

Cyber security? You're right, it's a hot topic.



Cyber security is a hot topic – and so it should be! Recently, we have seen that the marine industry is far from immune to cyber-attacks and security breaches, and the consequences can be far-reaching.

One of the key challenges associated with increased automation and digitalisation is the vulnerability to cyber-attack; as the industry continues to invest in digital systems, the risk will only increase.

What is cyber security?

Cyber security is not just about preventing hackers gaining access to systems and information that can potentially result in loss of confidentiality and/or control. It is also about addressing the maintenance of integrity and the availability of information and systems, ensuring business continuity and the ongoing utility of digital assets and systems.

Why is cyber security now top of the agenda?

Information and communications technology (ICT) is revolutionising shipping, bringing with it the ‘digital ship’ era. Today’s leading manufacturers and ship operators want to innovate using the latest ICT systems, going beyond traditional engineering to create ships with enhanced monitoring, communication and connection capabilities – ships that can be accessed by remote onshore services at any time and from anywhere. The rapid evolution in the use of, and reliance upon, digital and communication technologies, as well as the advances in automation and the potential for the integration of multiple electronic systems, increases the importance of addressing inherent vulnerabilities.

What does this really mean for the shipping industry?

Ships are becoming increasingly complex and dependent on the use of digital and communication technologies; in line with increased connectivity comes a new need to implement secure technologies and processes to mitigate threats to operational technology (OT).

ICT and OT used to be separated by numerous human-centred processes, allowing for an incremental approach to cyber ICT security. As the boundaries of autonomous systems extend, however, these ‘fire walls’ are disappearing and cyber security must be considered with the utmost importance as a fundamental component in the risk profile of critical assets that are connected.

Do you have a digitally-enabled ship?

Ship-based digitally-enabled systems include: navigation systems, including electronic charts, global positioning systems (GPS), and dynamic positioning systems (DPS); radar and automatic identification systems (AIS); communications systems, including radio communications (terrestrial and satellite) and data communications (broadband, voice over IP (VoIP), internet access and e-mail); integrated bridge systems; control systems for the wide range of electro-mechanical systems on board ships, such as main engine, generators, ballast tanks, life support, fuel and oil pumps, watertight doors, fire alarms and controls, cargo hold fans and environmental controls; and equipment used by charterers, such as survey equipment (sonar and seismic survey systems, for example), wireless access points, IP ports and wireless phones.

If my cyber security is not optimal, what are the potential risks?

Compromise of a ship's systems may lead to various unwanted and harmful outcomes at an individual ship or fleet level. For example: physical harm to the system or the shipboard personnel or cargo (the worst-case scenario being a risk to life and/or the loss of the ship); disruptions caused by the ship no longer functioning or sailing as intended; loss of sensitive information, including commercially sensitive or personal data; and permitting criminal activity, including kidnap, piracy, fraud, theft of cargo and the imposition of ransomware.

Poor security could also lead to potential financial loss or penalties, loss of customer and/or industry confidence, reputational damage, and even litigation.

Why would I want to increase the digitally-enabled capability of my operations?

Digital systems transform a ship into a total system of interlinked systems ('a system of systems'). While digital systems are not exact substitutes for traditional electro-mechanical systems on board ships and for operators, they provide opportunities to combine these traditional components with more complex behaviour. When designed properly, the use of ICT can increase efficiency and safety through improved monitoring and communication, and greater situational awareness on the bridge, in the engine room and in other operational areas.

Specifically, digitally-enabled systems impact ships by: interconnecting systems through computer networks; integrating systems; creating layers of embedded and/or application software that separate the operator and the ship; changing the role of the operator to a manager of many linked, complex systems; shifting the operator's perception of the ship and its environment to one defined by human-machine interfaces; enhancing the ability and efficiency of the crew – or changing the organisation of work – through automation; and creating the potential to remotely monitor and change the operation of the ship using a wide range of data from anywhere in the world.

What does 'good' cyber security look like?

Because a digital ship consists of multiple interconnected systems and because of the rapid pace of technology development, assuring that a digital ship will be safe cannot be prescriptive and cannot rely on knowledge gained from previous systems. Instead, it requires a 'total systems' approach – one that takes account of all the different systems on board and on shore, how they are designed and installed, how they

connect and how they will be managed.

This is the approach that Lloyd's Register (LR) takes, applying a non-prescriptive, risk-based process from the earliest concept stage, through onboard integration, to operation – one that is based on extensive experience of system design and installation on board ships and other marine platforms.

Cyber security is a through-life issue in a digitally-enabled ship that requires consideration from project inception to asset disposal. In addition to its impact on system development, special consideration must be given to the education and associated organisational culture of all related staff. Incident response planning and the maintenance of an asset's security status through timely, carefully tested patching also needs to be considered throughout an asset's lifecycle. Cultural Risk Factors specific to the maritime industry also need to be considered and revisited. This includes factors such as: low awareness of maritime cyber security, complexity of the maritime ICT environment, fragmented maritime governance context, inadequate consideration of cyber security in maritime regulation, lack of a holistic approach to maritime cyber risks, overall lack of direct economic incentives to implement good cyber security in the maritime sector, and slow regulatory change.

Cyber security needs continual maintenance!

The cyber security landscape is a constantly changing one, as new threats and countermeasures emerge. Even with the best cyber security strategy in place, at some point you may suffer a breach. It is important to have in place robust incident response plans that can be deployed quickly and effectively. And it is vital that staff know what to do in the early stages of a cyber security threat. In fact, the greatest security vulnerabilities come from people –

90% of cyber security incidents can be traced back to human error or intent. Good security outcomes are therefore underpinned by positive security behaviours, so training is vital to increase the overall awareness of cyber security risks and ensure that the appropriate behaviours, awareness, attitudes and technical skills are embedded within a business.

What should I do to address cyber security?

Across the industry, there's still huge variation in levels of awareness and preparedness for the increasing role of digital technologies and the cyber security risk you can be exposed to. Understanding the level of cyber security readiness is the essential first step to identifying, mitigating and managing the risk. LR conducts readiness reviews to quantify existing digital (including cyber security) capabilities and help develop strategies to maximise the benefits while minimising the risks. Uniquely, LR takes a 'whole asset' approach and looks at all the connected equipment, systems and software, both individually and in terms of their interactions with, and potential impact on, each other. LR can undertake a detailed technical assessment of the entire asset, identifying theoretical cyber security threats and vulnerabilities. And we can carry out practical interventions, such as penetration testing and ethical hacking, ascertaining the real, practical risks. This combined desk-based and practical work approach provides a robust, objective and fully quantifiable basis for developing a cyber security strategy. LR can also review the levels of cyber security readiness within offices and identify awareness and technical training

needs. This assessment also allows for the identification of the residual risks – those that cannot be reduced or avoided currently, and must therefore be understood, accepted or insured against.

How can LR help?

LR has created cyber security requirements as part of its digitally-enabled ships guidance and procedure. The recently revised Digital Ships ShipRight procedure, which details LR's framework for accepting digital technologies used for autonomy and remote access/control and was the industry's first ShipRight procedure, includes a Cyber SECURITY descriptive note as part of any assessment of digitally-enabled systems. This helps to raise awareness of cyber security and recognises that cyber security has been assessed (in the context of design and build), and that an appropriate cyber security governance system is in place to mitigate the risk of introducing vulnerabilities to cyber-attack, or other unauthorised access, during the design, procurement, construction and installation of the digital systems.

In addition, a Cyber Secure programme has been developed that consists of a set of consultancy services designed to help ship operators understand how cyber secure they are now and what level of security they want to achieve in the future. The recent acquisition of Nettitude strengthens LR's existing broad portfolio of cyber security services, spanning certification, compliance, training, auditing and security consulting and now including penetration testing, information security consulting, managed security services and incident response.

Together, Nettitude and LR now provide a complete suite of cyber security assurance services to help clients identify, protect against, detect, respond to and recover from cyber threats.



Get in touch

Visit www.lr.org/cyber for more information or contact Elisa Cassi, Product Manager, Cyber Security:

T +44(0) 33041 40727

E elisa.cassi@lr.org

Lloyd's Register
71 Fenchurch Street
London
United Kingdom
EC3M 4BS



Lloyd's Register and variants of it are trading names of Lloyd's Register Group Limited, its subsidiaries and affiliates. Copyright © Lloyd's Register Group Limited, 2018. A member of the Lloyd's Register group.