The IMCA HSSE Security Committee continues to work to raise awareness of security issues that can potentially harm member companies. The HSSE Security Committee concerns itself with two main areas. The first and main focus is 'traditional' maritime security, the threat posed to our members' crews and ships, from piracy, criminality or terrorism. The second is the more general threat of cyber security, which potentially affects us all - all individuals and all organisations.

Information provided in this regular Security Bulletin is intended to be used by members to either directly pass on to employees or use the material it contains as part of an existing company security awareness programme.

# Cybersecurity Briefing

## 1 Unified Requirements for Cyber Security – E26 and E27

The International Association of Classification Societies (IACS) has recently published new unified requirements for cyber security: E26 and E27. These will be mandatory for classed ships and offshore installations contracted for construction on or after 1 January 2024. This will have implications for IMCA members.

The new requirements will cover:

- Scope of applicability, including operational technology (OT, as distinct from IT – information technology) systems for important vessel functions;
- Identification and protection against cyber threats;
- Detection of incidents;
- Means to respond and recover;
- Hardening and security capabilities of systems and components.

**E26 Cyber resilience of ships**: the introduction notes that *"interconnection of computer systems on ships, together with the widespread use onboard of commercial-off-the-shelf (COTS) products, opens the possibility for attacks to affect personnel data, human safety, the safety of the ship, and threaten the marine environment. Attackers may target any combination of people and technology to achieve their aim, wherever there is a network connection or any other interface between onboard systems and the external world. Safeguarding ships, and shipping in general, from current and emerging threats involves a range of measures that are continually evolving. It is then necessary to establish a common set of minimum functional and performance criteria to deliver a ship that can indeed be described as cyber resilient."* IACS considers that minimum requirements applied consistently to the full threat surface using a goal-based approach is necessary to make cyber resilient ships. See https://iacs.org.uk/download/14104

**E27 Cyber resilience of on-board systems and equipment:** the introduction notes that *"technological evolution of vessels, ports, container terminals, etc. and increased reliance upon Operational Technology (OT) and Information Technology (IT) has created an increased possibility of cyber-attacks to affect business, personnel data, human safety and the safety of the ship*" as well as possibly a threat to the marine environment. Safeguarding shipping from current and emerging threats must involve a range of controls that are continually evolving; this would require incorporating security features in equipment and systems at design and manufacturing stage. IACS considers that it will be necessary to establish a common set of minimum requirements to deliver systems and equipment that can be described as cyber resilient and goes on to specify unified requirements for cyber resilience of on-board systems and equipment in E27. See https://iacs.org.uk/download/14105

## 2 The NIS2 Directive: "A High Common Level of Cybersecurity in the EU"

The original Network and Information Security (NIS1) Directive was the first piece of EU-wide legislation on cybersecurity, and its specific aim was to achieve a high common level of cybersecurity across EU member states. For a number of reasons, its implementation proved difficult. To respond to the growing threats posed with digitalisation and the surge in cyber-attacks, the European Commission has submitted a proposal to replace and strengthen the NIS Directive and thereby strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU.

On 16 January 2023, the Directive (EU) 2022/2555 (known as NIS2) entered into force replacing the earlier NIS1 directive. The NIS2 directive can be found here. Member States now have until 17 October 2024, to transpose its measures into national law.

There is a widened scope of application of this directive with a potentially large impact for some countries. The Security committee considers that the expansion in scope of the applicability of the new Network and Information Security directive could have an impact on the operations of IMCA members.

Affected organisations will need to implement "*appropriate and proportionate technical and organisational security measures to manage the risks posed by network and information systems*" and will also find that senior management becomes accountable for ensuring that the security standards deployed by their organisation are sufficient, through approving the risk management measures that are in place and having oversight over their implementation.

See also NIS 2.0—the EU looks to bolster its cybersecurity laws - Lexology

For more information, please contact Nick.Hough@imca-int.com