Photo courtesy of Inmarsat

Maritime gets with the program on cyber security

The maritime sector is well-known to be slow to respond to new cyber threats, as awareness remains low and training varies vastly form vessel to vessel. However, shipping's exposure to the NotPetya virus forcefully raised its awareness of the cyber threat. Inmarsat is working hard to ensure that the wake-up call moves an entire industry to action.

The recently-published UK Government 'Cyber Security Breaches Survey for 2017' of 1,523 private companies indicated that 46 percent of those canvassed had discovered at least one cyber breach or attack in the past year. Not surprisingly, 74 percent described cyber security as a high priority. However, few had taken steps to deal with the risk: Only a third had a formal cyber security policy, while just 20 percent of staff had attended any form of cyber security training.

A lack of preparedness

If the lack of preparedness raises alarm, it is trumped by ocean-going shipping – the industry responsible for delivering over 90 percent of world trade. A comparable Crew Connectivity Survey conducted by Futurenautics in 2017 on behalf of Inmarsat suggested that 87 percent of ships officers have received no cyber security training whatsoever.

Historically, shipping's lower participation in the Internet of Things (IoT) offers mitigation, but the vulnerabilities exposed in Maersk APM Terminals systems last year by NotPetya saw a startled industry suddenly wide awake to the threat delivered with new levels of highspeed ship/shore connectivity.

"Cybercrime is an inevitable downside of the digital economy, on land or at sea," said Peter Broadhurst, Senior Vice President of Safety and Security at Inmarsat Maritime, who oversaw the bringing to market of the Fleet Secure cyber security solution in the second half of 2017.

Broadhurst describes Fleet Secure as "the industry's first and - so far only - fully-managed service to detect vulnerabilities, respond to threats and protect ships from cyberattack, isolate infected areas on the network and protect against compromised USBs/devices." Integrated with Inmarsat's highspeed Ka-band/L-band Fleet Xpress, the

Peter Broadhurst, Senior Vice President of Safety and Security at Inmarsat Maritime

Unified Threat Management (UTM) service requires no additional outlay on hardware and has no impact on contracted bandwidth.

Fleet Secure is currently undergoing multiple server testing, with a first shipboard installation expected before the end of Q2 2018, according to Broadhurst. Inmarsat is also beta testing 'end-point protection,' to uphold security through ship network scanning and virus-protection at the user terminal level.

Complacency won't be shifted overnight

Broadhurst stresses that complacency on cybersecurity is unlikely to be shifted overnight, but adds that, already, he has noticed a profound change in attitudes among hardware installers. "It's fair to say that, in the past, there's been a tendency to use default passwords, but that has changed rapidly; we continue to reinforce the message with refreshers for our own guys and the installers to reinforce what's been in our training guide all along."

Less easy to address are the systems already in service, and Broadhurst points out that those upgrading connectivity routinely find that ship systems are infected in some way. "Although patching will have cleaned the system in many cases, there may be a little virus sitting in the network, so the first task will be a clean-up."

At the same time, the low crew numbers on board commercial ships today make them heavily reliant on self-managing systems. Broadhurst says that, whether delivered by email attachment or infected USB/device, the software weaknesses in PC network connections therefore give attacks like NonPetya a special kind of potency in the maritime context.

"As the vessel is operating on a satcomms link, updates can often be turned off, with no anti-virus software in place and old versions of Operating Systems in play," Broadhurst explains. It is into this environment that the common 'human errors' seen elsewhere (phishing, plugging an infected USB in, or downloading from untrusted source) are introduced.

"This is why cyber security at sea is not just about software patching and systems configuration; failures in processes and mistakes by people present a significant security loophole," says Broadhurst.

All this makes cyber security training for the world's 1.6 million seafarers a matter of urgency, he adds: "We are now starting to see a number of maritime focused training courses."

Getting the ground rules right

However, getting the training ground rules right will be essential. Broadhurst recently participated in discussions with academics at the World Maritime University in Malmö over what future classroom-based and e-learning cyber security

Inmarsat network operations centre

course content might include for Maritime Safety and Security Diploma students.

"Inmarsat is not a training company, but clearly we are an interested party in ensuring that cyber risk awareness is high, and that training is straightforward. Even where cyber security is being developed, there is still a failure to see how it applies at the individual level. Attitudes such as 'I'm not the target, it can't be me, we have security in place, or I will be protected by Anti-Virus software' remain embedded."

Inmarsat issues guidelines and best practices for crew to follow as standard but "I think that everyone agrees that, ultimately, cyber security training will become part of the STCW [Standards of *Training* Certification and *Watch*-keeping] Code requirements; the question now is how best to incorporate it," Broadhurst added.

Cyber training cannot be just a tick in the box

Inmarsat is party to the Joint Working Group on Cybersecurity run by The International Association of Classification Societies (IACS), whose members classify over 90 percent of the world's cargo carrying ships for design, construction and through-life regulatory compliance. The satellite group has retained Prof Paul Dorey, Director, CSO Confidential & Visiting Professor, Royal Holloway to act as group facilitator.

Cyber security risk assessments are expected to be included in the 2021 upgrade of the International Maritime Organization's ISM Code (the UN agency's maritime International Safety Management Code). Creating the 'risk map' for ISM will provide a platform to develop training for cyber-safe shipboard operations, Broadhurst says, with a JWG report expected to form the basis of an initial IACS submission on risk assessment to IMO.

The white paper 'Unchartered Waters,' written by Professor Dorey for Inmarsat to summarise issues observes: "We don't expect or desire identical standards to be developed everywhere, but consistency of approach to risk management would help a lot." IACS has broken the mapping process down into 12 principles, which include ship design, installation procedures, and support, and is seeking to establish a risk assessment procedure for ships being built today, before developing a practice for retrofitting.

In the interim, Broadhurst says he envisages developing short multi-lingual packages for seafarers which get the cyber risk message across by responding in an interactive way to the choices users made within different storyboard scenarios.

"Cyber training cannot be just a tick in the box; constant reminders and real-life examples are needed to raise awareness because this is often the quickest way to stop bad practice and establish cyber resilience." ■

Photo courtesy of Inmarsat

GVF Satellite. Solutions. The World.

● GVF serves as the unified voice of the international satellite industry ●

www.gvf.org