Cyber Security

WAKE UP CALL

Image: © SOCP Information Systems Security Awareness CBT. To obtain your free copy of the ISSA CBT, please contact the SOCP at programadmin@socp.us

Mariners Urged to Get In Front of Growing Threat

By Patricia Keefe

Before any vessel gets ready to head out to sea, shore-based personnel and onboard crew run down a lengthy list of safety, compliance and regulatory checks, all part of a standard risk management exercise. What's often not on that list is an invisible, but looming risk that if ignored, could leave ships off course, off schedule or even dead in the water, thanks to infected computer systems, phony or corrupted charts and blocked communications signals.

Cyber crime has come of age in the maritime sector. Observers like Futurenautics claim the maritime industry is actually "overexposed" when it comes to cyber risk management. From modern vessels virtually run by massive doses of technology and limited crew, to older ships chugging along with out-of-date and insecure applications, all are vulnerable in their own way to the stealth threats to shipping security and safety. The seeming lack of awareness among companies, if not their crews, has many government, security and industry organizations very concerned, and very anxious to help the industry get out in front of this looming problem.

> "It has to start with the leadership first – if they aren't willing to effect change – you can't educate employees."
>
> – Michael Crean, CEO, Solutions Granted, and Bluetide Communication's security partner

The last two years has seen a flurry of activity around cyber security. With zero funding, the U.S. Coast Guard pulled about 80 personnel with the necessary security and IT credentials out of other units to form the U.S. Coast Guard Cyber Command. Last August, it released a Cyber Security strategy paper, which provides a framework and a 10-year plan designed to reduce risk to the maritime cyber critical infrastructure.

Industry alliances, including BIMCO, CLIA, Intertanko, Intercargo, ISC and others, recently published "The Guidelines on Cyber Security Aboard Ships," a blueprint for companies seeking to aggressively address cyber security. Separately, Insurers Marsh & McLennan Companies published a cyber security report targeted at educating executives, while Futurenautics surveyed 3,000 crewmen on their experiences with cyber attacks. Last December, International Association of Classification Societies (IACS) leadership added cyber security as the third pillar of its oversight, alongside hull and machinery, and talked about creating a cyber system safety framework.

Where's the Fire?

What could possibly happen to a vessel out in the middle of the ocean? A lot, actually, thanks in part to the industry's increasing reliance on technology. A look at the incidents reported so far – ranging from fake charts and invoices, to drug smuggling, to compromised rigs and ship systems – is just the tip of the cyber iceberg lying in wait for a modern-day unprepared Titanic, worry security experts.

The attacks run the gamut, employing phishing, social engineering, malware, viruses, worms, denial of service, keystroke capture, skimmers, Trojans, ransomware, signal jamming, identity, manifest and corporate data theft, cargo diversion and smuggling, phony bills, etc. While SATCOM vendors like KVH and Bluetide Communications enable clients to block web sites, divvy up and even physically separate internet bandwidth to meet business, personal and entertainment demands, it's not enough to bar the cyber door. One unsettling truism is that hackers are always a generation or two ahead of their victims.

Crew data, financial data, cargo manifests and high value cargoes are all at risk. Fake invoices are said to be epidemic in the bunker fuel sector. From a safety standpoint, protecting and backing up your electronic navigation systems and GPS signal will be key.

A wide range of players, from criminal syndicates looking for money; to political or environmentalist hacktivists bent on making a statement or stopping a company's activities; to corporate and nation-state espionage that seeks to steal information and cripple economies; and even just lone wolves looking to build street cred or test their skills, are all in on it. And they don't need to be particularly sophisticated. Attacks can be outsourced to hackers for hire, the new career path on the dark side.

Your Own Worst Enemy

It might surprise some, but the cyber security community sees employees both as a bigger problem than technology, and the key to success. The SANS Institute, a bellwether provider of security training, has a program devoted to "securing the