint comes with extensive **built-in reporting functionality** which can help in this exercise. A full report can be created on the vessel, containing a record of all devices connected to the network, their hardware and the software that is installed. This report can be given to port state control and/or authorities to show them the vessel has been taking adequate steps to minimise cyber security risks on board. While Fleet Secure Endpoint implementation does not by itself achieve compliance, Fleet Secure Endpoint **reporting** is fully **IMO compliant**.

The Fleet Secure Endpoint Security report shows the following:

- Network connected devices with Fleet Secure Endpoint installed, devices without Fleet Secure Endpoint installed
- System specifications such as free disk space, CPU and amount of memory
- Installed software and their version
- Security events such as neutralized viruses and blocked USB drives
- Acknowledgements of the Security Operations Centre team based on security events

Reports are generated in formats like PDF and can be printed onboard so that the master of the vessel can circulate them among staff and easily integrate

them into a vessel's safety management manual, or show port inspectors that steps have taken steps to protect the vessel and its assets. Even if a vessel has not been the target of an attack, Inmarsat recommends that these reports are periodically reviewed to steer ongoing improvements to a vessel's cyber risk management plan. Any Cyber Review in the Change Management Process should

- Include ICT staff when making major changes in ship's system
- Ensure Cyber Security is considered in the end-to-end process when supplying new equipment

MANAGEABILITY

Using the **Fleet Secure web portal** the ship operator/owner can remotely upload configurations to be implemented onboard so that Fleet Secure Endpoint can be configured remotely. The user can also configure alerts to reflect owner/operator preferences, so that events such as virus detections or blocked network attacks are also flagged up.

In common with any proposed solution, **Fleet Secure Endpoint will only assist in reaching IMO compliance when correctly implemented**: this means the risk assessment needs to have been completed, while the Fleet Secure Endpoint monthly report will included in the Safety Management Manual.

FLEET SECURE ENDPOINT - 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 organization, 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.

4. Fleet Secure Endpoint helps you, as a ship owner/manager to:

- **Step 1 Know What you have**: Fleet Secure Endpoint includes a module logging any new hardware added to your network.
- **Step 2 Defend what you have**: via strong AV, WebControl, Network Monitoring.
- **Step 3 Recover** – Fleet Secure Endpoint's crew training module covers a significant part of the training needs demanded for IMO 2021 Compliance.

FLEET SECURE ENDPOINT KEY FEATURES AND BENEFITS":

- No additional hardware is required. Protections are primarily introduced at the network level, with 'lightweight' software installed on the end-user machines to handle updates and communicate system status back to the server PC
- Multi-layered security. In addition to anti-virus, Fleet Secure Endpoint features anti-phishing, anti-spyware and botnet protection among other features
- Enhanced network oversight: Fleet Secure Endpoint includes sophisticated remote network monitoring of endpoints
- Remote monitoring and auditing: Shore-based portal lets in-house IT teams keep track of all security events, set up alerts and remotely roll-out configuration updates
- 24/7 Security Operations Centre: Fleet Secure Endpoint is supported by a dedicated team of trained cyber security experts and marine engineers, with engineers having been onboard vessels and so fully aware of the environment
- Low bandwidth consumption: Averages only 7Mb data per vessel per week, with lower options available on request (for vessels that are at always-on connection with no data limit the data usage is higher)
- Tailored for maritime: One server located on the vessel to manage all endpoints

08
FLEET SECURE ENDPOINT - INSTALLATION AND USE

Despite its superior scope and functionality, Fleet Secure Endpoint is as straightforward for the user's ICT team to install as conventional anti-virus software developed by Inmarsat to protect ship systems (AmosConnect AV and Globe AV).

FLEET SECURE ENDPOINT INSTALLATION

For a standard vessel network and under normal circumstances, and taking account of safety guidance offered by vendors, the installation can be expected to be completed on clean computers in approximately two hours.

The clean computer provides the optimum case for any anti-virus software installation. However, pre-existing anti-virus software can present challenges and the user's ICT team will need to remove it before Fleet Secure Endpoint is installed. Inmarsat provides user guides/scripts to support the removal of third-party anti-virus software.

Even so, it should be emphasised that there is no requirement for the ship network to stop working in order to install or operate Fleet Secure Endpoint. Fleet Secure Endpoint has a built-in firewall, where ports can be opened for the most commonly used applications on board.

The Inmarsat Security Operations Centre offers oversight for internet-connected ships to support installation and the removal of old systems.

FLEET SECURE ENDPOINT IN USE

Once installed on a device, Fleet Secure Endpoint will start reporting to the web portal. The web portal can then be used to view elements such as (but not limited to):

- Installed software
- Running windows services
- How long the system has been running
- Device hardware, such as remaining hard drive space, type of processor, etc.
- Which operating system the device is using

The portal has two versions, namely ship and shore. With the ship version, all activities performed onboard can be accessed, including holding download files for clients manuals and mapping out of all endpoints onboard the vessel. However, the shore side portal holds detailed information such as events and alerts for the fleet and also for each vessel. The IT team of the vessel or fleet will have access to the shore side portal.

It is also possible to view the results of the network scans performed onboard and see which devices do or do not have Fleet Secure Endpoint installed. For the devices that have Fleet Secure Endpoint installed advanced logging is available, allowing users to see things such as (but not limited to):

- Firewall logs (when an attack or an event happens which triggers the firewall)
- Device control logs (when USBs were inserted, whether they were blocked)
- URL blocker logs (whether sites were blocked)

DASHBOARD AND ALERTING

The Fleet Secure Endpoint web portal can be used to view events that occur on the vessel and configure alerts based on those occurrences. Alerts will notify the user or multiple users via E-mail. The user can configure alerts for events such as (but not limited to):

- Virus threats (receive a notification if a virus is detected)
- Firewall events (receive a notification when an attack/event happens which triggers the firewall)
- When a new device has been detected on the network that does not have Fleet Secure Endpoint installed
- Software version control (receive an alert when a new version of installed software is available)
- User intrusion detection (receive an alert when a failed login occurs)

Multiple OS Fleet Secure Endpoint supports

multiple operating systems. For Windows operating systems, Vista and up is supported. OSX, Linux and their mobile counterparts IOS and Android are also supported.

Fleet Secure Endpoint is distinguished from Endpoint Detection & Response (EDR) packages. While these solutions are highly effective, they demand strict ship networking setup to 'signature' and check every file on the vessel, consuming huge amounts of data. Fleet Secure Endpoint addresses attacks and infections without needing to signature each file, saving on costs and data usage. In fact, Fleet Secure Endpoint frequency and control reporting times can be adjusted, with data usage as low as 7MB a month. Where ships have internet connectivity, Inmarsat recommends more frequent reporting of network status so that its security operation centre can take swift action when malicious traffic is detected.

In addition, Fleet Secure Endpoint can be used onboard vessels using FleetBroadband as their connectivity solution. In this case, trench rules need to be set correctly and onboard firewalls (if any) must be updated to accommodate Fleet Secure Endpoint IPs and port numbers.

FLEET SECURE ENDPOINT USE IN CONTEXT

As noted earlier, Fleet Secure Endpoint installation provides a route towards IMO 2021 compliance, rather than offering a complete compliance solution. However, in summary IMO 2021 can be achieved using Fleet Secure Endpoint and its cyber security reporting/response functionality covers all of the IMO 2021 guidelines into the ship's Safety Management Manual.

Scenario: a crew member opens a phishing email

The Fleet Secure Endpoint response:

- **Scenario 1**: If Fleet Secure Endpoint is fully updated then it should detect that virus.
- **1.1**: The Inmarsat Security Operations Centre is notified of this activity.
- **Scenario 2**: Fleet Secure Endpoint is not updated, the virus is not detected, and the ransomware process is not stopped.
- **2.1**: The Inmarsat Security Operations Centre is notified of this activity.
- **Scenario 3**: The firewall in Fleet Secure Endpoint introduces segmentation of the network so that the virus cannot spread to other PCs as they block the incoming attack.

Fleet Secure Endpoint handles all of these scenarios automatically. An option is also available to block out an endpoint from the network remotely.

09
CYBER SECURITY, CREW TRAINING AND AWARENESS

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 2018 Futurenautics survey that recorded 47% of vessels as having come under cyber attack and 80% of cyber breaches as resulting from individual errors also saw 85% 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 mobile devices (including secondhand 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 latest Ship Inspection Report Programme (SIRE) questionnaire to include cyber awareness training in IMO guidelines mandatory requirements.

Inmarsat has been one of the partners contributing to a Maritime Cyber Security Awareness training course developed for Stapleton International by MLA College, which is available to users of Fleet Secure Endpoint at a discounted rate. Using a combination of video modules, transcripts and a concluding test, the course has been developed in accordance with BIMCO, IMO, ICS and IACS guidelines and has been approved by the Institute of Maritime Engineers, Science and Technology and the University of Sunderland, UK. It is also in line with the provisions of TSMA self-assessment.

Uniquely, the course is deliverable by an app for download through Google Play and AppStore to smartphones, tablets and laptops, after which it can be accessed offline. Guidance based on the full extent of IMO Cyber Awareness expectation can therefore be learned during voyages without the need for scheduled classroom training during busy port stopovers, or even connectivity whilst at sea.

Focusing on the basics of cyber security for the maritime user, the course is suitable for all levels ashore and at sea, enabling seafarers to familiarise themselves with attacks they are likely to encounter in their day-to-day duties. It also offers practical tips on how to avoid becoming a victim or endangering their vessel.

Each 30-minute training module covers:

- Digital threats using personal information
- Digital threats using IT devices
- The physical and human threat
- Final competency test and completion certificate

Subject to achieving a score of 80% from 20 randomised questions, seafarers receive a certificate valid for four months from the University of Sunderland and a certificate of Continuing Professional Development from the Institute of Marine Engineering, Science and Technology.

By completing this course, all personnel will be able to further understand the principles and actions they must adhere to, thus ensuring that they are fully compliant with IMO regulations. It will also help allay the fears of many within the sector and ensure that they remain cyber safe at sea.

10
FLEET SECURE ENDPOINT - REAL CASE STUDIES

CASE 1

Vessel type: Undisclosed

Assailant: Multiple infections with normal anti-virus installed

The customer was using Palo Alto cyber security software when the vessel was hit by multiple infections, including Trojans, Worms and data exfiltration viruses infesting the system. The customer decided to install Fleet Secure Endpoint as part of a shipboard trial. Inmarsat's engineer found 79 infections that had not previously been detected.

Among the significant findings, the HTTP Filter detected users onboard unknowingly visiting websites serving malicious code. The connection was dropped, and the user informed accordingly. Again, the Fleet Secure Endpoint email filter detected infected attachments, including:

- CoinMiner.T trojan (A trojan which uses system resources to mine cryptocurrency for its distributor)
- TrojanDownloader.Agent.OJL trojan (a trojan capable of downloading and executing other malicious code)
- Agent.AQ trojan (A trojan agent template frequently used as a starting point for malicious code that can be modified to do whatever the malicious actor wants)

The Fleet Secure Endpoint email filter disposed of these infections, preventing further infections.

CASE 2

Vessel type: Liquid Ethylene Gas Carrier

Assailant: Emotet trojan, causing vessel operations to stop

Emotet is well-known as a trojan in banking circles but was detected as infecting the majority of machines onboard a LEG Carrier, becoming active whenever a PC was switched on. The virus can intercept and exfiltrate data transmitted and saved when the user is browsing banking websites, resulting in leakage of sensitive data and malicious use of the user's banking details.

As part of a Fleet Xpress agreement, the ship was equipped with two Fleet Secure Endpoint security modules, installed across all PCs onboard:

- **Advanced Memory Scanner** – This detected Emotet in the memory, terminated and blocked it from recurring.
- **Heuristic Intrusion Prevent System (HIPS)** – This detected the malicious code being executed and stopped the execution of this code.

The virus was successfully cleared from the memory on all infected devices.

CASE 3

Vessel type: Undisclosed

Assailant: Sohanad worm

A USB memory stick infected with the NCB worm Sohanad was connected to an endpoint onboard ship. Sohanad spreads via removable media and shared folders: once it has infected any part of the network, it tries to replicate itself by infecting applications and files.

Two Fleet Secure Endpoint security modules were implemented:

- **Real-time file system protection** – Detected that files were being infected and automatically halted the process from accessing files so it could be investigated by the engine.
- **Heuristic Intrusion Prevent System (HIPS)** - Detected the malicious code that was causing the replication and stopped the execution of this code.

Fleet Secure Endpoint was able to stop the infection from continuing, cleaning 17,000 infections in the process.

CASE 4

Vessel type: Bulk carrier

Assailant: CoinMiner

The vessel in question had trialled Fleet Secure Endpoint. After the trial's conclusion, the ship ran for two months without Fleet Secure Endpoint. On re-installation of Fleet Secure Endpoint, all devices onboard that were tested were found to have been infected with a CoinMiner. CoinMiners use a device's processing power to mine cryptocurrency for the attacker without the user's knowledge.

Fleet Secure Endpoint was able to neutralise all threats.

11
NEXT STEPS - HOW TO PROCEED

CYBER RESILIENCE FOR IMO 2021 – NEXT STEPS
HOW TO PROCEED WITH FLEET SECURE ENDPOINT

APPOINT	Appoint a person on board for cyber security planning for IMO requirements
REVIEW	Review and check Cyber Security Plan against guidance on onboard ICT covering communication and ship networks for business/crew
PURCHASE FLEET SECURE ENDPOINT	Purchase Fleet Secure Endpoint – one month free trial available
PREPARE	Remove any existing anti-virus software on each endpoint
DOWNLOAD	Download and run the installer
SET-UP	Set-up dashboard, manage reports
CREW TRAINING	Crew to complete MLA e-learning module, records kept for compliance purposes
REPEAT	Repeat crew cyber awareness training annually – periodic threat intelligence offered via Fleet Secure Endpoint

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

inmarsat.com