New focus on cybersecurity as IMO 2021 looms

When it comes to cybersecurity in the maritime sector, one size certainly doesn't fit all! To achieve the best protection, vessel owners need to put in place appropriate procedures and protocols which relate directly to their ship and the way it operates, advises satcom specialist IEC Telecom.

The COVID-19 pandemic has escalated the drive towards digitalisation for the shipping industry, with a significant increase in the processes conducted over satellite and data links as well as a doubling in crew welfare usage. As a result, IEC Telecom says it is seeing a significant increase in interest in cybersecurity packages, particularly with the impending introduction of the International Maritime Organisation's (IMO) new cybersecurity resolution in January 2021.

Nabil Ben Soussia, CEO Asia, Middle East & CIS at IEC Telecom Group, said: "We are seeing an increased demand across the board, including sectors where in the past vessel owners were reluctant to fit more than the bare minimum system. Now customers are asking detailed questions about what the levels of security are and are definitely taking it very seriously."

The IMO's requirement for issues of cybersecurity to be addressed in vessel Planned Maintenance and Safety Management Systems (PMS & SMS) is certainly a driving factor, together with awareness of recent damaging high-profile cyber-attacks on companies such as Maersk.

"It is a shame that it takes regulations for some people to take their cybersecurity seriously but at least now it is a 'hot topic' and everyone is looking closely at their vessels and operational risks," said Mr Ben Soussia.

IEC Telecom pioneers a number of maritime satcom solutions including the ground-breaking OneGate system which incorporates double levels of cybersecurity. However, as Mr Ben Soussia points out, off-the-shelf systems can go 60 per cent of the way towards meeting your vessel's cyber needs but to be truly protected requires detailed analysis of your unique requirements.

"There is no 'one size fits all' solution for ship cybersecurity," he explained. "Everyone needs a specialist system suitable for their individual vessel needs.

"While there are core functions which everyone must ensure are installed in their vessel security, there is no magic solution that works for everyone. Every vessel should be individually assessed to consider how it operates, what systems it is running, and where it sails. It is important to know for example, how many terminals are in use, who accesses them, what data is produced and what is done with this data – for example is it stored on the vessel or transferred to shore?"

Mr Ben Soussia highlights the diversity of equipment throughout the maritime industry and explains that is why IEC Telecom sees its discussions with each individual customer and vessel operator as an essential factor in the identification and installation of suitable cybersecurity measures. He stresses the need for each company to produce a carefully thought-out cybersecurity policy which is rigorously implemented and regularly updated, stressing: "This is an ongoing process not something which can be done once and forgotten about."

Mr Ben Soussia's comments chime with BIMCO's new cybersecurity guidelines, the starting point of which is to identify where threats may exist and the potential vulnerabilities within a company's electronic systems. Then, depending on risk exposures, to develop protection and detection measures in order to prevent an attack from succeeding.

Meeting the new IMO requirements is likely to be more challenging for smaller owners and operators who may not have their own dedicated IT teams. The BIMCO guidelines advise that establishing an emergency response plan should if necessary involve assistance from external advisors, such as specialist companies like IEC Telecom, IT experts, lawyers and others.

IMO's Resolution 428(98) is widely seen in maritime circles as a "game changer", stating that, from 2021, a vessel's SMS will need take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code. Member governments are 'encouraged' to ensure that safety management systems address cyber risks no later than the first annual verification of the Document of Compliance after 1 January 2021.

The risks of not taking cybersecurity seriously impact not only the operation of the vessel and the safety of those onboard, but also the whole maritime business. As marine law firm Hill Dickinson advises: "There is a risk that deficiencies in anti-viral software and security systems could render a ship 'unseaworthy' in legal terms.

It points out that: "The list of access points is pretty endless with exposure to communication systems, bridge systems, AIS, ECDIS, proportion and machinery management, emissions and ballast controls, smart containers and crew welfare systems. There is no particular sector of the industry that is more exposed than any other. It's the systems and access points that create the issues."

The maritime industry has already seen incidents of pirates accessing manifests in order to target high-value cargo. There have also been suggestions that pirates were able to access the schematics of citadel constructions in order to defeat this form of antipiracy measure. The possibility to imitate AIS and GPS data is real and experts have indicated how an ECDIS system can be hacked potentially resulting in a significant collision, grounding or major incident.

Given the potential risks, it is no surprise that the IMO would seek to encourage greater focus on the cybersecurity of ships. In its MSC-FAL.1/Circ.3 Guidelines on Maritime Cyber Risk Management, IMO states its overall goal is safe and secure shipping which is operationally resilient to cyber risks.

IMO highlights the need to consider information technology, operational technology systems and the data exchange within these systems. It speaks of vulnerabilities arising from inadequate operation, integration, maintenance and design of cyber-related systems, and from intentional and unintentional cyber threats.

While threats can be presented by malicious actions such as hacking or the introduction of malware, IMO highlights the unintended consequences of failures in software maintenance or user permissions. It says: "In general, these actions expose vulnerabilities (e.g. outdated software or ineffective firewalls) or exploit a vulnerability in operational or information technology. Effective cyber risk management should consider both kinds of threat."

"Cyber discipline is now something which must be practiced at all levels in the command chain, both onboard and ashore. It is important creating vulnerabilities such as are created by unauthorised access to critical systems," said Mr Ben Soussia.

The IMO's circular refers to the dangers of failing to install network segregation, which is something IEC Telecom is keen to highlight and which plays a crucial role in systems such as OneGate where critical vessel functions and crew welfare traffic are carefully compartmentalised.

"It is important to ensure that critical systems such as bridge navigation or main propulsion systems, or the many vessel sensors which provide mission-critical data are not compromised," he said. "It is not just crew members using the internet or plugging in an infected USB or corrupted phone that pose a risk. We also need to consider how many other people may be given access to the vessel's technology.

"For example, an engineer may need to access a system remotely in order to carry out an essential repair and that access needs to be carefully managed as it immediately creates a vulnerability. Our systems can provide a third network for certified third parties and limit their access to just one system or piece of machinery and for just one occasion – ensuring that the person accessing remotely cannot interfere or impact on any other operations or technology either deliberately or accidentally. So the cost of any mistake is limited to one area only and is unlikely to shut the entire vessel down."

Mr Ben Soussia stresses the importance of robust procedures and regular, quality training to ensure that opportunities for 'human error' are minimised. For example, he points out that crew must understand the potential impact of bypassing a system or process. "We need to anticipate mistakes such as thinking what would happen if a crew member rerouted a faulty sensor via the crew welfare network in order to make it work. That would risk infection or corruption of that sensor and potentially provide an access route through to other vessel systems. That's why segregation and careful procedures are so essential."

Nabil Ben Soussia, CEO Asia, Middle East & CIS at IEC Telecom Group.

He believes in the importance of having company-specific cyber policies and rules. "You can't just bring an internet connection onboard a vessel and then leave the crew to just do what they want," he said.

IMO agrees, saying that effective cyber risk management should ensure an appropriate level of awareness of cyber risks and preparedness at all levels of an organisation, appropriate to roles and responsibilities and encourages the implementation of risk control processes and measures.

Maritime surveys regularly identify crew training standards as being perceived as one of the top cyber risk problems.

In addition he points out that, as ships become more digitalised and dependent on data analysis, it is vital to ensure the verifiable authenticity of that data. "For smart ships there is one level of threat posed by a loss of connection – which basically means that you lose your data but you are aware that the connection has dropped and the data supply has failed. However, if a vessel is corrupted in some way, either mistakenly or as a result of an attack, how will you know that the data received is correct? It may be used to tell other systems to take actions – such as telling the ship to change course – so it is very important that you are able to verify and authenticate all data as it is recorded."

It is important that these risks be addressed as more devices are connected and as operations become more dependent on the connectivity. It has been reported that today a single ship can host 5,000 data tags and 3,000 sensors in the main control and engine rooms alone. Mr Ben Soussia noted: "A network is only as secure as its most vulnerable device, therefore access and permissions must be set accordingly.

"Today, in the midst of the COVID-19 pandemic, we are careful who we allow onboard our vessels and we have in place procedures to verify the identity and health of those stepping across the gangway. I would like to see it become second nature to also verify the 'health' of any equipment brought onboard too before it is allowed to connect to or access any vessel systems." DS