Published by Cyber Magazine, 23 July 2017,
http://magazine.milcyber.org/stories/cybermakingwavestheneedformaritimecybersecurityframeworks

Cyber Making Waves: The Need for Maritime Cyber Security Frameworks

By Ian W. Gray

90% of the world's goods are shipped via the oceans on over 51,000 merchant ships belonging to multiple different countries. For the last several years, the International Maritime Organization (IMO), a specialized agency of the United Nation concerned with the safety and security of international shipping, has been discussing the possible implications of cyber-attacks to global commerce. This has been prompted by multiple developments within the Maritime Industry. As ships, port terminals and businesses become more interconnected, they also risk becoming more vulnerable to cyber intrusions and possible attacks. However, the maritime industry has not had a significant cyber incident that could help quantify the possible losses, until recently.

In June 2016, the IMO published Interim Guidelines on Maritime Cyber Risk Management (MSC.1/Circ.1526) with the intent to provide a risk management framework and prevent large-scale cyber-attacks that could potentially endanger lives, affect the availability of network based shipping systems, or stall global trade. These threats manifested themselves on June 27, 2017 when A.P. Moller-Maersk was affected by a strain of ransomware dubbed "Petya."

The Petya ransomware exploited the same Microsoft Windows vulnerability (Eternal Blue) from the WannaCry ransomware strain that infected thousands of computers in May 2017. That ransomware spread through a patched vulnerability that was unavailable for unsupported versions of Windows. The attack was likely not targeted towards Maersk, spreading throughout organizations with operating systems that are beyond their lifecycle.

The ransomware spread through a file-sharing bug that affected organizations around the world, encrypting hard drives and halting critical business operations. Petya had a similar effect on the Danish shipping company, forcing them to shut down systems to contain the attack. Though Maersk's ships were able to safely maneuver, Maersk's APM Terminal units, which serve 76 port and terminal facilities in 59 countries, were unable to load or unload cargo in select sites around the globe. Several major ports were

impacted, including the Port of Los Angeles, Port Elizabeth in New Jersey, the Jawaharlal Nehru Port Trust near Mumbai, affecting their ability to clear cargo.

The attack came just days after the Maritime Safety Committee (MSC) 98 meeting in June 2017 where a paper (MSC 98/5/2) proposed making cyber risk management onboard ships as mandatory, where previous International Union of Marine Insurance made these requirements voluntary. The guidelines for these risk assessments were developed by shipowner association and classification societies such as Baltic and International Maritime Council (BIMCO), the International Chamber of Shipping (ICS), Intertanko, Intercargo and Cruise Lines International Association (CLIA). These organizations exist to maintain standards throughout the maritime industry, among international stakeholders and governmental organs like the IMO.

The cyber risk management proposal arrives as the shipping industry is leaning heavily towards digitization and automation. In May 2017, Maersk published a statement announcing that they were partnering with IBM to digitize their administrative processes and transactions with blockchain technology. The blockchain will help track shipments around the world through a universal ledger and transition to a paperless system that will keep a reliable and secure record of shipping transactions.

Other partnerships with companies like Microsoft similarly promise to streamline supply-chain management and lower operational costs through data science. Additionally, several shipping companies are beginning to test autonomous operations onboard ships to increase safety and efficiency. Such autonomous systems would likely include cargo handling and navigation, while the drive to lower operational costs could possibly automate the entire shipping process.

While the industry is developing in a direction that will likely increase efficiency and decrease costs, the necessary safeguards to protect these automated systems is not fully realized. The Petya ransomware illustrated the potential effect of a cyber-attack on a major shipping company and port terminals. The attack could have been far more severe, affecting navigation or engineering systems on merchant ships with possible threat to human life or the environment.

If ship owners begin to take accountability for cyber security, the industry is likely to progress towards a less vulnerable state. The cost and initiatives to harden their digital infrastructure will take a considerable amount of time and resources. These actions will require, at the least, significant threat modeling to include additional measures like penetration testing, table-top exercises, and periodic audits. The progressive move towards an automated and digitized shipping infrastructure increases the urgency of

these corrective actions, as existing vulnerabilities could be exploited by attackers for financial gain or strategic objectives.

The proposal (MSC 98/5/2) for the MSC 98 advocated for ships to identify cyber risks and implement safeguards. Additional recommendations from MSC.428(98) recommended that cyber safeguards take effect under the International Safety Management (ISM) Code, with a deadline of 1 January 2021. Owners risk having their ships detained if they fail to meet the ISM standards for cyber risk. However, the potential for a cyber-attack on these ships could also prevent them from safely pulling into port.

While there have been previous incidents of cyber-attacks on merchant shipping, whether targeted or proof-of-concept, the Petya ransomware illustrates the potential large effect of a piece of ransomware. The 1 January 2021 date is a practical deadline for ship owners to implement cyber risk management frameworks; however, it is currently unclear if existing cyber practices can meet the rapid pace of new technology onboard ships. The shipping industry will have an upstream battle to implement safeguards and identify methods to assess vulnerabilities. The consequences of failure to meet these standards could affect not only the ship owner, but global commerce.

Nearly a week after the initial attack, Maersk resumed normal port operations. The shipping company has not yet assessed the financial damage of the cyber incident, though it significantly affected its ability to load and unload cargo. Multiple bookings had to be cancelled, and Maersk needs to deal with settlements and liability issues with individual shippers. However the cyber incident is quantified, ultimately the effects were felt throughout the world. This attack has created a sense of urgency to implement new controls, and hopefully they can be met before the 2021 deadline.

About the Author

Ian W. Gray is a senior intelligence analyst at Flashpoint, where he focuses on producing strategic and business risk intelligence reports on emerging cybercrime. Ian is also a military reservist with extensive knowledge of the maritime domain and regional expertise of the Middle East, Europe, and South America.

Photo credits: All photos within article from Wikipedia Commons