Not all quiet on the global shipping cyber security front

Photo: Wikimedia Commons

A long way to go

by **Peter Broadhurst**, *Senior VP of Safety and Security, Inmarsat Maritime*

Whether in pursuit of personal data or money, cyber crime is now a big and highly automated business, ready to strike at the most vulnerable part of an organisation's defence 24/7, anywhere in the world.

inmarsat

The mobile satellite company

Inmarsat was set up in 1979 by the International Maritime Organization to enable ships to stay in constant touch with shore or to call for help in an emergency, no matter how far out to sea. Today, the company's fleet of 13 satellites serves not only the needs of merchant shipping but also governments, humanitarian aid agencies, airlines, the broadcast media, and the oil & gas, mining, and construction industries. For more info, please click www.inmarsat.com

As a case in point, speaking on a panel at the World Economic Forum earlier this year, Jim Hagemann Snabe, Chairman, A.P. Møller-Mærsk, revealed that responding to the NotPetya ransomware attack of June 2017 had required the reinstallation of 4,000 new servers, 45,000 new PCs, and 2,500 applications, all within ten days. During this period, the company reverted to manual systems. In hitting a company equipped with experienced cyber security specialists, NotPetya showed that the cyber threat is as real for shipping as it is for any other connected business, especially where legacy systems proliferate.

Cyber ambivalence

If the warning should be sinking in, an Inmarsat Research Programme report from 2018, *The Industrial IoT on land and at sea*, suggests that maritime minds are slow to change. The unique study drew on testimony from 750 survey respondents across a range of industries to establish preparedness and perceptions regarding the adoption of solutions based on the Industrial Internet of Things (IoT).

The survey found 87% of maritime respondents saying they believed that their cyber security arrangements could be improved. It also saw more of them identifying data storage methods (55%), poor network security (50%), and potential mishandling/misuse of data (44%) as likely to lead to breaches in cyber security as an outright cyber attack (39%).

Given the self-diagnosis, it is perhaps surprising to find that only 25% of maritime respondents said they were working on new IoT-based security policies. In fact, Inmarsat's research exposed ambivalence as one of shipping's leading feelings towards IoT-based solutions. With some owners engaging at the level of blockchain, others take their lead from their need to comply with regulation: this is an industry which simultaneously sustains just over 30% of shipping respondents as 'IoT leaders' and just under 30% as 'IoT laggards,' the report says. For every owner signed up to the benefits of condition-based monitoring and predictive maintenance based on real-time connectivity, there appears to be another for whom maintenance is something that takes place at regular and predictable intervals, or whenever is most convenient.

Inconsistent views on cyber security also appear free to coexist with immature ones. Around 70% of respondents identify reducing marine insurance premiums as the main driver for IoT uptake, where

insurers have shown themselves as especially sensitive to cyber threats. At the same time, other studies have found attitudes such as "I'm not the target/we have security in place, don't we?/I will be protected by AntiVirus" alive and well among seafarers.

How to maintain integrity

For those prepared to engage in the IoT, today ships sustain crews in small numbers, representing both an opportunity and challenge for automation, and indeed for cyber security. On the one hand, low crew numbers align strongly with operational technology (OT) that is remotely updated, self-managing, and supported by automated security and from third parties and OEMs, such as voyage planning, weather routing, navigation, fuel management, etc. On the other hand, the opportunities to 'patch' embedded OT safely are not frequent, and patches usually require certification by control system manufacturers.

The broader point, though, is that cyber security is not just about software patching and system configuration. Ship operators do not buy computer processors, disk storage, and software, and then build them into a system: they procure turnkey systems. Again, shipboard engineers may well be IT-literate, but no space has been made on the crew roster for cyber security specialists.

In these circumstances, the integrity of the systems on ships is best maintained by software which can identify, contain, and resolve threats wherever they appear in the network. Such Unified Threat Management (UTM) detects all deviations from the 'known good' configuration as anomalies and potential threats to security and can update securely, even during operation. Some specialised functions, such as an in-depth analysis of alerts or security forensics, will need to be delivered remotely.

Inmarsat believes that a collaborative approach – that includes shipboard systems as well as the crew operating them and the processes involved – is vital to develop the maturity response demanded by multiple threats from cyber villains, whatever their origin. For this reason, we have been working with some of the best security-focused experts available, to tailor products and services to meet the shipping industry's requirements. Our work with Trustwave, a cyber security subsidiary of Singtel, for example, has brought Fleet Secure into the industry as the first independent service designed to detect vulnerabilities, provide alerts, respond to threats, and protect ships from cyber attacks. In fact, Fleet Secure is a UTM, available without additional outlay on hardware which also has no impact on contracted bandwidth. It can identify external attacks through high-speed broadband connectivity, including malware introduced accidentally to the ship's local area network. It then isolates that part of the operating system infected to prevent wider disruption.

What makes for good cyber security practice

However, software is only part of the answer: cyber security and vigilance for 'the human element' and a well-thought-out recovery strategy to mitigate against multiple, automated assaults are also critical. Process failures and mistakes made by people can present the security loophole that, if unchecked by the UTM, can compromise the entire network. Weaknesses in the first line of defence (to phishing, plugging in an infected USB, downloading from an unreliable source, etc.) are common, but in the case of satellite-connected ships, it is also common to see updates turned off and no antivirus software in operation. Today, cyber security training is not compulsory for the world's 1.6m seafarers, while expertise in antivirus software is inevitably more likely to be based ashore.

As far as awareness is concerned, it is fair to say that there is likely to be more temptation to risk plugging in a memory stick that might be infected once a vessel is underway. Creating awareness for seafarers and staff is a continuous task because good cyber security practice is the shipping's first line of defence against a cyber intrusion.

Inmarsat has recently participated in discussions with academics at the World Maritime University in Malmö over what future classroom-based and e-learning cyber security course content might include for Maritime Safety and Security Diploma students. While Inmarsat is not and does not aspire to be a training company, it is, nevertheless, an interested party that's very much concerned with what's happening in the cyber domain. As such, we are fully aware that training is not just a tick box exercise and must be backed up with monitoring and reinforcement. We also know that using tools to identify breaches of policies, such as USB usage, help reinforce the message: constant reminders and real-life examples are often the quickest ways to stop a bad practice.

But to address future cyber security risks effectively, we need the involvement of ship designers, builders, regulators, verifiers, equipment manufacturers, service providers, and, of course, owners and operators. We were, therefore, one of the founding partners in a Joint Working Group run by the International Association of Classification Societies (IACS) whose members survey and certificate more than 90% of the world's commercial vessels, ensuring that ships are fit-for-purpose and comply with safety and quality regulations. The Working Group, which includes representatives from across the maritime sector, has developed a cyber security framework that is likely to form a basis for risk management that will contribute to future seafarer training requirements and the International Maritime Organization's International Safety Management (ISM) Code, a standard for the safe operation of ships. A further outcome is likely to be a recommendation relating to how a cyber security module can be best integrated into standard seafarer training courses, probably as part of the Standards of Training, Certification and Watchkeeping (STCW) Code.

For its own part, Inmarsat does issue guidelines covering best practice, but it is also evolving capabilities that support greater cyber maturity in the seafaring community, most recently through Fleet Secure Endpoint and Fleet Secure Cyber Awareness. The first of these has been developed together with digital security specialist ESET and is powered by Port-IT to protect desktop computers and other devices connected to shipboard networks and has been available since the beginning of 2019. Fleet Secure Cyber Awareness, meanwhile, has been developed in collaboration with Stapleton International and the Marine Learning Alliance to help seafarers educate themselves on the possible tactics that cyber criminals can use to infiltrate a company's IT infrastructure.

Over the line

There is no doubt that digitalisation and new smart technologies are transforming ship operation at an exponential pace, but Inmarsat's view is that to accelerate this transformation all stakeholders interested in optimising the efficiency of ships and crew welfare must exert themselves if the industry is to be carried over the line.

This means we must not only be training our seafarers more effectively, better managing our processes and protecting our systems but nurturing awareness of best cyber security practice, even on vessels that have little or no cyber security protection at all. Clearly, there is still a long way to go. ■