From digital infancy to a harsh new risk reality

by Geir Inge Jensen, *Chief Information Security Officer, Dualog*

Dualog's December warning to beware the hidden dangers in e-mails, particularly prevalent during the holiday season as greetings were exchanged, was especially timely as the introduction of the new IMO 2021 cybersecurity regulations came into force from the beginning of the year. It is now essential that cyber risk is firmly integrated into safety management systems. Failure to be compliant may leave ship owners exposed to the risk of having their vessels detained.

For the maritime industry, there has been a steep climb on the digital maturity ladder, from infancy to puberty. As key maritime players began adopting digital practices and technologies, IT was seen as an operational cost rather than a strategic business approach.

Today, more and more ships, systems and networks are connected to the Internet, making them accessible from practically anywhere on Earth. At the same time, this makes ships much more vulnerable to cyber-attacks, both targeted and random ones, and it is no secret that the maritime industry is on the hackers' radar.

Increasing digital reliance has unlocked huge efficiencies and operational benefits. Still, it has also opened a Pandora's Box of cyber threats – a risk reality that shipping needs to understand and navigate.

Cybercrime is no hype

Cyber risk has fast become the new normal for the maritime sector. According to the Allianz Risk Barometer 2018, cybercrime is considered one of the top five threats to the global maritime industry. Certainly, we at Dualog have seen week-on-week increases in the number of attacks as shipping has become an ever more attractive target for hackers who see the opportunity to extort significant sums of money from the industry.

While the shipping industry is legally obliged to comply with the safety management rules on cybersecurity of the new International Safety Management Code, the truth is that there are many strong reasons for taking the issue seriously. Although financial loss can be significant, in many cases, it only represents a fraction of the problem. Shipping is going digital, and the industry increasingly integrates with other parts of the global supply chain, including enterprise resource planning and logistics systems. For operations to run smoothly and efficiently, shipping needs to make available more and better data to customers, regulatory bodies and vendors – and at a faster pace, often in real-time. If such operational data is stopped or lost, the business consequences can be devastating.

As steps are taken to repair damage to systems and loss of data, many days can be lost. And even as some restoration of systems occurs, it will take a considerable time for all systems to be running at 100%. The effects of this are twofold: not only does the downtime have a financial cost, but also, it impacts greatly on the reputation of the company as it struggles to fulfil its commitments. In many cases, the money can be recouped more easily than the company's reputation is restored. It is not difficult to remember the names of those companies that have

suffered a major cyber-attack, even many years on.

With security in mind

When looking at maritime cybersecurity measures, it is essential to take a wide-ranging approach that encompasses every system on ship and shore. Vessels are becoming increasingly complex and dependent on information and communications technologies throughout their operational life. There is no single solution to combating cyber risks. It is a collaboration of many people alongside technical and procedural measures. A company's cybersecurity is only as good as its weakest link.

The obvious place to start is with hardware. Ensure that it is always kept up to date and that backup units are maintained. Choosing the hardware supplier carefully and understanding how they operate means you can be sure that all components have been designed and delivered with security in mind.

Even companies that are heavily reliant on IT can be guilty of neglecting to install patches and software updates. Unless there is a strong emphasis on the importance of patching and updating, which percolates from the IT Director down, there is always the chance that vital upgrades will be missed.

At the design stage, make sure that ICT infrastructure has been developed with security in mind, using techniques which make it harder for attackers to compromise data or systems. The separation of business systems and operational technology from each other and those used socially by the crew, for example, can minimise the risk of cross-contamination if one is compromised. The fewer critical shipboard systems connected to uncontrolled networks or directly to the internet, the better.

People make mistakes

Human error has long been recognised as a significant contributor to cyber breaches. Still, it is rarely malicious, so designing systems that keep the possibility of human error to a minimum protects your people and equipment from the consequences of failure. Furthermore, you should be aware of exactly who has access to the different systems, allowing a granular permission system – don't be tempted to give unnecessary consents.

Accept that people make mistakes and then steps can be taken to safeguard teams and equipment by installing the best possible protection products. Managers should be kept informed as to what safeguards exist and how to implement them.

People can only be expected to use systems securely if they are given regular training, key information is displayed at the point of use, and regular testing of systems occurs. By communicating in an engaging way that helps the workforce understand the essential nature of cybersecurity, it should be possible to carry them with you so that every team member understands that they are an important element in the fight against cyber-attacks.

This kind of cyber drill training may prove invaluable, both on a day-to-day basis as well as when cybercriminals are particularly active. As mentioned at the beginning, the shipping industry must be extra vigilant during the holiday season. According to our findings, December is the busiest month for cyber-attacks because hackers will often hide malware in holiday greetings e-mails (e-mail, in general, being the number one attack vector used by hackers to get access to your company's confidential data). As much as 90% of all attacks start with email 'spear phishing,' a fraudulent practice of sending messages ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information. The current situation is worsening because of the emergence of new threats such as the Emotet and Trickbot trojan malware programmes which can render endpoint security and firewalls ineffective. Every hour, more than 15k messages pass through our MailDefence system where they are carefully filtered (scans by multiple antivirus engines, anti-spam scoring mechanisms, e-mail fingerprint analysis, phishing checks, and domain sanity checks) and delivered only when deemed safe. Nearly half of the messages are rejected as they represent a danger. So-called spoofing is yet another threat; here the company's domain can be forged in an e-mail attack. Methods like Sender Policy Framework, DomainKeys Identified Mail, and Domain-based Message Authentication, Reporting and Conformance should be used to protect against spoofing attacks. It is also important to block all e-mails with macro-enabled documents and password-protected archives from unknown senders.

Defence in depth and in breadth

Thankfully for all concerned, there are products in the market that can protect a company's network, the best of which offer a Total Systems Approach, providing a multi-layered protection structure that operates from the Domain Name System-level up, blocking unwanted data traffic and malware.

To protect against malware or phishing, anti-virus and anti-malware software should be installed, maintained and updated on all personal work-related onboard computers to reduce the risk of users inadvertently introducing malware into the ship's operating systems. Continuous scanning of systems can identify any security risks at an early stage. Carefully choosing technology, which has the highest specification of built-in cyber resilience and security, and developing a close relationship with the supplier IT departments can ensure that their digital environment stays safe.

Today, maritime cybersecurity needs to be considered as part of the overall approach to safety and security risk management. Safeguarding the fleet from current and evolving threats and vulnerabilities requires a holistic approach involving personnel, procedures, and technology. This means owners or managers need to have a comprehensive cybersecurity management plan in place on ships and within the entire organisation. And having installed the best possible technology, they must make sure that every user understands how to use it correctly.

The complex and persistent nature of cybercrime creates a need for constant monitoring and multiple layers of protection measures, also known as 'defence in depth and in breadth.' When implemented together, they constitute an entire ecosystem of layered security, providing the foundation needed to tackle all possible cyber threats and secure premises and equipment both onboard and ashore. ■

dualog Established in 1994, Dualog is a maritime digital solution provider which ensures that Internet, e-mail, and cloud services work reliably and securely on-board. The company enables and optimises all the IT services and tools one needs for efficient management of your vessels. Dualog's solutions are installed on more than 4,000 ships. The company is also recognised for assisting customers by providing streamlined operations, a guaranteed service uptime of 99.5%, and a 24/7 operational support team. Head to **www.dualog.com** to learn more.