MARITIME CYBERSECURITY AND THE IMO

> The maritime industry is becoming increasingly digitalised on many fronts: at sea, at port and on land. Vessels are undergoing digitalisation, with IT and OT equipment being installed to support new business demands. Bridges are being equipped with digitalised ECDIS systems, sensors are being deployed onboard to measure different aspects of vessel performance, and connectivity is enabled and boosted in order to support real-time monitoring and optimisation for the whole fleet. IT and OT systems are being connected to bridge the gap between the business and maritime operations in order to optimise operations, increase efficiency and create new opportunities and products.
>
> .

With increased digitalisation comes new challenges. Cybersecurity is one of the new areas where shipping is facing new challenges. The maritime industry has been slow to adopt cybersecurity in their IT and maritime operations.
Some reasons for not prioritising cybersecurity are:

- Lack of understanding of cybersecurity in the whole organisation, from top management to crew
- Lack of regulatory requirements regarding cybersecurity
- Lack of support and budget for cybersecurity from management
- Lack of human resources in IT, OT and specifically cybersecurity
- Complex IT and OT environments on board vessels

Considering the reasons listed above, we recommend that the maritime industry and operators need to do the following:

- Get top management support for cybersecurity

Top management support is essential for implementing an organisation-wide cybersecurity programme. Without the support and budget from top management, the chances of success are low.

- **Identify and assess the cybersecurity risks in your environment**

In order to know what needs to be done, the risks in the environment need to be identified and assessed so that a comprehensive action plan can be created.

- **Based on the identified cybersecurity risks, create an action plan to mitigate those risks**

The action plan, which is based on the identified risks, will be the top management-approved strategy for how the organisation will address and mitigate the identified risks.

- **Create a cybersecurity management system to manage the governance of all cybersecurity efforts. Use familiar standards like ISO27001**

Cybersecurity is a complex field, from top-level policies and processes down to technical details and the configuration of devices in the environment. There are existing frameworks and standards that can be used to build the cybersecurity programme so that you do not have to do everything from scratch yourself. Use standards like ISO27001, NIST Cybersecurity Framework and ISO/IEC 62443 as a baseline for your cybersecurity programme so that you can rest assured that you have an industry-based standard to establish your work on that is also recognised by third parties, customers and regulators and is auditable.

- **Train all employees in cybersecurity**

Employee support and understanding are key to any successful project. Ensure that your employees, from top management to crew, know what cybersecurity means and what they can do to ensure that your environment is kept secure. This can be done by cyber-security awareness efforts, training, courses and webinars, as well as internal communications from those responsible for cybersecurity in your organisation.

- **Get external help from a knowledgeable partner in cybersecurity that can help with cybersecurity risk management and implementing cybersecurity in your environment**

Cybersecurity is a complex endeavour that requires specialised knowledge that is hard to find. Your IT and OT teams are most likely already working hard with their regular tasks and projects, and it can be easier and cheaper to get help from knowledgeable third parties specialising in maritime cybersecurity instead of hiring hard-to-find experts in your organisation.

By taking these actions, cybersecurity will be better managed and aligned with the upcoming cybersecurity regulations that have been published by the IMO.

Cybersecurity has not previously been a priority and has not been part of the regulatory requirements. Without such regulatory requirements, cybersecurity is usually not prioritised as there is no direct return on investment (ROI) for the efforts. Due to the increasing risks with cybersecurity in the maritime sector, the IMO published Cybersecurity Risk management regulations and guidelines for maritime operators in 2017:

- MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management
  http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

- Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems
  http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution%20MSC.428(98).pdf

These regulations and guidelines aim to ensure that maritime operators take cybersecurity risks into account in their operations and specifically in their Safety Management System (SMS) in order to improve cybersecurity in the maritime industry.

These new regulations and guidelines are much needed in the maritime sector, and operators need regulations in order to make cybersecurity a priority. If these regulations are not managed, operators risk their ships being detained in port. Although these regulations are needed, they do suffer from being vague and non-descriptive, which is not always good for the maritime sector, where crew members and employees are usually quite practical and take an ad-hoc approach to their work. A clearer and more detailed approach to maritime cybersecurity regulation would be more advisable, although more difficult to create to fit the diverse organisations and environments.

Maritime industry associations such as BIMCO (Baltic and International Maritime Council) and DCSA (Digital Container Shipping Association) have created additional guidelines for their members in order to help maritime operators in their cybersecurity efforts. These guidelines are usually more descriptive and practical than the IMO regulations and are hence a good source and baseline for maritime operators.

- BIMCO - The Guidelines on Cybersecurity Onboard Ships, version 3 https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships
- DCSA - Implementation guide for Cyber Security on Vessels https://dcsa.org/initiatives/cyber-security/

Other associations have similar guidelines, but those listed above are the most comprehensive and detailed.

Although these regulations and guidelines have been published and have been available for a few years, the maritime sector is still lagging behind. Some maritime operators have been proactive and have implemented cybersecurity in their environments, while others have not and are still in the process of trying to understand what they need to do and what the business impact of a cybersecurity incident would be.
Using the recommendations above, maritime operators should start planning and implementing cybersecurity based on the identified risks. This can be done in the form of an implementation project that will then be incorporated into regular day-to-day business operations.

Starting a cybersecurity project is by no means an easy task and will require budgeting, human resources and technical solutions. A cybersecurity project will include areas like:

- Cybersecurity policies and procedures
- Cybersecurity governance and organization
- Asset management (IT and OT equipment)
- Access control (logical and physical security)
- Operational security
    - System configuration management
    - System log management and monitoring
    - Anti-malware protection
    - Vulnerability and patch management
    - Backup management
- Third-party supplier management
- Compliance and audit management

If there are no experienced cybersecurity professionals in-house, we highly recommend partnering with a maritime cybersecurity company to help with the implementation of the necessary policies, procedures and technologies. Many parts of the implementation can be done together with third party providers, without requiring the recruitment of expensive cybersecurity professionals. This is specifically relevant in maritime environments where the teams responsible for IT and OT environments are already burdened with managing the existing infrastructure and do not have the resources available to allocate to implementing and managing cybersecurity.

DEDUCTIVE LABS

Deductive Labs (www.deductivelabs.com), an experienced and specialised partner for maritime cybersecurity.

.

PROTECT · PREVENT · PERFORM