Company Cyber Security Procedures

IMO Resolution (MSC.428(98)) stipulates 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.

IMO Resolution (MSC.428(98)) stipulates 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 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.

For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this procedure.

Scope of Procedure

In order 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. This procedure applies to all your employees, contractors, volunteers and anyone who has permanent or temporary access to your systems and hardware.

Considerations - Risk Management

MSC-FAL.1/Circ.3 – Guidelines, provides high-level recommendations for maritime cyber risk management, and can be incorporated into any existing risk management processes and are complementary to the safety and security management practices. 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:

- Technical such as software defects or outdated or unpatched systems
- Design such as access management, unmanaged network interconnections
- Implementation errors for example misconfigured firewalls
- Procedural or other user errors
- Procedure

Ships are increasingly using systems that rely on digitisation, digitalisation, integration, and automation, which call for complete cyber risk management on board. As technology continues to develop, information technology (IT) and operational technology (OT) onboard ships are being networked together – and more frequently connected to the cloud/ internet.

This brings a far greater risk of unauthorised access or malicious attacks to ships' eco-systems and networks. Risks may also occur from personnel accessing systems on board, for example by introducing malware via removable media such as flash drives/USB sticks.

Transferring data introduces security risk. Companies must ensure that their infrastructure and systems are secure and meet with the provisions of IMO Resolution MSC.428(98) / MSC-FAL.1/Circ.3, in so far as ensuring that these measures are built within their Safety Management System.

The Voyager system is designed to help protect against threats faced by shipping companies today.

The Voyager PC Healthcheck application scans the PC to check that virus protection is up to date and the PC is not unnecessarily exposed to security risks.

How Voyager supports cyber security onboard

For additional peace of mind, the Voyager system is designed to help protect against threats faced by shipping companies today**.** It provides essential security capabilities to help protect both people and assets in the face of emerging strategic and operational business challenges.

Voyager PC Healthcheck

Protection on board starts at the point of ship's connectivity which is usually the vessel's PC. With cyber threats on the increase and continually evolving, there is an increasing need to monitor and analyse system activity to identify and prevent attempted incursions.

Our **Voyager PC HEALTH CHECK** application helps protect the on board PC by bringing together lots of tools in one comprehensive programme that identifies the security vulnerabilities and configuration issues.

Secure transfer of data to ECDIS with V-Drive

USB/flashdrive has evolved as the most common way to move data from the connected PC back of the bridge to the ECDIS to help keep the front of bridge environment secure.

The dedicated V-DRIVE USB provides a very simple way to manage AVCS updates and protect the ECDIS from malware.

Navigating officers simply plug the V-Drive into a USB port on their Voyager PC to automatically download and transfer all necessary ENCs, updates, permits and, new for Version 8, the Route file, required to navigate safely and compliantly to the VDrive so that it can uploaded in the ECDIS.

For more secure updating, the V-Drive is automatically reformatted every time it is plugged into the Voyager PC and reloaded with updates to remove any existing content and help prevent the transfer of malware to the ECDIS.

Voyager Worldwide also provides whitelist IPs to enable external connectivity on bridge PCs and laptops to be locked down while still accessing all of the secure Voyager Worldwide data services in the Voyager CLOUD.

Voyager within Safety and Security Management processes

The following may be referenced in a customer's Safety and Security Management processes for the use of Voyager and V-Drive:

- Voyager Worldwide Private and Public infrastructure is fully hosted in highly secure datacentres behind full managed firewalls.
- Voyager Worldwide Private and Public infrastructure is fully protected by the latest Virus definitions and security updates.
- Voyager Worldwide conduct regular external penetration tests on our IT systems and web services.
- Voyager PLANNING STATION connects to the Voyager Worldwide servers and downloads updates and other information via a secure connection.
- Voyager updates are encrypted and compressed before transmission then decompressed and decrypted by our on-board Voyager software.
- The Voyager update data that Voyager Worldwide supplies is fully tested prior to live distribution to vessels.
- V-Drive ENC updating process, formats the USB stick before any data transfer to ECDIS and there is a secure USB option to lock the USB to prevent any inappropriate use of removable media. (2.1.6 of MSC-FAL.1/

The dedicated V-DRIVE USB helps protect the ECDIS from the risk of malware.

Voyager Worldwide's Private and Public infrastructure is fully hosted in highly secure datacentres behind full managed firewalls and protected by the latest virus definitions.

Voyager Worldwide conduct regular external penetration tests on the IT systems and web services that support vessels worldwide.

Circ.3)

Whilst Voyager Worldwide endeavour to provide secure data it is highly recommended that our customers also implement sufficient IT security protection on-board vessels and ashore. We can ensure the data we provide is Virus free but we cannot take responsibility for Antivirus threats from other sources from an onboard network and equipment.

Maritime Cyber Security Awareness Training – MCA approved

As an additional support to shipping company

customers, Voyager Worldwide has partnered with the team at Be Cyber Aware at Sea to provide cyber security awareness training for the Maritime and Offshore industries. This course is aimed at one of the biggest vulnerabilities on board, 'The Human Element' and helps to develop an understanding and awareness of the emerging cyber threat.

www.becyberawareatsea.com

Voyager Worldwide's 3i Cyber

Voyager 3i Cyber Security Framework

Security Framework is a simple and memorable way to help both improve understanding of cyber security and develop best practice.

In defending against any threat, it is good practice to have more than a single measure. Cyber security is no exception. For this reason the Voyager 3i Framework is based upon a layered approach with each of the elements and measures working in combination to form a robust, yet easily understandable, strategy to achieve effective cyber security protection.

The Framework comprises three main elements of people, process and technology, supported by the measures of inform, implement and integrate.

The Framework also provides six simple steps that everyone can take to significantly reduce the risk posed by cyber security threats long before the need to invest in professional support or high-technology. It also helps make individuals, organisations and systems more resilient.

Promote cyber security awareness for everyone

Cyber security, like first aid, firefighting or watertight integrity is everyone's responsibility – a whole ship activity. Simple measures, employed by all can go a long way to preventing costly, and sometimes dangerous, cyber security problems.

Control access

Physically and through strong passwords, controlled access to IT systems, supported by policies and processes, ensures that they are only used by those authorised to use them, for the purposes they are intended, in a way that they should be used.

Back up data (in more than one place)

Backing up critical data prevents its loss and puts it beyond the reach of cyber-criminal ransomware. If you have accessible copies of your data in different locations, you turn a catastrophe into an inconvenience.

Always use a firewall as an outer layer of defence

Firewalls can be used to decide whether to allow or block traffic and often represent the first line of technological defence, providing a hardware or software barrier between secured and controlled networks and untrusted outside networks such as the internet.

Keep your systems and software up to date

Modern business software and anti-virus programs feature regular updates which should always be downloaded and run – they are useless if not implemented – and can be set to 'auto-update' on trusted systems.

Think before you click. Does it look right?

The 'WannaCry' ransomware attack demonstrates the need to think twice before clicking on anything that is not familiar. If it doesn't look right, don't click on it and seek advice from an IT professional or delete it.

Systematic Vulnerabilities

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

- Bridge systems
- Cargo handling and management systems
- Propulsion and machinery management and

power control systems
- Access control systems
- Passenger servicing and management systems
- Passenger facing public networks
- Administrative and crew welfare systems
- Communication systems

The Compliance Checklist

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.

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.

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 and back-up all documentation and files 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.

Conclusion

Cyber Security and cyber-resilience on-board vessels is ultimately the responsibility of the shipping company to ensure that their IT departments implement sufficient firewall, network and antivirus security as defined in the ISM Code and that these measures are covered in their safety and security management system. Acquiring the proper cyber risk coverage to ensure that catastrophic security failures don't capsize the business is part of the digital resilience equation that company's must adopt.

About Voyager Worldwide

Voyager Worldwide is a leading maritime solutions company and the world's number one provider of digital navigation solutions.

Uniquely, we use data intelligence to help our customers buy the navigational products and solutions they need with precision and accuracy that also helps them to reduce costs and improve efficiency.

We work with the biggest names in shipping worldwide - large and small. We have a powerful Voyager ecosystem that collects data from vessels and enables that data to be shared with shore-based stakeholders. We also collect, store and analyse millions of other data-points ranging from AIS positions to Port State Authority and Flag State data every day.

Since 2015 we have captured over 1.6bn data points relating to 120,000 vessels worldwide. This data forms a huge Voyager Worldwide data lake that through the help of our analytics and our Voyager FLEET INSIGHT web service, our customers then use to help them manage navigation (and increasingly) other aspects of their operations more effectively. Our goal is to turn data into information and information into insight.

Our Voyager NAVIGATION as a SERVICE product enables you to buy navigation supplies at cost price – so we have an unambiguous shared objective not to sell you more than you ever need. Since launch in mid 2019, Voyager NaaS has become the preferred way to buy ENCs for thousands of ships worldwide and has delivered an average of 31% savings on navigation spend – by providing the data analytics and software that shipping companies need to identify and buy exactly the products vessels need - at lowest possible prices.

To find out more contact your preferred Voyager worldwide office from the list below or email us at customerservices@voyagerww.com. Alternatively, visit our web site at

www.voyagerww.com

Germany
Hamburg
T: +49 40 374811 00

Greece
Athens
T: +30 216 400 5000

Japan
Kobe
T: +81 78 332 3422
Yokohama
T: +81 45 650 1380

Hong Kong
T: +852 2854 3688

Turkey
Istanbul
T: +90 216 493 7401

Singapore
T: +65 6270 4060

UK
Aberdeen
T: +44 1224 595 045
North Shields
T: +44 191 257 2217

USA
California
T: +1 562 590 8744