Issue 2
April 2021

Managing Cyber Risk

Support for Vessel Operators

A whitepaper by

Sperrymarine
the navigation experts

Maritime Cyber Risk Management

In 2017, the International Maritime Organization (IMO) adopted resolution MSC.428(98) on **Maritime Cyber Risk Management in Safety Management Systems** (SMS). This resolution required the SMS to consider cyber risk management in accordance with the objectives and functional requirements of the International Safety Management (ISM) Code. In particular, the IMO Resolution encourages administrations to ensure that cyber risks are appropriately addressed in the SMS. In the same year, IMO also approved **Guidelines on Maritime Cyber Risk Management** set out in MSC-FAL.1/Circ.3. These in turn reference the **Guidelines on Cyber Security Onboard Ships** produced and maintained by BIMCO and others which explain how cyber risks should be managed in a shipping context.

Support for Vessel Operators

This whitepaper has been prepared to assist ship owners and operators in their assessment of the cyber risk exposure of a vessel with respect to the navigational and other bridge equipment supplied by Sperry Marine. It is intended to help ship owners and operators develop appropriate protection and mitigation strategies and thereby reduce the likelihood of vulnerabilities being exploited, and the impact of any such exploit, to an acceptable level. Vessels carry both Information Technology (IT) and Operational Technology (OT) systems - this Whitepaper has a focus on OT systems and addresses Navigation equipment in particular.

The Sperry Marine Approach

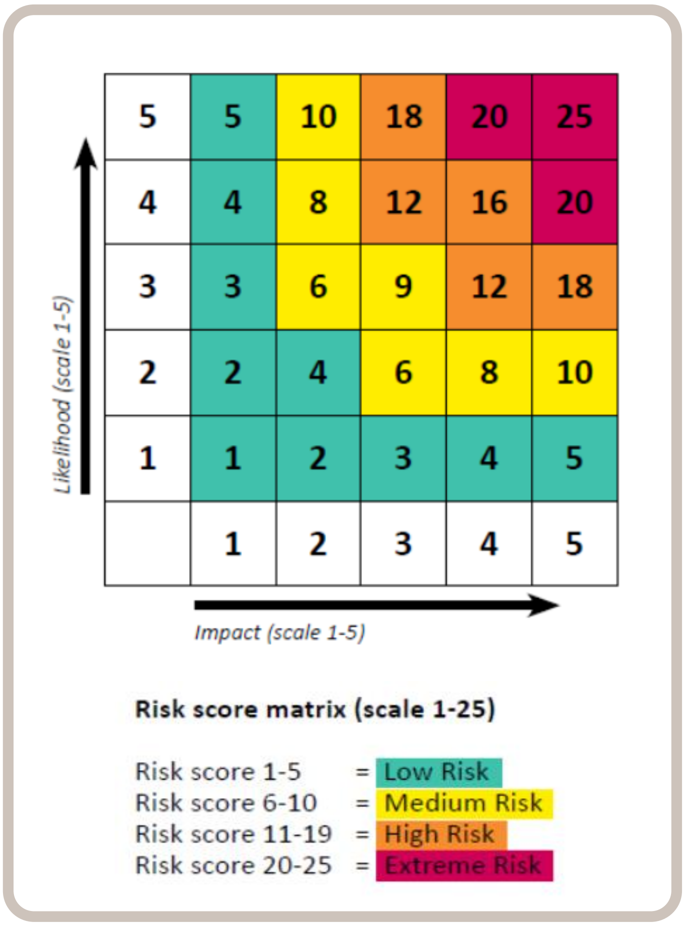
At Sperry Marine, we draw on a considerable knowledgebase to guide the deployment of cyber-resilient solutions and this includes our parent organisation, Northrop Grumman - the leading high-end cybersecurity provider to the US Federal Government. The services of third-party security organisations are used when needed. Sperry Marine’s approach to cyber resilience is one of Defence in Depth – involving physical, technical and procedural defences. Cyber risks are managed through the delivery of secure systems, including design, deployment, operation and maintenance, a resilient supply chain, and a secure and resilient infrastructure (https://www.sperrymarine.com/cyber). We are committed to embedding a culture of awareness within our organisation to ensure that cyber risks are managed through the delivery of secure systems. We continually review and develop our procedures to ensure that our cyber maturity is developing to match emerging threats.

Sperry Marine have received Cyber Essentials Plus certification from a National Cyber Security Centre (NCSC) approved accreditor.

From an organisational standpoint, Sperry Marine's Business Systems are designed around Confidentiality, Integrity and Availability and, as well as the external Cyber Essentials Plus certification, we operate to our own high internal Corporate Standards. Contingency measures in the form of Business Continuity Plans (BCP) and Business Resumption Plans (BRP) are in place in the event of a significant disruptive event.

Assessing the Risk

The guidelines published by BIMCO et al. offer a tool for assessment of the severity of a cyber-risk. The tool uses a matrix, reproduced below, to calculate the risk of a cyber-security event through assessment of its *Likelihood* and *Impact*. The *Likelihood* of a cyber-security event happening is determined by the product of the *threat* and the *vulnerability*. Thus, if either of these two factors is close to non-existent, so will the Likelihood be. If the *initial risk* calculated is above what is acceptable, the risk will need to be further mitigated for the *residual risk* to reach an acceptable level.



Likelihood (scale 1-5)
Impact (scale 1-5)

5	5	10	18	20	25
4	4	8	12	16	20
3	3	6	9	12	18
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5

Risk score matrix (scale 1-25)

Risk score 1-5	=	Low Risk
Risk score 6-10	=	Medium Risk
Risk score 11-19	=	High Risk
Risk score 20-25	=	Extreme Risk

The *Threats* identified, and the factors used, will depend on a range of issues including:

- The exact nature of the system under consideration
- The environment in which it is installed
- The physical layout of the vessel
- The vessel's operating procedures

Sperry Marine recognise that any approach to cyber risk management is both company and vessel specific. Any assessment of the Threats and Mitigations set out in the table below should be tailored to reflect company procedures and the specific equipment carried on board.

Mitigating the Threats

The information below is intended to assist vessel operator when assessing the potential threats and, as mentioned earlier, is focussed on the Navigation Equipment within an OT system. The risk assessment for a particular vessel will depend on the exact equipment carried, the physical environment and the procedures in place, as well as which mitigations are in place.

Attack vector	Threat	Mitigation
Network interfaces	Network interfaces between the IT and Navigation OT networks offer a potential attack vector that could allow threat actors outside the secure area, and potentially off the vessel, to gain access to the OT system. Such access can be used for a range of purposes, including the gathering of confidential data, the distribution of malware, or reconfiguring the system in such a way that it does not operate as designed.	Network equipment should be located in a secure area with cable runs being protected from unauthorised access. Unauthorised network equipment should not be connected to the navigation system. This includes unauthorised wireless access points and mobile devices. Equipment in the navigation system supplied by Sperry Marine should only be reconfigured by authorised Marine Service Engineers. Where a VDR includes a network interface to the vessel's IT network, particular care should be taken to ensure the interface is appropriately secured. Sperry Marine offer SperrySphere’s Secure Maritime Gateway that provides secure communication between the IT & OT networks.
Serial interfaces	If a threat actor was to gain physical access to the Navigation OT system, the serial data flow between sensors and other navigation equipment could be caused to fail, be intercepted or be spoofed (Man-in-the-middle attack). Effects range from incorrect sensor data being received to complete loss of sensor data (e.g. failure of position, speed, depth). Commands to the autopilot could also be impacted.	Areas containing sensitive equipment should be secure, with cable runs being protected from unauthorised access.
USB ports and removable media	External devices connected by USB may contain malware that prevents the navigation system from functioning correctly, or at all. Once present on a system, malware may propagate over network interfaces from one system to another. (See Malware, below.) USB ports may be used by crew members to charge external devices, risking Electromagnetic compatibility issues and damage to the Navigation OT system.	Unauthorised devices (e.g. mobile phones) should not be plugged into ports on navigation equipment. Authorised devices should be restricted to a specific use, kept in a secure area and scanned for malware before use . SperrySphere's *Connected ECDIS* capability allows delivery of charts and transfer of routes without the use of removable USB devices.

Attack vector	Threat	Mitigation
Malware	Malware may be injected onto the system through the above interfaces. It may propagate over a network interface from one part of the system to another. The malware may prevent the system from operating as designed. Effects may include a breach of the Confidentiality, Integrity or Availability of data on the system.	Sperry Marine regularly review the security updates available for the Operating Systems used by our products for applicability and incorporates these into software updates. Sperry Marine's Service Agreements provide an arrangement for ensuring that the system and software are kept up to date. Sperry Marine assess the Windows Group Policy and registry settings used by VisionMaster and compare these against recognised benchmarks used within the cyber security industry, with role-specific tailoring. This results in vulnerable protocols being disabled; unused operating system features being removed; hardening of the network stack; and unnecessary system services being identified and deactivated. USB ports are prevented from running executable files when external drives are inserted. Sperry Marine will be adding real-time anti-malware scanning to VisionMaster software in a future release, increasing the defences deployed. Anti-malware procedures described in the User Guide should be followed. Only authorised Marine Service Engineers trained in and practicing appropriate cyber security measures should be used to maintain the equipment.
Electronic Navigational Chart(ENC) data	ENC data received by the vessel may be unofficial. Such data may lack the quality assurance of charts issued by official Hydrographic Offices. The ENC and Nautical Publication delivery system may be intercepted by threat actors and the data substituted with compromised data, impacting safe navigation.	Unofficial hydrographic data is indicated as such on VisionMaster's user interface. When IHO S-57 ENC charts are in use they should be encrypted using the IHO S-63 Data Protection Scheme. Charts and Nautical Publications should be delivered securely to the vessel through a service provided by an authorised distributor. SperrySphere's *Connected ECDIS* capability allows delivery of charts without the use of removable USB devices. Delivery on read-only media (e.g. DVD) provides an additional level of protection against tampering.

Attack vector	Threat	Mitigation
User reconfiguration	The navigation equipment may be reconfigured by a threat actor in such a way that it does not operate as designed. The navigation equipment may be reconfigured, inadvertently or deliberately, by a threat actor in such a way that it loses cyber hardening.	Sperry Marine apply a system lockdown strategy that prevents the equipment, including application software, operating system and firmware as applicable, from unauthorised access. As a result, the operational software is incorporated into the equipment in such a way that the navigator cannot augment, amend or erase it. Only authorised Marine Service Engineers trained in installing, commissioning and maintaining the equipment should be used. The equipment should be left in the standard operational mode after maintenance.
User data import	User data files can be imported into VisionMaster. Examples of such data files includes routes, parallel index lines and clearing lines. Such data, if malformed (inadvertently or deliberately) could cause the equipment to malfunction or fail. Such data, if tampered with (inadvertently or deliberately) could impact safe navigation.	VisionMaster performs data validation which protects against the import of malformed data. Removable devices used for data import should be authorised for this purpose, restricted to this specific use and stored in a secure area.
AIS VHF interface	AIS data received over VHF is, by design, neither encrypted nor authenticated and may be subject to interruption, jamming or spoofing. Data intentionally transmitted by other vessels may not be correct.	Mariners should be trained to understand the risks and limitations received from the AIS and should cross-check with alternative sources of data. Radar target tracking provides an alternative that uses sensors onboard own ship and is not impacted by compromised data sent from other vessels.
GNSS/RNSS	Satellite positioning systems may be subject to jamming or spoofing impacting own ship's position and velocity.	Where two sources of positioning are available, VisionMaster will automatically indicate when a discrepancy exists. The mariner may use radar overlay to help detect position discrepancies on an ECDIS. The mariner may use the ECDIS Line of Position capability to fix own ship's position. Sperry Marine are also able to offer positioning systems that counteract the effects of deliberate spoofing.

Cyber Secure System Design

Business requirements for improved operational efficiency, economy and safety increasingly result in a need for the integration of on-board systems. It's important that this integration adequately considers cyber security, ensuring that the Information Security goals of Confidentiality, Integrity and Availability are not compromised. This is where Security by Design is important, ensuring that cyber security is considered from the earliest stages of the definition of the system architecture.

Sperry Marine's system integration experience is wide-ranging and includes systems such as CCTV, special-purpose radars and third-party software packages. We ensure the cyber risk is considered from the outset, resulting in a secure solution for the vessel particularly when both IT and OT networks are involved. Sperry Marine can provide support to the vessel allowing a full cyber security assessment to be made by the vessel's IT professionals. This may include the provision of information such as network architecture diagrams, associated data flows and protocols and support to vessels undergoing vulnerability assessment by cyber security experts.

Class Societies play an increasingly important role in demonstrating that a vessel has met or exceeded the goals of IMO Resolution MSC.428(98). Examples include DNV's three Cyber Secure class qualifiers assigned through the allocation of Security Profiles; Lloyds Register's Cyber Security ShipRight Procedures which evaluate "Design & Build Procedures" or "Operational Procedures" to assign one of four Capability Levels; and the American Bureau of Shipping's range of Cybersafety Notations. Sperry Marine are able to provide support to vessels that have particular class requirements.

Global Service Network

Incident Prevention through Software Maintenance

Sperry Marine's Maintenance Contracts provide an arrangement that, as well as helping to reduce the total cost of ownership, also helps to mitigate the cyber-risk by delivering software updates to address emerging vulnerabilities. There are a range of service contracts, and all options can include training and reports if required:

- Fixed-price coverage of navigation and communication equipment, including Sperry Marine and other vendor equipment
- Fixed-price management fee per vessel, plus time and material for service
- Customised plans for certain equipment and scopes of work

Sperry Marine's global service network ensures that wherever a vessel finds itself, there is a Sperry Marine service team nearby, cutting the time to respond and recover.

Incident Response

Vessels should have a cyber-Incident Response plan in place to respond effectively to security incidents. This plan should include regular back-up of all operational data to allow restoration after an incident.

Sperry Marine's Global Service Network is available to act as part of a Incident Response plan, with the goal of ensuring the vessel returns safe and secure operation as quickly as possible.

If you think that your system may have been subject to a cyber-incident, contact Sperry Marine's Global Service Network as soon as practical. Cyber incidents can also be reported via Sperry Marine’s public web site: https://www.sperrymarine.com/contact/customer-feedback.

SperrySphere

SperrySphere is Sperry Marine’s family of digital ship support, navigation and vessel performance solutions that is built around increased connectivity and a ship-based and shore-side platform infrastructure. From safe navigation, regulatory compliance, vessel performance and risk mitigation to remote access, maintenance & assistance, this platform enables safer, greener and more efficient vessel operations. SperrySphere’s **Connected ECDIS** and the **SperrySphere Workstation** can be used as part of a cyber-risk mitigation strategy to counter the risks associated with USB transfer when transferring electronic charts to the ECDIS and when exchanging routes with the ECDIS.

Cyber security is an essential aspect of SperrySphere and the security features of the **SperrySphere Workstation** and **Secure Maritime Gateway** are described below.

- Security by design
- Consistent security profiles
- Security maintained throughout the lifecycle

SperrySphere Workstation

The **SperrySphere Workstation** is situated on the vessel’s IT Network and communicates with the OT Navigation Network via the **Secure Maritime Gateway**. Cyber security is provided through the application of the UK National Cyber Security Centre (NCSC) “End user device (EUD) security guidance”. Security features provided include:

- Applications securely deployed using Microsoft Endpoint Manager
- SperrySphere cloud services comply with NIST SP 800-171
- Access to the BIOS/UEFI is password protected
- Secure Boot is enabled
- Charts are encrypted in transit
- Standard Windows event logs are maintained for analysis purposes
- A Mobile Device Management strategy is used to ensure that the System, device and user configuration policies are correctly and consistently applied, enforced and updated as required
- Accounts are password protected
- Passwords comply with Microsoft password policy
- The disc drive is encrypted, ensuring that data is encrypted at rest
- Real-time malware scans with automatic download and installation of updates
- Automatic download and installation of security updates is configured
- Windows applications run as a Standard User (limited privileges)
- USB ports are prevented from running executable files when external drives are inserted

Secure Maritime Gateway

The Secure Maritime Gateway, designed to the requirements of IEC 61162-460 “Digital interfaces: Ethernet interconnection – Safety and security”, provides network segregation between the IT Network and the OT Navigation Network. The device provides the mariner with a secure network share within its DMZ where data can be passed between the two networks (for example the transfer of charts or exchange of routes). It can also host software to automatically download charts from a chart distributor. The gateway has been security hardened in accordance with best practice recommended by the Linux community and tailored using Centre for Internet Security (CIS) benchmarks. Security features provided include:

- Accounts are password protected
- Access to the BIOS/UEFI is password protected
- Strong passwords are used through the system
- Real-time malware scans with automatic download and installation of updates
- The disc drive is encrypted, ensuring that data is encrypted at rest
- Secure Boot is configured
- Network-facing services run inside heavily restricted and isolated environments (e.g. separate namespace, mandatory access controls, read-only file systems)
- Windows applications run as a Standard User (limited privileges)
- Automatic download and installation of security updates is configured
- Standard Windows and Linux event logs are maintained for analysis purposes
- Secure Boot ensures only trusted software can boot on the machine
- Trusted Execution Technology protects against software-based attacks aimed at stealing sensitive information by corrupting system or BIOS code

Bibliography

- IMO MSC-FAL.1/Circ.3 - Guidelines On Maritime Cyber Risk Management
- IMO Resolution MSC.428(98) - Maritime Cyber Risk Management In Safety Management Systems
- The Guidelines on Cyber Security Onboard Ships - BIMCO et al.
- Cyber Security Workbook for On Board Ship Use - BIMCO, ICS and Witherby Publishing Group
- DCSA Implementation Guide for Cyber Security on Vessels - The Digital Container Shipping Association
- VisionMaster FT Cyber Protection (MIB 222) - Northrop Grumman Sperry Marine
- IEC 61162-460:2018 - Digital interfaces: Ethernet interconnection – Safety and security
- National Cyber Security Centre - End user device (EUD) security guidance
- Center for Information Security: CIS Benchmarks®
- NIST Special Publication 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems

Safe, Secure, Compliant
Solutions from Sperry Marine

The Navigation Experts

118 Burlington Road, New Malden, Surrey, KT3 4NR England
Phone +44 (0) 20 8329 2000