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

February 2016

Maritime cybersecurity

Dennis L. Bryant

The maritime community is no more immune from cyber threats than any other entity that relies on computers and the internet.

The maritime industry, though, constitutes part of the world's critical infrastructure. Thus, the consequences of a successful cyber-attack on a maritime entity could be far greater than a successful cyber-attack on, for instance, a bakery.

Consequently, it is important that the maritime sector and its numerous constituents adopt reasonable measures to deter, detect, and recover from cyber-attacks.

Currently, much of the world's attention is focused on terrorism. Cyber-attacks by terrorists are a real threat and steps must be taken to counter them. More commonly, though, cyber-attacks are launched by criminals, nation-states, and corporate spies. While the different groups have different motivations for cyber-attacks, the methodologies are basically the same – find a weakness and exploit it to gather information, steal monies or property, and/or disrupt operations.

While a robust cybersecurity plan may not totally stop a determined and sophisticated cyber-attack, it will cause most attackers to seek a softer target. Thus, the goal of a vessel, waterfront facility, or other maritime entity should be to have the best or one of the most robust cybersecurity plans available. A consortium of international maritime associations recently posted guidelines for cybersecurity onboard ships, intended to complement IMO requirements and company plans and procedures, while focusing exclusively on unique shipboard issues.

The US Coast Guard has been working diligently to enhance its cybersecurity plans and programs. In June 2015, the agency posted its Cybersecurity Strategy. It has also taken a number of steps to harden its communications and information technology (IT) structure.

For several years, the Coast Guard has been urging the maritime community to adopt cybersecurity plans. The problem is that no two vessels, waterfront facilities, or other maritime entities are the same. Some have only very basic computer systems, while others have highly sophisticated systems with dedicated in-house IT staffs. Some have converted their operations to

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

be heavily dependent on computerized coordination and interaction, while others use electronics only as an adjunct to traditional operations. Thus, one cybersecurity plan will not be able to address the myriad situations.

While it is vital that each element in the maritime sector adopt a cybersecurity plan, it is obvious that each cybersecurity plan be tailored to address the circumstances of that particular entity.

The Coast Guard has issued guidance to its field units and the Area Maritime Security Committees (AMSCs) regarding cybersecurity plans. In October, the House Committee on Homeland Security conducted a hearing entitled: "Protecting Maritime Facilities in the 21st Century: Are Our Nation's Ports at Risk for a Cyber-Attack?" A bill is pending in Congress that will, if enacted, provide the Coast Guard with specific authority to mandate cybersecurity plans within the maritime industry.

The Coast Guard seems to favor the legislation, but at the same time believes that it has in the Maritime Transportation Security Act of 2002 (MTSA) sufficient authority to get the job done. A recent federal appellate court decision supports that position. In that matter, the Federal Trade Commission (FTC) brought suit against a major hotel chain alleging that the defendant's cybersecurity program was insufficiently robust to protect its clients against hackers. The hotel chain defended itself by asserting that, while the Federal Trade Commission Act prohibited "unfair or deceptive acts or practices in or affecting commerce", it provided the FTC with no authority regarding cybersecurity. Evidence showed that, prior to the litigation, the hotel chain had been the subject of at least three computer hacks in which clients' financial information had been stolen. The court held that Congress had given the FTC a broad mandate and that it was not inappropriate or unreasonable for the FTC to interpret that mandate to include cybersecurity.

A similar situation exists regarding the Coast Guard and the MTSA. In that statute, the Coast Guard is given responsibility of deterring and responding to a transportation security incident, defined as a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area. The MTSA also gives the Coast Guard specific authority to require covered vessels and facilities to prepare and submit for approval security plans that include provisions for establishing and maintaining physical security, passenger and cargo security, and personnel security; establishing and controlling access to secure areas; procedural security policies; communications systems; and other security systems (emphasis added). Given today's environment, there is little doubt at, if litigation ensued, a court would uphold the authority of the Coast Guard to require that security plans of covered vessels and facilities include a cybersecurity component.

The problem for the Coast Guard is, as noted above, no one cybersecurity plan will be appropriate for all vessels and facilities.

Thus, it is likely that any initial cybersecurity plan requirements adopted by the Coast Guard will be vague. As experience and capacity develops in this arena, those requirements will become more specific and meaningful. The maritime sector will, with encouragement and a little

prodding, implement increasingly robust cybersecurity measures, further protecting itself from hackers of all persuasions.