Digital defence

CYBER RISK As owners act to fortify their ships and shoreside operations against cyber risk in the face of evolving threats and imminent regulation, the classification society DNV GL has expanded its services to cover control systems, software, procedures and human factors

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 AP Moller-Maersk for several weeks, has transformed attitudes. Today the maritime industry acknowledges the potential dangers and is taking steps to address cyber risk at various levels.

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 by statistics: the number of attacks on OT in 2016 was double that of the preceding year and four times the level seen in 2013. So whereas before it was mostly a company's finances and reputation at risk, this has now escalated to safety of life, property and 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. Last year 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 this January.

Digital concepts on board ships pose a multitude of cyber threats

Because TMSA is essential in winning charter contracts, tanker operators now have a commercial incentive to demonstrate that 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 to the list of ISM Code requirements. Strongly encouraged to start on January 1st 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

Ultimately, managing cyber risk is no different to managing any other risk, remarked Patrick Rossi, DNV GL's Maritime Cyber Security service manager. "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 do not frequently visit vessels, when they come aboard to update the ECDIS 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 in the system. Moreover, the consequences may not 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 categorised as minor or major to ensure personnel with appropriate authority can approve them. This, Rossi said, is virtually identical to the process for gaining approval prior to carrying out welding.

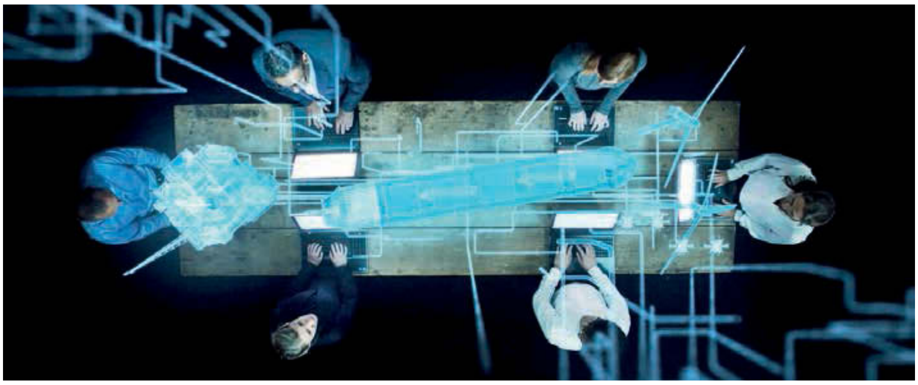
NotPetya lessons

If there was one positive outcome of the NotPetya ransomware attack on Maersk last spring, reasoned Rossi, it was awakening 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."

However, shipowners and operators are at different stages on the learning curve in formulating a response, he observed. "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 offering to assist owners and operators working to protect their assets against an evolving threat landscape and to ensure they satisfy new industry rules and regulations.

It now provides services for educating and raising the awareness of all stakeholders, both on shore and at sea; assessing and implementing defensive and reactive countermeasures; and monitoring and reviewing effectiveness and robustness of barriers, emphasising continuous improvement.


The classification society is expanding its training options for crew and onshore staff

These are purposely designed not to be system specific, so as to work equally for conventional information technology and industry-specific operational technology, which is important when systems are interlinked. It also prevents them from obsolescence. While the consequences of an OT outage are likely to be more serious, they can often be traced back 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, with which the industry was still getting to grips. We took care to write it in a maritime language and contextualise it in a maritime setting", said Rossi.

The focus was on practical steps, stressed Rossi. "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."

For example, DNV GL's RP takes into account common constraints such as limited budget and resource availability. The core methodology is to identify weaknesses, assess their severity and then prioritise 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 task by sending interdisciplinary teams to engage with onshore personnel and offshore crews to identify and address specific business risks.

"While operators typically understand the guidance as it is written down on paper, translating those principles into action is sometimes more challenging," noted Rossi.

Such collaboration results in a highly methodical approach to developing procedures that are effective both at reducing risk and mesh neatly with the operator's structure and working practices. In addition to technical mitigations for closing any cyber security gaps, this appraisal also considers system management and the human factor.

After countermeasures and new risk management procedures are 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 that nothing has been overlooked," Rossi explained.

In this process, authorised 'white-hat' hackers do their best to compromise the IT and OT defences to validate comprehensively that safeguards work as they should and risk vectors have been closed.

Lifecycle management

DNV GL also provides third-party verification of cyber security requirements throughout the newbuild project lifecycle. "Our cyber security team recently worked with a major cruise line on a newbuild project to devise a process for embedding cyber resilience from the very beginning of the vessel design phase," said Rossi.

This was accomplished by introducing defined procedures for handling and accommodating risk for 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 the potential attack surface area for 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," Rossi said. "Cyber risks are multifaceted. So 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 noted, was overwhelmingly positive. "Tackling cyber security right from the beginning of a vessel's lifecycle enables stakeholders to take a proactive, rather than reactive, approach to the problem. It provides more opportunity to insert barriers."

Based on these advisory services, DNV GL has developed its first classification notations covering cyber resilience. The cyber secure notations have three qualifiers: Basic, Advanced and '+'. Basic is primarily intended for ships in operation, while Advanced is designed to be applied throughout the newbuilding process. The '+' qualifier is available for systems that are not part of the default scope of Basic and Advanced.

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, for example, 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, resulting in behaviour that fails to contain the damage.

DNV GL has therefore expanded its options for training through its Maritime Academy. Courses covering cyber security from both management and technical angles and even include lessons in hacking to give participants an insight into how cyber attackers operate. In addition, it has developed tools – incorporating friendly phishing campaigns and simulations of other social engineering techniques – to assess staff alertness, enabling customers to fine-tune the level and frequency of cyber awareness training.