David Sinclair

Simulators can train mariners to protect against cyber attacks on shipboard systems

Tackling the **ship hacker**

USMRC wants to extend cyber-security training to curb the risks to vessels at sea, reports *John Gallagher*

An incident in which drug traffickers hacked into a container terminal at the port of Antwerp is often used to illustrate the importance of cyber security in the maritime sector. But a US-based training facility wants as much attention paid to the risk of cyber attacks on ships.

The US Maritime Resource Center (USMRC) in Middletown, Rhode Island, is developing a programme for mariners that it believes will not only raise awareness of shipboard hacking but help prevent it.

"If Citicorp and the White House can be hacked, I would dare venture to say a ship can too," Alex Soukhanov, vice-president of international shipping and maritime operations at USMRC, told *IHS Maritime*.

Soukhanov is in a position to know the cyber risks for seafarers. He is also a master mariner and a practising ship pilot in New England, with experience piloting tankers through Buzzards Bay, Massachusetts, reefer ships from North Africa, and passenger vessels to and from islands off of Cape Cod.

"There have been some shipboard incidents, mainly regarding AIS spoofing and other disruptions of GPS," he said. "And there may have been some isolated incidents reported. But then again, how would you know you're being hacked unless you're being told that you are?"

Key points

- USMRC is working on 'assurance framework'
- IMO draft guidelines seen as too 'broad'

As an operational risk research firm, USMRC is spearheading technical research to develop a maritime 'cyber assurance framework' through partnerships with industry groups such as class societies, flag states, shipowners, ship operators, and insurers.

Building momentum for the effort has been a challenge, however, mainly because USMRC is basically starting from scratch. Soukhanov pointed out that the IMO's draft guidelines published in March are the first maritime standards for dealing with cyber security holistically.

"But even those are just recommendations and are very broad and general, especially when having to consider a vast industry such as the maritime sector," he said. "When you consider that over 90% of the world's cargo moves on the ocean, and this communications medium has no global standards, it tends to stand out as a risk."

So many systems are Ethernet-based, or are integrated with systems that are, that disruptions to shipboard operations can be almost infinite, he said. Assessing shipboard cyber risk can start with the electronic chart display information system (ECDIS), but systems including cargo management, engine performance, remote access monitoring of engineering systems, and dynamic positioning can all be either integrated or connected to the internet or influenced by updates through removable media.

No vessel type, at this point, appears to be especially vulnerable or resistant to an attack. "Every ship is configured differently, which is the big challenge," said Soukhanov. He lists "interdisciplinary concerns" of "cross-cultural concerns, different registries, different insurance, different ownership parameters".

USMRC has started working with the Liberian Registry and Class NK to tackle the problem. "This is a complex issue, but we first wanted to build some partnerships to bring in the best and brightest to help analyse this," he said. USMRC is looking to have a mariner training programme for shipboard cyber-security risk in place by the end of summer or early autumn.

Building awareness of shipboard cyber security, while developing a cyber-security training programme for mariners, should be headed by the maritime industry rather than mandated by regulation, he added.

"The maritime industry knows its systems better than anyone else and, with the wide variety of configurations out there, it really must be an industry-centric approach," he stressed. "In addition, the shipowners are really the customers here. They have systems that they have purchased and installed on their ships and trust that they're true and reliable. Mariners are in the same situation as the owners, because they're the ones who use the systems, and assume they're true and reliable."

Unfortunately, Soukhanov cautions, there are currently no incentives across the industry to prove the resilience of these systems against a cyber attack. "That's a concern for us," he said.

john.gallagher@ihs.com
Published online 28/5/2015