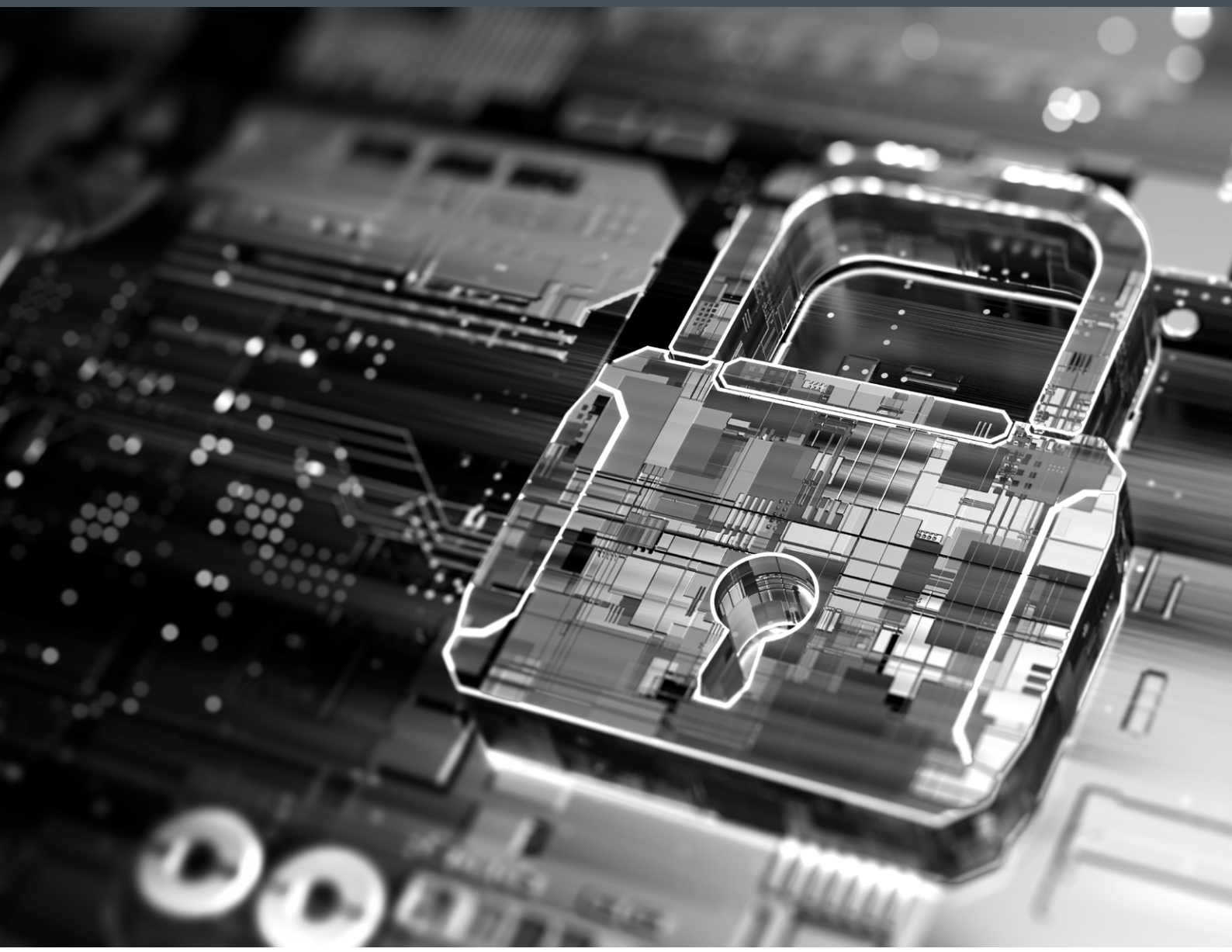

CYBER RISK ADAPTABILITY AND RESPONSIBILITY

For years, service providers to the shipping industry have warned of the industry's increased reliance on cyber technologies and their potential vulnerabilities. Yet, until recently, this perceived threat had not been addressed by lawmakers and, to some degree, operators.

On 16 June 2017, the Maritime Safety Committee (the **MSC**) of the International Maritime Organisation (the **IMO**) adopted Resolution MSC.428(98)[1] on Maritime Cyber Risk Management In Safety Management Systems (the **Resolution**). At the same sitting, the MSC approved and paved the way for Guidelines on Maritime Cyber Risk Management (MSC-FAL.1.Circ.3[2]) (the **Guidelines**), which, on 5 July 2017, replaced their earlier, interim version (MSC.1/Circ.1526). The Resolution and the Guidelines recognise that cyber risks are not merely a technical issue, but must also be addressed in existing safety management systems required by the International Safety Management (**ISM**) Code.

Compliance

The Resolution encourages administrations to include cyber risks management in their assessments of safety management systems, yet fails to clarify whether it is a requirement for administrations. The Resolution itself also provides no guidance on how to satisfy its requirements, but does refer to the Guidelines, which do. The Guidelines, however, provide only high-level recommendations for maritime cyber risk management and guidance on how to conduct an assessment for complying with the Resolution.

Owing to the ambiguity of the Resolution and the Guidelines, we expect implementation of the new standard to vary enormously by flag state. Some administrations, such as the US Coast Guard, have set out stringent enforcement plans which come into force from 1 January 2021 (see the US Coast Guard (the **USCG**) Work Instruction dated 27 October 2020[3]). The USCG will require operators of US flagged ships, and foreign flagged ships that call on US ports (through port state control), to ensure cyber risk management is appropriately addressed in their safety management systems. The UK Maritime and Coastguard Agency (the **UK MCA**), in Marine Information Notice MIN 647 (M)[4], also set out guidance to surveyors on considering cyber security in their ISM audits. For the most part, it confirms which sets of guidelines are acceptable as standards for ship operators to follow.

Given the enforcement of the Resolution also via port state control inspections, the varying standards imposed by different flag states may cause problems to operators. Operators are advised to be aware of this and try to adhere to the highest standard in jurisdictions they trade in.

To help operators, there is further guidance available from industry bodies and organisations. A good example of this includes the Guidelines on Cyber Security Onboard Ships by BIMCO[5]. These were produced with support from Cruise Lines International Association, International Chamber of Shipping, Intercargo and InterManager. The USCG was also consulted on various aspects of these guidelines. Given the cross-industry participation in their drafting, the BIMCO guidelines are considered by many to be the most comprehensive. Accordingly, adherence to them should go some way to ensure compliance with the Resolution and its derivative national legislations. For example, in MIN 647 (M), the UK MCA suggests that the BIMCO guidelines are an acceptable compliance standard. They also refer to the Code of Practice Cyber Security for Ships produced by the Institution of Engineering and Technology (IET), the ISO/IEC 27001 Standard and the Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework).

Third parties and managers

One subject touched upon by the BIMCO Guidelines is ensuring compliance with the new standards by third parties and contractual counterparties:

"Companies should evaluate the cyber risk management processes for both new and existing contracts. It is good practice for the company to define their own minimum set of requirements to manage supply chain or 3rd party risks."

Compliance by counterparties is important to minimise your own cyber risk exposure. A good start to ensuring compliance by counterparties to charterparties is incorporating the BIMCO Cyber Security Clause 2019[6]. The clause, drafted by BIMCO with assistance from HFW, is designed to fulfil the following functions: (i) raise awareness of cyber risks, (ii) provide a mechanism for ensuring that parties have in place procedures and systems to help minimise the risk of a cyber incident happening in the first place, and (iii) ensure that parties mitigate and resolve the effects of an incident when it occurs, while also cooperating to assist each other.

Whilst operators should take into account adherence by counterparties, they need also to ensure that their own obligation to comply with the requirements does not fall between the cracks within their operation. Under BIMCO's standard un-amended technical ship management agreement, SHIPMAN 2009, the technical manager is responsible for compliance with the ISM Code. Operators should review and consider their management arrangements to ensure that cyber risk management is not overlooked and is indeed considered by their managers.

Financing

Under many financing agreements, lenders require shipowners/borrowers to comply, and to procure compliance by the managers, with all provisions of the ISM Code (including obtaining and maintaining valid Documents of Company and Safety Management Certificates, as required). Failure to comply with the maritime cyber risk management elements of the ISM Code can, therefore, put a borrower in default of their financing arrangements. As maritime cyber risk management continues to gain prominence,

1 https://www.register-iri.com/wp-content/uploads/MSC_Resolution_42898.pdf
2 https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf
3 https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/CG-CVC/CVC_MMS/CVC-WI-027(series).pdf
4 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/933785/MIN_647_-_FINAL.pdf
5 https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships
6 https://www.bimco.org/contracts-and-clauses/bimco-clauses/current/cyber-security-clause-2019

“Industry stakeholders must adapt and take individual responsibility for protecting themselves and, thereby, global trade from potential catastrophic disruption that a cyber incident could cause.”

financiers may begin paying specific attention to this at both the financing arrangement and administration stages.

Seaworthiness

Another consequence of the Resolution coming into force is the effect on the relationship between cyber security and seaworthiness. Currently, failure to address cyber risk management may cause a vessel to be deemed unseaworthy. Given the current lack of clarity about the level of due diligence required, however, a claimant would face an uphill battle. Once the Resolution comes into force, the same claimant will be likely to have a much better chance of successfully arguing unseaworthiness, unless an operator can show that it has exercised due diligence in managing cyber risks in accordance with the Regulation. This may then have implications under contracts of carriage and the vessels’ insurances. HFW will soon be publishing a dedicated chapter on the effect of deficiencies in cyber risk management on autonomous vessels’ seaworthiness following Swansea University’s Sixteenth Annual International Colloquium on Disruptive Technologies, Climate Change and Shipping Law.

Insurance

The marine and cyber insurance markets have been offering, for some time, various products to cover shipowners’ exposure against cyber risks. Whilst the majority of marine cyber insurance products focus on business interruption cover, a handful will cover physical damage to vessels/cargo. P&I covers should respond to cyber incidents already, barring the usual exclusions to cover relating to war risks and terrorism.

The ‘new normal’

Industry commentators have warned of marine cyber risks for some time. Industry service providers (such as insurers, surveyors, technical equipment suppliers, etc.) have, also for some time, offered various products to protect ship operators against these risks. The uptake has been limited, however, due to the lack of high profile incidents. In the last few years, there has been a rise in the number of marine cyber incidents, some of which have been very disruptive. This has inspired a renewed interest, not only from commentators and services providers, but also from legislators who are trying to get ahead of the rapidly shifting technological landscape. The Regulation is a positive step that will result in various national legal frameworks addressing these issues. It is unsurprising, however, given the risks are still evolving and extremely varied, that clarity is absent. This is intentional and designed give operators the flexibility to adhere to standards without conflicting with their unique internal processes. Industry stakeholders must adapt and take individual responsibility for protecting themselves and, thereby, global trade from potential catastrophic disruption that a cyber incident could cause.

For more information, please contact the authors of this briefing:

PAUL DEAN
Partner, London
T +44 (0)20 7264 8363
E paul.dean@hfw.com

DENIS NIFONTOV
Associate, London
T +44 (0)20 7264 8092
E denis.nifontov@hfw.com

HFW has over 600 lawyers working in offices across the Americas, Europe, the Middle East and Asia Pacific. For further information about our shipping capabilities, please visit hfw.com/Shipping.

hfw.com

Americas | Europe | Middle East | Asia Pacific