Maritime Cybersecurity: A Growing Threat Goes Unanswered

Posted on October 22, 2014 by Blank Rome LLP
Reply
By Steven L. Caponi and Kate B. Belmont

The maritime industry may be one of the oldest in the world, but in-depth reports issued by the United States Accountability Office (“GAO”) and the European Network and Information Security Agency (“ENISA”) confirm that our industry is as susceptible to cybersecurity risks as the most cutting-edge technology firms in Silicon Valley. With the ability to commandeer a ship, shut down a port or terminal, disclose highly confidential pricing documents, or alter manifests or container numbers, even a minor cyber attack can result in millions of dollars of lost business and third-party liability. Unfortunately, cybersecurity on board merchant vessels and at major ports is 10 to 20 years behind the curve compared with office-based computer systems and competing industries throughout the world. Like other industries critical to the global economy, such as the financial services sector and energy, it is time for the maritime industry to adopt a proactive response to the growing cybersecurity threat.

Economic and Security Perspectives

Although not yet treated as a significant business risk, cybersecurity has for some time been viewed as a considerable threat by the governmental agencies responsible for both national and international maritime security. In late 2011, ENISA issued a sobering report focused on the cybersecurity risks facing the maritime industry, and provided recommendations for how the maritime industry should respond. Unfortunately, the most recent report issued by the GAO in June of this year confirms that the threat has grown more significant, but that the maritime industry has failed to make cybersecurity a priority. Copies of both the ENISA and GAO reports can be obtained by visiting Blank Rome’s cybersecurity blog, Cybersecuritylawwatch.com.

ENISA was prompted, in part, to issue its 2011 report because the maritime sector is universally viewed as critical to the security and prosperity of European society. ENISA noted that in 2010, 52 percent of the goods trafficked throughout Europe were carried by maritime transport, compared to only 45 percent a decade earlier. The ENISA report further noted that, throughout Europe, approximately “90% of EU external trade and more than 43% of the internal trade take place via maritime routes." The industries and services belonging to the maritime sector are responsible for approximately three to five percent of EU Gross Domestic Product. This vast amount of trade flows into and out of the numerous ports located in 22 EU member states.

From both an economic and security perspective, the ability to disrupt the flow of maritime goods in Europe or the United States would have a tremendous negative impact on the respective local economies, and would also be felt worldwide. According to ENISA, "The three major European seaports (i.e., Rotterdam, Hamburg, and Antwerp) accounted in 2010 for 8% of overall world traffic volume, representing over 27.52 million TEUs." Additionally, these ports "carried in 2009 17.2% of the international exports and 18% of the imports." For its part, the GAO noted that, as an essential element of America's critical infrastructure, the maritime industry "operates approximately 360 commercial sea ports that handle more than $1.3 trillion in cargo annually." The Long Beach port alone services 2,000 vessels per year, carrying over 6.7 million TEUs, which accounts for one in five containers moving through all U.S. ports. Long Beach ranks among the top 21 busiest ports internationally, with significant connections to Asia, Australia, and Indonesia.

Given the interconnectivity of the maritime industry and paramount need to keep ports moving with speed and efficiency, a cyber attack on just one of the major EU or U.S. ports would send a significant negative ripple throughout the entire industry. With the ability to impact so many nations and peoples at once, the maritime industry presents a fruitful target for both private and political actors. Threats of cyber attacks can range from rival companies, to those wishing to advance a political or environmental agenda, to nation states advancing a national agenda, to terrorist organizations, and even cyber attacks from pirates or freelance hackers.

What Would a Cyber Attack Look Like?

Both the GAO and ENISA agree that the soft underbelly of the maritime industry is its reliance on Information and Communication Technology ("ICT") in order to optimize its operations. As was clearly noted by ENISA, ICT is increasingly used by all levels of the maritime industry "to enable essential maritime operations, from navigation to propulsion, from freight management to traffic control communications, etc." Examples of these technologies include terminal operating systems, industrial control systems, business operating systems, and access control and monitoring systems. ICT systems supporting maritime operations, from port operations management to ship communication, are commonly highly complex and utilize a variety of ICT technologies.

Further complicating cyber defense efforts, ICT systems used by ships, ports, and other facilities are frequently controlled remotely from locations both inside and outside of the U.S. Presenting an even higher level of concern, some ports have adopted the use of automated ground vehicles and cranes to facilitate the movement of containers.

Consistent with the threat facing other critical infrastructure sectors, cyber threats to the maritime industry come from a wide array of sources. As noted by the GAO, these include:

"Advanced persistent threats—where adversaries possess sophisticated levels of expertise and significant resources to pursue their objectives—pose increasing risk. Threat sources include corrupt employees, criminal groups, hackers, and terrorists."

While the source of the threat may vary, there is no doubt that the desire and willingness to act against the maritime industry is real. Major shipping companies have already begun to suspect that they have been victims of deliberate hacking attacks. It is well known that between 2011 and 2013, there was a cyber attack on the port of Antwerp orchestrated by organized criminals who breached the port IT system, facilitating the smuggling of heroin and cocaine.

Government and Industry Response

Numerous governmental agencies in both the EU and U.S. are starting to respond to the cyber threats facing the maritime industry. They have not yet, however, promulgated concrete guiding plans and policies. Instead, the governmental agencies have assumed the role of loudly sounding a clarion call to action and taken a supporting role for industry participants. Responsibility to actively defend against the risks of a cyber attack and be in a position to effectively respond to an incident rests squarely on the shoulders of individual ship owners, shipping companies, port operators, and others involved in the maritime industry. The failure to assume this responsibility will undoubtedly lead to serious and potentially devastating consequences, including government fines, direct losses, third-party liability, lost customers, and reputational damage that cannot be repaired.

Mitigating the Threat

Companies looking to learn more about the steps they can take to meet the evolving cyber threat head-on should consult with cybersecurity professionals and available literature. Widely available resources include the National Institute of Standards and Technology, which issues the Framework for Improving Critical Infrastructure Cybersecurity and the National Infrastructure Protection Plan ("NIPP"), developed pursuant to the Homeland Security Act of 2002 and Homeland Security Presidential Directive 7 ("HSPD-7"). These documents, along with numerous others, can assist companies in developing a risk management framework to address cyber threats and use proven risk management principles to prioritize protection activities within and across sectors.

Online article; Cyber Law Watch; www.cybersecuritylawwatch.com; 22 Oct 2014; aritime Cybersecurity: A Growing Threat Goes unanswered; http://cybersecuritylawwatch.com/; accessed 12 November 2014