2017

The flipside of industrial 4.0 – Cyber security risk

Pratichi Rajan Mallick
World Maritime University

The Flipside of Industrial 4.0 – Cyber Security Risk

Name	: Pratichi Rajan Mallick
University	: World Maritime University
Specialization	: Shipping Management and Logistics
Expected Date of Graduation	: 5th November 2017
Email ID	: s17077@wmu.se
	pratichi.m6857@gmail.com
Phone No.	: +46 725682359

Introduction

In the current scenario of market volatility and globalization, the shipping industry is under immense pressure in terms of growth, revenue expansion, trading condition and cost optimization. From the advent of steam powered vessels to the current fiasco of autonomous vessel, the industry has evolved albeit slowly to a data focused industry. The wave of data collection, sharing and utilization to optimize operations via automation is the next phase of industry revolution, Industry 4.0. The convergence of real and virtual worlds as a result of digitalization has been a crucial driver of change and innovation in the shipping sector. Data has been elemental in developing sustainable mobility and logistics helping companies like Maersk, securing a competitive position. The Age of industry 4.0, which is based on platform-based cooperation between liners, ports and logistic service providers and innovation based strategy incorporating weather and traffic data to optimize operation exposes companies to many challenges.

Apart of the traditional nature of shipping which is inert to changes, the introduction of disruptive technology amalgamated with the competitive nature to be the first mover in a data driven and interconnected ecosystem, exposes all the players to a multi-dimensional cyber-security threat. Logistical (Vessel automation, Container tracking) and infrastructural (Port operations, Vessel management) systems are under a tremendous risk of cyber attack. Though change is good, this essay posits a devil's advocate perspective to the digitalization in shipping and required changes to mitigate these challenges.

Cyber Security Risk in Shipping

A clustered industry consisting of manufacturers, owners, operators, port authorities, logistic service providers, the container sector which generates enormous amount of data, is vulnerable to cyber risk which not only threatens security but also the safety of the vessels. Information technology (IT) and operational technology (OT) in the sector are increasingly being networked together (BIMCO, 2016). This not only pose data security threats but also safety risks. The Petya-Ransomware for example, an untargeted attack disrupted all of Maersks operations in 76 ports on 27th of June, 2017. The affects on Maersk Line, one of the front-runners in IT-development, is a warning sign to the entire maritime industry (Reuters, 2017). In an asset heavy and capital intensive industry with innumerous moving parts, the system with a large number of end users is wide-open to untargeted (Phishing, water holing, ransomware) and targeted (Spear-phishing, Deploying Botnets, Subverting system) attack (BIMCO,2016). One must understand Digitalization and Cyber Risks are two-sides of the same coin.

The Chrysler Car-hacking system highlighted the risk of autonomous vehicles, ships with systems including software to run engines, electronic chart displays and information system, global position system et al are highly vulnerable to hostile take over or disruption of maneuvering ability. Hacktivist can hack systems, and minor changes like stowage plans can risk the physical safety of the vessel. At high seas, GPS jamming could be the next level of piracy. Currently, the threats and safety requirements in ISPS, SOLAS, ISM highlight a strong focus on physical security and minimal focus on cyber security. The regelation of cyber risk to the IT departments instead of acknowledging it as a systemic risk in the current stage of digitization is startling. Though the IMO FAL committee has issued “GUIDELINES ON THE FACILITATION ASPECTS OF PROTECTING THE MARITIME TRANSPORT NETWORK FROM CYBERTHREATS”, a more regulated cyber security system needs to be incorporated in the maritime sector. Complacency in this matter is counteractive to sustaining a smooth logistic infrastructure. Addressing cyber infrastructure and investing to safeguard maritime industry is crucial in the changing ecosystem.

Mitigating Cyber Risks

As an industry moving towards a connected cloud based environment cyber security becomes fundamental element of risk management. In a hyper-dependent supply chain, cyber risk as mentioned above are systemic and disruptive due the domino effect. From a merge topic to be discussed at conferences, there is an urgent need to dwell in regulating and standardizing cyber safety. Although the IMO FAL committee guidelines offers shipowners and operators guidance to assess and maintain security on board ship, a need for more collaborative approach involving all stakeholders like manufacturer, port operators and service providers is imminent. There is also a need to expand IT teams specific to various departments in shipping. Sensitive Data breach from damage or disposed hard disks, within companies can also have serious consequences (Greenberg, 2010). As Lars Jensen, CEO SeaIntelligence consulting pointed out, most organization can tackle cyber security threats using the current tools, but its often a matter of ensuring systems are update and security features are regularly tested (Informa Group, 2017). This requires resource availability and allocation, which in turn highlights the need for training personal and expanding IT teams.

Considering the rate of digitalization, there is also a necessity for IMO and national organizations to set minimum security standards in terms of software and tools required by operators and owners. Manufacturers like Wartsila and MAN are also at risk as the latest engines on board the mega container carriers are remotely connected to their mainframe for

data collection. GPS, ECDIS and other bridge management systems are also vulnerable to cyber attacks and jamming. The shipping industry must take cue from the airline industry to ensure backup system apart from the minimum navigation and operation knowledge of seafarers. Cargo management system and power control systems on shore are also at risk and terminal operators should upgrade systems not only to improve efficiency but also safety.

Along with an overall development of the security system, the industry must encourage inclusion of cyber security policies, controls and procedure in Safety Management Manual (SMM) and Ship Security Plan(SSP). A Designated IT person for fleet or vessel pool would be an added level of safety against IT malware. Regulatory steps to standardize equipment (both ship and port machinery), ship construction protocols and backups systems to mitigate hacking or disruptive threat would be essential to ensure safety and security. Policies and procedures to conduct risk analysis and upgradation of IT systems at regular intervals, safe disposal of hard drive (on board and on shore), authorization requirement for remote access and an incremental protective framework based on operational significance, should be developed. An increased use of big-data, and Internet of things will increase the data available to hackers, a risk versus reward approach would point towards a top-down cyber safety approach, within maritime firms with strategic initiatives to understand and develop required IT skill-set.

Conclusion

A safety and security matrix in the maritime industry which is constantly moving towards digitalization comprises more than just physical threats to safety and security. Hackers are the new pirates. Cyber security risk management is becoming a crucial component of the maritime sector and the global supply chain. Still at a primitive stage, IT systems have a lot of room for improvement. Being systemic in nature, stakeholders need to take steps to ensure their systems are secure, vigilant and resilient as discovering the threat and recovering from it quickly is paramount to reduce losses. IMO and the governments need to devise regulations and protocols as soon as possible, as the pace of digitalization in the industry and the ever-changing threat landscape has the potential to create massive disruption as shipping is a part of critical infrastructure. Companies and authorities should upgrade system to secure infrastructure, protect data, customers and employees. End-user are most prone to such attacks and steps need to be taken to improve IT and OT system protocols. Developing in-house IT system might not be economically possible for all parties and third party IT risk assessment companies and tools like wireshark could be useful. Following NIST framework

as mentioned in the IMO guidelines or a custom built system should be developed to maximize data security. As the maritime sector casts itself into the industry 4.0 setting, shipping organizations are underprepared to handle attacks from hackers and it is high time to moved away from legacy systems to dynamic cyber specific systems.

Bibliography

BIMCO. (2016, Feb) The Guidelines on Cyber Security Onboard Ships. Vol. 1.1. Bagsvaerd: BIMCO, 2016. Www.ics-shipping.org. BIMCO, Feb. 2016. Web. 27 June 2017.<http://www.ics-shipping.org/docs/default-source/resources/safety-security-andoperations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=14>.

Greenberg, A. (2010, May 01). Beware Who Fixes That Broken Laptop. Retrieved June 30, 2017,from https://www.forbes.com/2010/01/05/data-recovery-privacy-technology-cio-networkbreaches.html

Informa Group, KNect365, Maritime. (2017, April 09). 8 Experts Weigh In on Cybersecurity in Shipping & Maritime [Press release]. Retrieved June 28, 2017, from https://knect365.com/talentandtraining/article/56554e0a-1356-42ac-88cd-564a389bcd1e/cybersecurity-shipping-maritime

Reuters. (2017, June 29). Global Shipping Giant Maersk Is Reeling From the Ransomware Fallout. Fortune.com. Retrieved June 29, 2017, from http://fortune.com/2017/06/29/petyagoldeneye-maersk-ransomware-effects/