Safeguarding the Shipping Industry: Addressing the Growing Threat of Cyber Attacks

The shipping industry is undergoing a much-needed transformative digital upheaval, with the widespread adoption of electronic systems for navigation, cargo management, and communication. However, this steep inclination towards technology has also made the industry more vulnerable to various cyber threats. Of late, several high-profile cyber-attacks on multiple shipping companies have put a glaring spotlight on the need for robust cyber security measures in the shipping sector.

Recently, on 07th January 2023, ***DNV***, a major Norwegian shipping classification society, confirmed that their systems were hit by a malicious ransomware attack, subsequently impacting around 1,000 ships under their banner. ***DNV*** issued a statement wherein they disclosed that a pivotal software, ***ShipManager*** was primarily targeted by file-encrypting malware, forcing the organization to suspend operations and shut down their servers. Also, they further added that around 70 clients were directly affected by the attack, accounting for almost 15% of the total vessels liable under their management.

A critical aspect of cyber security in the shipping industry pertains to supply chain. Shipping companies must be vigilant and be aware of the security measures adopted and implemented by their partners, including suppliers, shipping agents, and terminal operators. A weak link in the otherwise sturdy supply chain can topple and crumble the entire network, putting everyone involved at risk.

In order to minimize the risk of such a mishappening, we at ***Verifavia*** (*a part of Normec group*), have implemented a multi-faceted ***Cyber Defense Plan***. Our system firewall works around the clock permitting only secured, verified and virtually non-threatening traffic in and keeping any dangerous or suspicions traffic at bay. Furthermore, we use one of the most secured and dependable cloud services, we ensure all our systems are up to date with the latest antivirus and antimalware systems in the market and we ascertain regular backup of vital data is taken periodically to prevent any unwarranted data loss, thus, minimizing the unforeseeable impact, lest any intruder is successful in his motive to invade.

Additionally, all incoming emails to our systems pass through a stringent email defender which automatically filters out and quarantines even remotely skeptical and fraudulent emails, which if left unchecked, eventually lead to unsuspected major infiltrations such as phishing, malware or ransomware attacks. We have also established, verification via a 2-factor authorization for all logins into the network, applicable to all employees irrespectively. One cardinal aspect in the implementation of this process is training and certification of our employees through multiple online tests and keeping everyone at par with developments on *Cyber Security* with emphasis on the *Dos and Don'ts* that one must adhere to at all times.

In conclusion, the shipping industry's growing sensitization to digital portals has also paved way for ever growing cyber security threats, hence, it is imperative for companies to take prognostic steps to protect against such threats:

- Effective holistic implementation of security network
- Relaying basic cyber security training to employees
- Liaising with partners to assess and to mitigate potential cyber security risks

By accomplishing a dynamic, all-encompassing approach towards cyber security, the shipping industry can safeguard all of its vital operations and protect itself against the ever-growing threat of cyber-attacks.

- Taranjeet Singh Puri, Marine Engineer, IHM Maintenance Executive