An introduction to EU cybersecurity risk management regulation of the maritime industry (EU-NIS 2).

By: Andy Watkin-Child & Peter Thornton MBE

September 2023

THE AUGUSTA GROUP

HILL DICKINSON

Executive summary

New European Union (EU) cybersecurity regulations are of particular interest to management boards of companies designated (or potentially designated in the future) as Operators of Critical National Infrastructure (CNI), Operators of Essential Services (OES) or similar. The measures required under the updated EU regulations will need to be considered well in advance of compliance deadlines if companies are to avoid disruption to their trade due to inadequate cybersecurity certification leading to service suspension and/or fines.

In January 2023 year the EU Network and Information Systems (NIS) 2.0 Directive[1] ("NIS 2") came into effect requiring EU Member States to implement new cyber-security laws by October 2024. NIS 2 is a regulation that has a significant effect on the cybersecurity risk management of the maritime sector.

In March 2023 the UK Government published updated guidance[2] for board members to govern cyber risk more effectively and announced that the UK's 2018 Network and Information Systems Regulations (NIS Regulations) will be updated and strengthened. This will include creating a new power to designate critical suppliers or services and will also provide a discretionary power to take appropriate and proportionate measures to secure such critical dependencies[3].

The US Securities and Exchange Commission (SEC) released its final rule on cybersecurity risk management on July 26th 2023, that is effective 5th September 2023. The final rule requires U.S domestic and Foreign Private Issuers (FPI) subject to the Securities and Exchange Act 1934, to disclose material cyber risks and material cyber incidents important to investors, from December 2023. Compelling registrants to report material cyber risk and material cyber incidents to the SEC and provide '*reasonable*' investors with enough information to make valued judgements of the ability of registrant's management to oversight, assure, attest and manage material cyber risk and material cyber incidents and their investor returns.

Across the global maritime industry, there are a several new cyber risk management regulations that require Directors, Officers and accountable executives manage cyber risk and increase their organisations and their personal legal and compliance risks.

Introduction

Global dependence on the maritime transport industry is profound. We rely upon a network of ships, ports and inland distribution centres for the movement of cargo ranging from commodities to personal packages. We rely on oil and gas, and increasingly on wind and waves to provide our energy needs via their associated infrastructure and the marine based communication systems must also not be overlooked. It is well known that around 90% of globally traded goods are carried by sea, a secure marine sector is critical for global trade[4]. As such the maritime sector is justifiably classified by governments as critical to national security and Critical National Infrastructure (CNI).

It is not difficult, therefore, to appreciate the degree of global disruption that can be caused through disabling international cargo and logistics distribution systems or attacking data networks critical to communications and

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&from=EN
[2] Cyber Security Toolkit for Boards - NCSC.GOV.UK
[3] Government response to the call for views on proposals to improve the UK's cyber resilience - GOV.UK (www.gov.uk)
[4] https://www.oecd.org/ocean/topics/ocean-shipping/#:~:text=The%20main%20transport%20mode%20for,are%20carried%20over%20the%20waves.

security. Cyber-attacks have already impacted the maritime sector; the 2017 Maersk cyber-attack demonstrated the effect of a cyberattack on the container industry, costing the firm up to $300 million[5]; CMA CGM was hit by a cyber-attack targeting customer information in 2020[6] and 2021[7]; the IMO suffered a cyber-attack in 2020[8]; Tokyo MoU reported it was affected by a cyber-attack in July 2022[9]; DNV's ShipManager software, used by vessel operators for fleet management was targeted in a ransomware attack in January 2023[10]; the recent attack in April on the US Navy's Marinete Marine Shipyard which halted production[11] and Japan's biggest port Nagoya was hit by a cyber-attack in early July 2023[12]. Are all good reminders of how vulnerable the maritime sector is from cyber-attacks.

In March this year, the EU Agency for cybersecurity (ENISA) published its first cyber threat landscape report dedicated to the transport sector[13]. The report highlights that Ransomware attacks on the transport sector doubled in 2022, more than half of the incidents were linked to cybercriminals seeking to steal money and almost a quarter of attacks were from hacktivists.

The threat of cyber-attacks to CNI is clearly increasing and is driving Governments to enhance cybersecurity regulations, which will require CNI providers to enhance their cybersecurity management.

On a positive note, shipping (specifically ship operations), with such a high level of multi-national dependency, has already been pro-active in establishing enforcement measures to counter cyber-attacks on vessels and their related services. This having been achieved through recommendations flowing from the IMO and subsequent adoption by flag State Administrations to ensure cybersecurity measures are incorporated into Safety Management Systems (SMS). However, of importance to shipping companies' management boards, updates to UK, EU and US cyber regulations to safeguard the services on which nations depend are in motion. These updates will see a move away from nations relying on guidance and persuasion, to the implementation of wider enforcement powers and penalties for infringements.

This article is to highlight the main regulations that are applicable to the maritime sector in the lead up to the revised regulations.

Details of who and how you can contact us for advice are at the side/end of this article.

Chronological of maritime cybersecurity regulations and guidelines

On 1 June 2016 the IMO issued MSC.1/Circ.1526 *Interim Guidelines on Maritime Cyber Risk Management* which highlighted the urgent need to raise awareness on cyber risk threats and vulnerabilities.

On 6 July 2016, EU Directive 2016/1148 *Network and information Systems Directive* ("NIS Directive") came into effect, requiring public and private operators of services in certain sectors to take appropriate security measures

[5] https://www.ft.com/content/a44ede7c-825f-11e7-a4ce-15b2513cb3ff
[6] https://www.reuters.com/article/uk-cma-cgm-cyber-idUKKBN26L2N0
[7] https://www.ship-technology.com/news/cma-cgm-reports-another-cyberattack/
[8] https://www.seatrade-maritime.com/technology/imo-hit-cyber-attack
[9] https://maritime-executive.com/article/tokyo-mou-reports-previously-undisclosed-cyberattack-in-2022
[10] https://www.seatrade-maritime.com/technology/dnv-ransomware-attack-concerning-cyber-threat-analyst
[11] Defending Our Shipbuilding Critical Infrastructure - Center for Maritime Strategy
[12] https://www.japantimes.co.jp/news/2023/07/06/national/nagoya-port-hack-resume-operations/
[13] Understanding Cyber Threats in Transport — ENISA (europa.eu)

and report incidents that significantly impact the continuity of the services they provide. The sectors include energy, transport, banking, financial markets, potable water, healthcare and digital service providers.

On 16 June 2017, the IMO published MSC 428(98) *Maritime Cyber Risk Management in Safety Management Systems* (SMS) which encouraged Administrations to ensure that cyber risks are appropriately addressed in SMS. This was to be achieved no later than the first annual verification of the Company's Document of Compliance after 1 January 2021.

On 5 July 2017, IMO MSC-FAL.1/Circ.3 issued its first version of *Guidelines on Maritime Cyber Risk Management* which is for all organizations in the shipping industry and set out that users should refer to specific Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices.

On 10 May 2018, the UK published SI 2018 No. 506 *The Network and Information Systems Regulations 2018* which defines organisations and companies that are Operators of Essential Services ("OES") under which the water transport subsector is designated. OES must take appropriate and proportionate technical and organisational measures to manage risks and take appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems. In doing so, they must have regard to any relevant guidance issued by the relevant competent authority when carrying out their duties.

As of 1 Jan 2021, vessels whose flag State had adopted MSC 428(98) must have addressed, and have in place, cybersecurity measures integrated into their SMS by their Company's first ISM DOC audit after 1 Jan 2021. In support of this requirement, several articles and guides have been published by industry bodies on how to implement cybersecurity into a company and vessel's SMS. Given that it is now well into 2023, such systems should be well established to counter new threats.

On 9 March 2022, the US Securities and Exchange Commission released a proposal for Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934, which includes UK and EU based foreign issuers. The proposal sets out the requirements of Covered Entities to provide numerous management reports to the SEC that will provide the SEC, investors and other market participants with information on the current management of cybersecurity risks.

On 7 June 2022, MSC-FAL.1/Circ.3/Rev.2 updated the IMO's *Guidelines on Maritime Cyber Risk Management*. Amongst other updates, it highlights the risk associated with companies and organisations operating on interconnecting networks. With the recommendation that cyber risk management should start at the senior management level the paper also provides a selection of industry guidance.

On 17 Jan 2023, EU Directive 2022/2555 NIS 2.0 Directive came into effect requiring Member States to prepare and legislate by 17 October 2024. The revised directive widens and strengthens Member States' powers to enforce compliance and seeks to harmonise the cybersecurity measures between Member States with the help of ENISA. The NIS 2.0 directive forms part of a suite of cyber regulations being developed by the EU to strengthen the resilience of EU Member States CNI. These include NIS 2.0, the *Digital Operational Resilience Act* (DORA 2022/2554) for the financial sector, the Resilience of Critical Entities Directive (EU 2022/2557) for CNI, and the proposed Cyber Resilience Act 2022/0272 (COD) for the security of hardware products and services.

On July 26th 2023 The Securities and Exchange Commissions (SEC) passed the cybersecurity risk management final rule ("final rule" or "rule")[14], that is effective the 5th September 2023 with compliance starts in December 2023. Requiring covered SEC registrants to report their '*material*' cyber risks and '*material'* cyber incidents to the regulator. The SEC cyber rule is both global in scope and industry sector agnostic, setting out requirements for reporting both material cyber risks and material cyber incidents as defined by a '*reasonable*' investor. Cyber risks and cyber incidents that require a registrant to have appropriate cyber risk management processes; governance; reporting and remediation; to identify appropriate board subcommittees; the cyber experience of the management that assess cyber risks and incidents; and the processes by which boards are informed of material cyber risk and incidents.

Highlights from EU NIS 2.0 relating to the maritime sector:

EU NIS 2 Annex 1 lists inland, sea and coastal passenger and freight water transport companies; managing bodies of ports; and operators of vessel traffic services (VTS) as highly critical maritime industry sectors. Annex 1 also brings into scope services providing electricity generation, distribution and transmission (encompassing wind and wave power generation); and oil and gas production, storage, distribution and transmission (encompasses upstream processes including drilling, extraction and storage)[15]. Annex II concerns other Critical Services and identifies the manufacture of transport equipment, which includes the building of passenger and cargo vessels, tankers, tugs, warships, drilling platforms and floating structures[16].

Of particular importance to those service operators is Article 20 which, among other things, directs that Member States shall ensure that the management bodies approve the cybersecurity risk-management measures (see Article 21); oversee its implementation, which includes training at all levels; and can be held liable for infringements. Note also that preamble paragraph (7) opens the door for Member States to identify not just entities that are medium sized and above but also small enterprises and micro-enterprises which fulfil specific criteria that fall within the scope of the directive. Consideration of the critical supply chains identified in Article 22 is also likely to be important here.

The risk-management measures expected of an OES under Article 21 are far reaching and should be based on an all-hazards approach. For example, an OES is to consider state-of-the-art and relevant European and international standards and the degree of the entity's exposure to risks; the entity's size; likelihood of occurrence; and their severity in relation to their societal and economic impact. It is therefore easy to foresee that it will be challenging for an OES to first identify and then subsequently establish suitable measures that will satisfy these wide-ranging considerations.

Article 23 ('*Reporting obligations'*) requires entities to report an early warning within 24 hours of becoming aware of the significant incident to its national Cyber Security Incident Response team (CSIRT), and an update to a national CSIRT within 72 hours. A Significant incident is defined as an incident that causes or is capable of causing severe operational disruption of the services or financial loss for the entity concerned. And/ or it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

[14] https://www.sec.gov/files/rules/final/2023/33-11216.pdf
[15] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:211:0094:0136:en:PDF
[16] https://ec.europa.eu/eurostat/documents/3859598/5902521/KS-RA-07-015-EN.PDF

Lastly, it is important for company management boards to appreciate that Member States' enforcement powers will be stepped up considerably. Measures include establishing a competent authority to have the power to conduct random audits, issue infringement warnings, stipulate remedial actions, suspend services and impose fines.

The Forecast

EU Member States have about 13 months (until October 2024) to implement national laws to satisfy EU NIS 2.0 (as well as the Digital Operational Resilience Act ("DORA")) and it is also expected that the EU will release a proposed Cyber Resilience Act (CRA - 2022/0272) later this year.

Covered markets registrants have 3 months before compliance reporting to the SEC final rule starts (December 2023). The final rule requires registrants to identify board committees or subcommittees responsible for the oversight of material cyber risks and material cyber incidents; publish their cyber risk management processes; the processes by which the board or subcommittees are informed of cyber material risk; management's role in assessing and managing the registrant's material risks; disclose the management positions and the relevant committee members expertise to oversight and assure cyber risks. It is important for such firms in the maritime industry to be well prepared for SEC disclosure. The SEC has a well-defined and tested enforcement program, supported by a Whistleblower regime. Disclosure of material cyber incidents, material cyber risks and oversight, assurance and attestation will be widely reported both to the regulator and investors that will question the effectiveness of compliance and of cybersecurity risk management.

In relation to the prospect of updated UK NIS Regulations, as the industry consultations have now been conducted it is expected that the government will soon implement revised regulations which will broadly be in-line with EU and US standards. In the meantime, by way of UK guidance, on 30 March this year the National Cyber Security Centre updated its Cyber Security Toolkit for Boards. This guide is useful, particularly the section on directors' duties[17] in the UK for keeping up to date with the UK Government's expectations on those responsible for cybersecurity within a company.

Generally, the more robust a shipping company's cybersecurity measures are now, any additional management measures required under NIS 2, US SEC or UK NIS Regulation amendments, the easier they will be to implement. Such measures can be pre-empted to a certain degree by management boards being familiar with the underlying requirements of the directives and proposals, augmented by the IMO and flag State cybersecurity requirements for vessels as well as any other maritime sector codes and industry papers. This in turn, should result in management boards being far less at risk of suffering the consequences of infringing national laws when they come into effect and of course, less likely to be the victim of a major cyber-attack.

Further information on the scope of the EU NIS 2.0 directive for company boards can be found in an article published by Jamie Foster and Andy Watkin-Child earlier this year: *The European Union (EU) Network Information Security Directive 2.0 (EU NIS 2.0): Implementing a high common level of cyber security across the EU* and *Cybersecurity: a compliance issue for boards*.

A selection of maritime industry cybersecurity standards:

- Code of Practice Cybersecurity for Ships produced by the Institution of Engineering and Technology (IET), supported by the Department for Transport (DfT) and the Defence Science and Technology Laboratory (Dstl)

[17] Cyber security regulations and directors' duties in the UK - NCSC.GOV.UK

- The Guidelines on Cybersecurity Onboard Ships produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.
- Consolidated IACS Recommendation on cyber resilience (Rec 166 rev.2)
- IAPH Cybersecurity Guidelines for Ports and Port Facilities