MARITIME REPORTER AND ENGINEERING NEWS

Tel 352 692 5493
Fax 352 692 5494

Dennis L. Bryant
Bryant's Maritime Consulting
4845 SW 91st Way
Gainesville, FL 32608-8135

December 2013

Marine cybersecurity

Dennis L. Bryant

On 12 February 2013, President Obama issued Executive Order 13636 – Improving Critical Infrastructure Cybersecurity. Citing repeated electronic intrusions into critical infrastructure, the document states that it is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with US private sector entities so that these entities may better protect and defend themselves against cyber threats. It directs the Secretary of Homeland Security (DHS), in coordination with Sector-Specific Agencies, to establish the Voluntary Critical Infrastructure Cybersecurity Program together with the owners and operators of critical infrastructure and other interested entities. If current regulatory requirements are deemed to be insufficient to protect critical infrastructure from electronic intrusions, the Sector-Specific Agencies are to propose prioritized, risk-based, efficient, and coordinated actions to mitigate cyber risk.

The prefix "cyber" is derived from a Greek adjective meaning skilled in steering or governing. The prefix is commonly used in the computer and electronic context to denote control. Thus, cybersecurity means control of computer or electronic security.

The National Institute for Standards and Technology (NIST) has developed a Preliminary Cybersecurity Framework (on the web at http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf). It provides guidance to public and private organizations on managing cybersecurity risk. The objective is to encourage organizations to consider cybersecurity risk as a priority similar to financial, safety, and operational risk, while factoring in larger systemic risks inherent to critical infrastructure.

The DHS has established a Cybersecurity Training & Exercises Website (on the web at http://www.dhs.gov/cybersecurity-training-exercises) to assist organizations in becoming familiar with and staying current on cybersecurity threats and available countermeasures. The site itself, though, is frequently outdated.

Of more relevance to the maritime community is the US Coast Guard cybersecurity site accessible through Homeport. I have to admit that I am not a fan of the Coast Guard's broad use of the Homeport website. Few things on the site are directly accessible. To get to the cybersecurity site, go the Homeport (on the web at https://homeport.uscg.mil), then click on

E-mail dennis.l.bryant@gmail.com
Internet http://brymar-consulting.com/

Maritime Security under Missions on the left side of the screen, and then click on Cybersecurity, the third topic down in the center of the new screen. The site provides access to a variety of background documents and links to other cyber-related websites.

The National Infrastructure Protection Plan (NIPP), (available on the web at https://www.dhs.gov/sites/default/files/publications/NIPP_Plan.pdf), provides overall guidance regarding government efforts and recommendations for protection of critical infrastructure. Implementing that overall plan are 18 sector-specific plans, including the Transportation Systems Sector-Specific Plan (TSSSP), (available on the web at http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf). In accordance with Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience, the Department of Homeland Security and the Department of Transportation serve as co-chairs of the Transportation Systems Sector. The US Coast Guard advises the co-chairs on maritime issues.

The Coast Guard has included cybersecurity issues in its various Area Maritime Security Plans. It also hosts the Cybersecurity Homeport Community. To join the Community, you must already have a Homeport account. You then send an email to homeportcyberscurity@uscg.mil, asking to join. Members are provided with recommendations and activities helping them keep abreast of cybersecurity issues.

All of this may appear overwhelming to a ship owner or operator. After all, what is the likelihood that a terrorist will target your particular company or vessel or facility? Admittedly, the odds are low, but not zero. We know from the terrorist attacks of 11 September 2001, as well as the maritime attacks on the destroyer USS Cole in Aden on 12 October 2000, the supertanker Limburg off Yemen on 6 October 2002, and the supertanker M Star in the Strait of Hormuz on 28 July 2010, that terrorists seek soft targets. Marine facilities have not been exempt from terrorism, with attacks on Ashod, Israel (13 March 2004); the Iraqi Khawr al Amaya crude oil terminal (24 April 2004); and the Karachi East Wharf in Pakistan (26 May 2004). If your company or vessel or facility appears to be hardened, the terrorist will probably go elsewhere.

There is plenty of evidence that the average maritime company or vessel or facility is vulnerable, particularly to a cyberattack.

Terrorism aside, there is a selfish reason for hardening your company, vessel, or facility against cyberattack. By taking such steps, you also may harden your operation against such threats as spurious electronic signals, malicious activity, industrial espionage, and criminal activities.

On 10 May 1993, the Coast Guard promulgated a regulation that came into effect on 9 July 1993 providing, among other things, that tankers equipped with an integrated navigation system (INS) could, under certain circumstances, use the INS with the auto pilot engaged while in the navigable waters of the United States. A suspension of the effectiveness of that regulation was issued on 6 July 1993 after a vessel utilizing its INS experienced a sudden, unintended, and drastic course change when the INS malfunctioned as a warship in the vicinity emitted a strong

electromagnetic pulse. In its suspension order, the Coast Guard stated that currently (in 1993) "there is no performance standard for a shipboard INS in terms of accuracy, integrity, or reliability. Although the Coast Guard recognizes that the use of INS with an autopilot offers the potential to improve navigation safety, adequate testing and evaluation of this technology has not been conducted. The Coast Guard intends to conduct further rulemaking concerning necessary testing and methodology for certifying that performance standards have been met and will provide further opportunity for public input." There have been no further developments regarding INS performance standards since 1993.

In the June 2003 edition of Maritime Reporter & Engineering News, I authored an article entitled: "AIS – Panacea or Pandora's Box". I pointed out that, when operating as intended, the Automatic Identification System (AIS) was an important navigational safety tool, particularly with respect to collision avoidance. I also pointed out, though, that because of the way the transceiver was configured, much of the data being transmitted could be manipulated. Specifically, I questioned reliance on AIS as a maritime security tool. I didn't know the half of it. It has recently been demonstrated that spurious AIS signals can be transmitted showing vessels to be far from their actual location and on incorrect courses and speeds. AIS signals can also be generated showing phantom ships. One can no longer inherently trust the AIS signals being received by your transceiver and displayed on your ECDIS. The system needs to be revised to incorporate an authentication program.

In the September 2013 edition of this same magazine, I authored an article entitled: "GPS spoofing". I pointed out that it is now possible to spoof Global Positioning System (GPS) and other space-based positioning, navigation, and timing (PNT) services. As with AIS, these PNT services must incorporate an authentication system or adopt other measures to avoid accidental or intentional presentation of erroneous data. Work is currently underway to address these issues. Even then, it will likely only make spoofing more difficult, but not impossible.

I do not claim to be prescient. I am only reporting the work of others, more technologically proficient than myself. I am saying, though, that steps should be taken by members of the maritime community to enhance their cybersecurity. There is a growing threat to marine safety, security, and environmental protection from the over-reliance on electronics to accomplish operational tasks. Adopting appropriate cybersecurity measures will reduce business risks.