Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

NORTON ROSE FULBRIGHT

Mitigating maritime cyber risks: the legal perspective

Steven Hadwin
Head of Operations, Risk Advisory & Cyber Security
Norton Rose Fulbright LLP
27 July 2017

The changing legal and regulatory landscape

ÅGeneral Data Protection Regulation

- ï Will replace the current framework of data protection law in Europe, which is based on The Data Protection Directive 1995 and takes the form of the Data Protection Act 1998 under the current UK regime
- ï GDPR will be in force from May 2018 ï less than a year away
- ï Broad, extraterritorial scope ï applies to non-EU organisations who are processing the personal data of EU citizens (which will be relevant for many international shipping companies)
- ï Mandatory requirements to report incidents relating to personal data
- ï Penalties of up to 4% of global turnover (much higher than the current cap of £500,000 in the UK)

The changing legal and regulatory landscape (2)

ÅNetwork Information Security Directive

- To be implemented by all member states by May 2018 (including the UK)
- Requires õoperators of essential servicesòto implement appropriate information security measures and to report incidents to the relevant authorities. Again, national authorities will have the power to impose heavy fines for non-compliance
- The definition of õoperator of essential servicesòwill be determined by each member state ï passenger and freight water transport companies and intelligent transport system operators are mentioned in the Directive and likely to be included within its scope

The changing legal and regulatory landscape (3)

ÅOther legal developments

- The English courts have recently recognised misuse of private information as a tort
- The Courts have also recognised that individuals may bring claims for losses resulting from breaches of the Data Protection Act even when no pecuniary loss has been suffered
- Class actions/group litigation orders
- As technology develops (IoT; autonomous transport, etc) more complex legal/regulatory landscape, so need to keep one step ahead

Managing cyber risk in the maritime industries

Draft and review data protection policies and incident response plans in order to promote compliance with the new legal and regulatory landscape	• Do your policies and incident response plans acknowledge the new mandatory notification requirements under the GDPR? • Do the policies and plans reflect other aspects of the GDPR, such as the concepts of privacy by default and by design?
Have you considered the other legal and regulatory requirements that are relevant to your business?	• Away from GDPR, are there data protection / cyber security laws that apply to you because of the regions you do business in?

Managing cyber risk in the maritime industries (2)

Consider cyber risk in a broader context	• Are cyber issues factored into your broader incident response plans and disaster recovery plans? • Are you taking account of emerging risks when maintaining these plans ï for example, do you have an established policy on how to deal with ransomware?
Consider the cyber risk management position of third parties	• Do charterers, contractual counterparties or other suppliers have adequate cyber security in place? • If not, what are the potential risks to you?

Mitigating cyber risk in the maritime industries (3)

Stress-test your policies and procedures by reference to worst-case cyber incidents, such as:	• Large losses of passenger / crew/ employee or business information • Interruptions to business caused by cyber issues such as ransomware or malicious hacking • Damage to or loss of vessels due to hacking or other cyber issues
Train your employees / crew on cyber risk and develop a culture of cyber-scepticism	• 36% of all of the cyber incidents we deal with involve some kind of employee error or misconduct • A further 40% involve security issues that could potentially be avoided if a greater awareness of cyber risk or better cyber hygiene existed within the organisation

Mitigating cyber risk in the maritime industries (4)

Ensure your board and senior management are familiar with the cyber risks you are facing and have considered whether those risks are adequately being mitigated

When an incident does occur, the priority should be to react quickly and efficiently

Engagement terms with lawyers, IT specialists, security specialists etc. should be pre-agreed so that when (not if) an incident happens, a response can be co-ordinated quickly


NORTON ROSE FULBRIGHT

Disclaimer

NORTON ROSE FULBRIGHT