What can the maritime industry do to be more cyber-secure

Photo: Rawpixel

Digital defence

by **Nikos Späth**, *Head of Media & Public Relations, DNV GL Maritime Communications*

DNV·GL

the Høvik-headquartered DNV GL is a classification society and accredited certification body. Since its foundation in 1864, DNV GL's purpose has been to safeguard life, property, and the environment. Today, the organisation is structured into five business areas: Maritime, Oil & Gas, Energy, Business Assurance, and Digital Solutions, alongside a Global Shared Services function and Group Centre. For more info please click www.dnvgl.com

Although the notion of a ship in the middle of the ocean being disabled by a software malfunction or by hackers was initially greeted with considerable scepticism and denial, a spate of incidents, including most notably an attack that disrupted operations at COSCO, has transformed attitudes. Today the maritime industry acknowledges the potential dangers and is taking steps to address the cyber risk at various levels. As owners act to fortify their ships and shore-side operations against cyber risk in the face of evolving threats and imminent regulation, DNV GL has expanded its services to cover control systems, software, procedures and human factors.

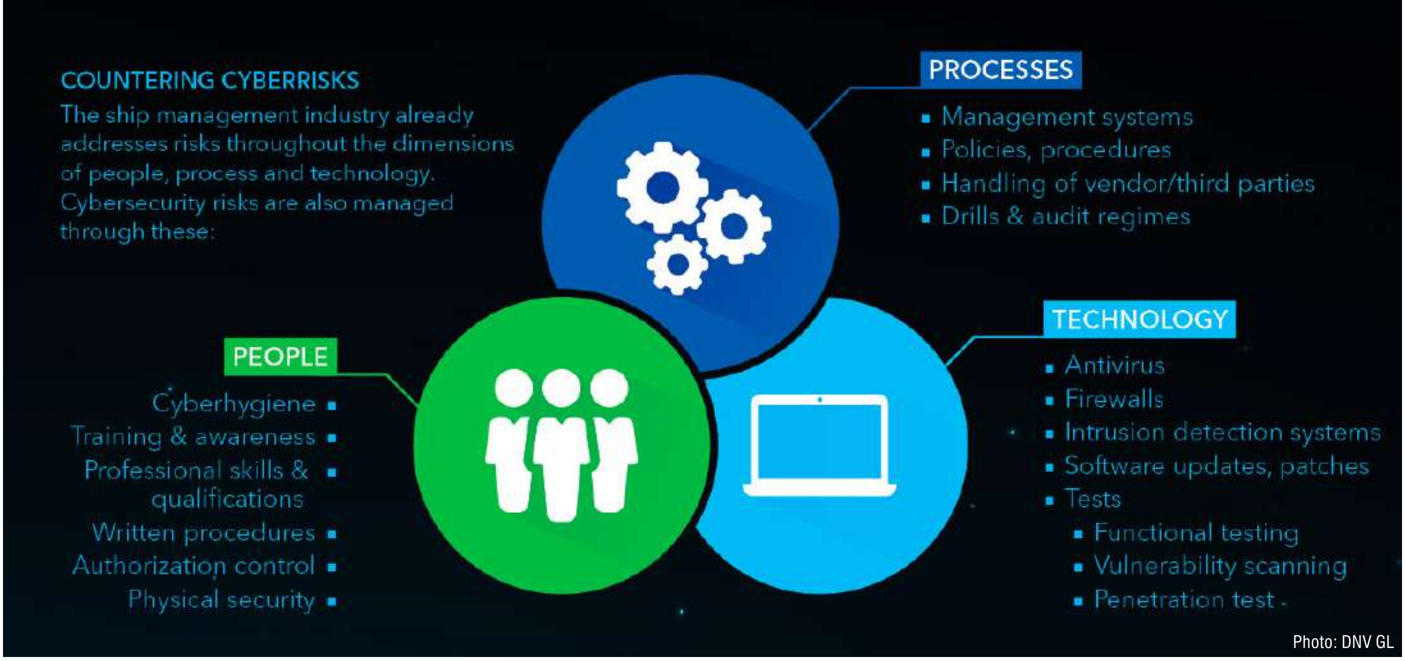
Cyber security is a moving target. Threats continue to grow in reach and complexity, with new vulnerabilities discovered on a seemingly daily basis. In the space of a few years, hacks and security breaches have jumped from being an exceptional event confined to a special breed of technology companies to becoming a fact of life-impacting everyone. No industry is immune.

While in earlier decades office IT systems were the predominant target, these days more incidents are affecting operational technology (OT) – the programmable control systems responsible for operating machinery. The trend reflects the growing complexity of such systems and a general increase in connectivity, which in turn increases the attack surface of a vessel.

This increase is borne out in the statistics: The number of attacks on OT in 2016 was double that of the preceding year and quadruple the 2013 level. So whereas before it was mostly a company's finances and reputation that were at risk, now the threat has escalated to confront the safety of life, property and the environment. The stakes are much higher. For this reason cyber security must now be considered an integral part of overall safety management in shipping and offshore operations.

Regulatory response

Fortunately, industry policymakers have not been asleep at the wheel. The year 2017 saw two particularly significant milestones in the regulatory environment. A section dedicated to maritime security – including cyber risk – was introduced in the third edition of the Tanker Management Self Assessment (TMSA), which came into effect in January 2018, as well as in the seventh edition of the Vessel inspection questionnaire (VIQ7) from the Ship Inspection Report Programme (SIRE), effective from September 2018. Because TMSA and SIRE



COUNTERING CYBERRISKS

The ship management industry already addresses risks throughout the dimensions of people, process and technology. Cybersecurity risks are also managed through these:

PROCESSES

- Management systems
- Policies, procedures
- Handling of vendor/third parties
- Drills & audit regimes

PEOPLE

- Cyberhygiene
- Training & awareness
- Professional skills & qualifications
- Written procedures
- Authorization control
- Physical security

TECHNOLOGY

- Antivirus
- Firewalls
- Intrusion detection systems
- Software updates, patches
- Tests
    - Functional testing
    - Vulnerability scanning
    - Penetration test

Photo: DNV GL

Scan the code to download DNV GL's Cyber Secure class notation

Scan the code to obtain your copy of DNV GL's Recommended Practice on cyber security resilience management for ships and mobile offshore units in operation

Scan the code to watch DNV GL's video about cyber security awareness

are imperative to gaining charters, tanker operators now have a commercial incentive to demonstrate they have given systematic consideration to potential vulnerabilities and implemented appropriate mitigations and safeguards to address them.

Shortly after, IMO's Maritime Safety Committee inserted Maritime Cyber Risk Management into the list of International Safety Management Code requirements. Strongly encouraged to start on 1 January 2021, the amendment leaves non-tanker vessel owners with little more than two years to achieve a similar level of preparedness as their tanker-owning colleagues.

Risky job

Managing cyber risk is ultimately no different to managing any other risk, remarks Svante Einarsson, DNV GL's Senior Cyber Security Advisor. "The equipment and terminology may be unfamiliar and somewhat daunting but the approach is fundamentally the same as, say, preparing for and carrying out hot work modifying a vessel's structure."

Software changes, for example, should not be done on a whim, which can often happen on ships. Because IT engineers don't frequently visit vessels, when they do come aboard to update the Electronic Chart Display and Information System or set up the latest version of a maintenance management application, the temptation is to be helpful. They click to install a new service pack and a backlog of other app updates. Nine times out of ten, this is fine. But occasionally it can disrupt settings elsewhere on the system. Moreover, the consequences won't become apparent until long after the engineer has left and the ship has set sail.

Instead, updates should be carefully planned, tested, approved and recorded. They should be categorized as minor or major to ensure personnel with the appropriate authority can approve them. This, Einarsson says, is virtually identical to the process for gaining approval prior to carrying out welding.

Lessons learned from NotPetya

If there was one positive outcome of the NotPetya ransomware attack on Maersk in 2017, reasons Einarsson, it was the awakening of owners and operators to the fact that cyber threats are not hypothetical. "Today there is much greater awareness of the real-world implications and acceptance that cyber risk has to be tackled," he says. However, shipowners and operators are at different stages of the learning curve in formulating a response. Einarsson also observes, "Some are bewildered by the scale of the problem and don't know where to begin; others have introduced some countermeasures but are uncertain whether they've covered everything they need to cover."

In its role as a classification society DNV GL has adapted and expanded its cyber security services to assist owners and operators in protecting their assets against evolving threats and ensuring their safeguards satisfy new industry rules and regulations. DNV GL now provides services for educating and raising the awareness of all stakeholders both onshore and at sea; assessing and implementing defensive and reactive countermeasures; and monitoring and reviewing the effectiveness and robustness of barriers with an emphasis on continuous improvement.

These services are purposely designed to be non-system specific so as to work equally for conventional IT and industry-specific operational technology, which is important when systems are interlinked. This also avoids obsolescence. While the consequences of an OT outage are likely to be more serious, they can often be traced back

Photo: DNV GL

to a weakness in IT systems, particularly if they originate from an external source.

Practical advice

In September 2016, DNV GL published a Recommended Practice (RP) to educate shipowners and operators on how to deal with cyber risk. "It was designed to demystify a subject the industry was still getting to grips with. We took care to write it in a maritime language and context," stresses Einarsson. The focus was on practical steps. "Most advice coming from industry bodies at the time, while produced with noble intentions, was very high-level. Our idea was to close the gap between theoretical concepts and the real world," he underlines. For example, DNV GL's RP accounts for common constraints such as limited budget and resource availability. The core approach is to identify weaknesses, assess their severity, then prioritize the most serious ones. The RP has been released as a free resource.

The next step for vessel operators would be to carry out a cyber security assessment. DNV GL can support this by sending interdisciplinary teams to help on- and offshore personnel identify and address specific business risks. "While operators typically understand the written guidance, translating those principles into action is sometimes more challenging," notes Einarsson. This collaboration results in a highly methodical approach to developing effective risk mitigation procedures that mesh neatly with the operator's structure and working practices. Apart from closing cyber security gaps by technical means, this appraisal also considers system management and the human factor.

Once countermeasures and a new risk management regime have been implemented, they can be followed up and qualified by penetration testing. "Testing the robustness of barriers is essential to ensure that assets are secure and nothing has been overlooked," explains Einarsson. In this process, authorized "white-hat" hackers do their best to compromise the IT and OT defences to validate that safeguards work as they should and risks have been eliminated.

Life cycle management

DNV GL also provides third-party verification of cyber security requirements throughout the newbuild project life cycle. "Our cyber security team recently worked with a major cruise line on devising a process for embedding cyber resilience from the very beginning of the vessel design phase," reports Einarsson. This was accomplished by introducing defined risk handling and accommodating procedures to all stakeholders in the project – not only the owner and yard but also the vendors. Incorporating technology and systems from third-party suppliers unavoidably adds complexity to a project and, from a cyber security perspective, increases potential exposure to malevolent actors. Meanwhile, shipyards are as much on the learning curve as vessel owners.

"For a large, sophisticated vessel like a cruise ship, which is dependent on technology for both operational and hotel needs, collaboration is absolutely critical," Einarsson stresses and then adds, "Cyber risks are multifaceted. The response has to mirror that. Everyone has to be involved in the conversation, because, as the saying goes, a chain is only as strong as its weakest link." The feedback from the project, he notes, was overwhelmingly positive, "Tackling cyber security right from the beginning of a vessel's life cycle enables stakeholders to take a proactive, rather than reactive, approach to the problem. It provides more opportunities to insert barriers."

Based on these advisory services, DNV GL has developed its first class notations covering cyber resilience. The Cyber Secure notations have three qualifiers: Basic, Advanced and "+". Basic is primarily intended for ships in operation; Advanced is designed to be applied throughout the newbuilding process. The '+' qualifier is available for systems not covered by the scopes of Basic and Advanced. Furthermore, DNV GL has introduced a Type Approval scheme to verify and test the cyber security reliance of components. The utilization of these reference standards ensures state-of-the art cyber security based on the 62443 standard of the International Electrotechnical Commission. The standards are applicable for the whole life cycle of a vessel from the perspective of manufacturers, yards and shipowners.

The human element

Of course, cyber security is not just a matter of firewalls and antivirus software. Up to 90% of incidents are attributed to human behaviour. Phishing and social engineering, unintentional downloads of malware, etc., remain common issues. At the same time, most crews and onshore staff are not taught how to respond to cyber attacks or major technology failure and consequently fail to contain the damage.

DNV GL has therefore expanded its options for training through its Maritime Academy. Courses cover cyber security from both management and technical angles and even include lessons in hacking to give participants an insight into how cyber attackers operate. Additional new tools incorporate friendly phishing campaigns and simulations of other social engineering techniques as well as features for assessing staff alertness so customers can fine-tune the level and frequency of cyber awareness training.

DNV GL can help vessel operators combine traditional IT security best-practices with an in-depth understanding of maritime operations and industrial automated control systems. DNV GL understands the importance of tackling and integrating the human factor when devising and implementing a cyber risk management strategy because ultimately, it is people who drive our industry. ■