Challenges in Maritime Cyber-Resilience

Lars Jensen

> *"Maritime cyber-attacks are no longer the stuff of science fiction. They are happening now, and the threats are growing."*
>
> Fred Roberts
> Professor of Mathematics and Director of CCICADA

The maritime industry has been shown to be under increasing levels of cyber-attack, with future attacks having the potential to severely disrupt critical infrastructure. The industry lacks a standardized approach to cybersecurity, a national approach will be counterproductive, and a global mandatory standard, while needed, will take a long time to implement. In the shorter term, this article recommends that the industry coalesce around a set of voluntary guidelines in order to reduce the risk profile and increase resilience. To provide context for these recommendations, this article examines the specific characteristics of the maritime industry in relation to cybersecurity. Examples of existing vulnerabilities and reported cyber-attacks demonstrate that the threat is current and real.

Introduction

The maritime industry is the foundation for the efficient functioning of all aspects of modern society, from the supply of raw materials such as oil, iron, and grain to virtually every product on the shelves of the local stores and supermarkets – and it is wide open to disruptive cyber-attacks.

In the wake of the 9/11 attacks on the Twin Towers in New York, the maritime industry saw an escalation in physical security procedures aimed at reducing the risk of paralyzing vital infrastructure; in particular, there was a focus on port security (IMO, 2015). However, a similarly security-conscious approach is found to be lacking in relation to cyber-risks. As this article will demonstrate, a closer investigation of the landscape of both cyber-threats and actual incidents in the maritime sector, shows that risks are indeed real and that the impact of an attack can range far beyond the company being attacked.

A hypothetical scenario to illustrate the point would be a cyber-attack that involved the deletion of operational data in a few large container shipping terminals. Such an attack would choke the entire supply chain for tens of thousands of companies. The 100 largest container ports globally each handle in excess of one million 20-foot containers annually (Lloyds List, 2014). Shutting down just a handful within the same geographical region means that the overflow cannot be handled elsewhere. The economic impact on society would be large. In 2002, the key ports on the western coast of the United States were shut down for ten days due to a labour dispute. At that point in time, it was estimated that this had a cost to the United States economy of $1-2 billion USD per day due to disrupted supply chains (Cohen 2002). Since then, the volume of containerized trade has grown significantly, and hence a cyber-attack shutting down key ports can thus be expected to have an even larger impact on the national economy of the affected country – or countries.

Four key sources provide an overall perspective on this issue:

1. A study by the European Union Agency for Network and Information Security (ENISA, 2011) provides a baseline analysis of maritime cybersecurity and the related policy context.

2. A policy paper by The Brookings Institution focused on critical infrastructure cyber-vulnerabilities in port facilities in the United States (Kramek, 2013).

Challenges in Maritime Cyber-Resilience

Lars Jensen

3. A United States Senate (2014) inquiry into cyber-intrusions emphasized the threat of cyber-attacks on the networks of the United States Transportation Command, which is responsible for Department of Defense transportation, including maritime transportation.

4. A whitepaper issued by the author's maritime cybersecurity company, CyberKeel (2014a), examined the vulnerability of the maritime industry to various cyber-risks and highlighted its lack of adequate defenses.

Generally, these studies all arrived at the same conclusion, albeit while covering different sub-domains. The various authors found the levels of cybersecurity to be very low and that significant and dedicated efforts were needed to improve the situation. They furthermore showed that the amount of publically reported incidents do not represent the actual amount of malicious activity ongoing in the industry – a fact particularly underscored by the US Senate inquiry, which revealed a large gap in reporting despite such reporting being mandatory in stated contractual terms with suppliers.

This article aims to propose immediate and longer-term steps the industry can take to improve its cyber-resilience. It will initially examine the specific characteristics of the maritime industry that are of importance in relation to cybersecurity. It will assess whether certain types of threats are to be considered theoretical or whether they have in fact already been seen, and then it will identify the likely entities behind the threats. Finally, the emerging view of the industry will be used to recommend how cybersecurity and cyber-resilience can be improved in the maritime industry in both the short and long term.

Industry Characteristics

In terms of cyber security, the maritime industry has a range of characteristics that makes it difficult to implement solid cyber-defenses. To illustrate the point, it is worthwhile examining how a generic container shipping line operates. A large container shipping line will have offices spread across 150 different countries. They own, and hence control, half of these offices, but for the other half, they rely on the services of local agents. The shipping line thus has to share access to key backend systems with a large number of local agents who have their own IT infrastructure, and where the shipping line usually has extremely limited insight, and influence, on the cybersecurity standards.

Additionally, the shipping line may be operating a fleet of 300 vessels of which they own 150. The other 150 vessels are chartered from a wide range of vessel-owning companies for short- or medium-term duration. The shipping line will not have the ability to control the IT structure onboard vessels chartered for a shorter period. Even for the vessels the shipping line owns, cybersecurity on vessels tend to be an issue. In many shipping companies, the IT department located at headquarters tends to be in charge of land-based IT systems, whereas the vessel-based IT systems fall under the purview of the marine technical department – who often have very limited IT background knowledge. Adding to the challenges, the shipping line may not be the one fully in control over the crewing of the vessel, hence opening an avenue for social engineering intrusion on board the vessels themselves. A tangible example of such a scenario was shared with CyberKeel by a physical maritime security company. They had experienced a vessel approaching the Gulf of Aden, which at the time had a significant piracy risk. However, prior to entering the Gulf of Aden, it was discovered that a person onboard the vessel had been uploading significant amounts of images to a Facebook account – images that provided a detailed look into the safety measures in place on the vessel. The ability to do this is a consequence of the recent, rapid roll-out of "crew welfare", which is the term most often used to indicate making Internet access available to crew using satellite connections.

Finally, when a container is moved from point A to point B, the information related to this movement may pass through between 10 and 50 different systems, each being controlled by different entities such as ports, customs offices, trucking companies, banks, shared-service centres, and industry information portals. These entities do not share a common IT infrastructure, nor do they have any agreed cybersecurity standards. At CyberKeel, we have asked several of the major players in the industry who provide IT systems or IT services how often their customers ask about the cybersecurity aspects of a link-up. The answers are that this is not the norm, the discussion is basically focused on functionality. Given that the successful movement of illicit cargo, or the theft of cargo, only requires successful penetration of one or two of these many hand-over points, it is easy to see how this system can be utilized by criminal elements.

The industry is hence characterized by companies who may have solid control of central parts of their own IT landscape, but have limited – or no – control over more "remote" parts of the landscape. These remote parts

Challenges in Maritime Cyber-Resilience

Lars Jensen

thus present an easy access approach to attacks directed at the central elements of the IT landscape.

Is the Threat Genuine?

As CyberKeel approached management layers in many maritime companies in the first half of 2014 on the topic of cybersecurity, many voiced the opinion that the threats appeared to be more theoretical than real. After all, the fact that something can be done is not the same as somebody actually going through the trouble of doing it.

As a consequence, CyberKeel issued a whitepaper (Cyberkeel, 2014a) and subsequently started a monthly newsletter called Marine Cyberwatch (tinyurl.com/ozxukd5) including an identifications of actual attacks across the maritime sector. Some attacks had already been known, particularly within the cybersecurity sector, but still appeared to be relatively unknown by maritime managers. Additionally, a number of attacks were described that, until then, had been relatively unknown.

One such incident was a cyber-attack against the Iranian shipping line IRISL, which took place in August 2011 (cited in CyberKeel, 2014a). The attacks damaged all the data related to rates, loading, cargo number, date and place, meaning that "no-one knew where containers were, whether they had been loaded or not, which boxes were onboard the ships or onshore" (CyberKeel, 2014a). Although the correct data was eventually restored, the company's operations were significantly impacted: the company's internal communication network was disrupted, cargo was sent to the wrong destinations, and the company suffered severe financial losses in addition to losses of actual cargo. A similar attack on a major international container line would have a crippling effect on the supply chains of thousands of international companies.

Another incident was first reported by CyberKeel based on a forensic analysis performed by Clearsky, a cyber-intelligence company (CyberKeel, 2014b). A number of maritime companies – principally shipping lines and bunker fuel suppliers – were infiltrated with a remote access tool. This remote access was used to monitor email communication and subsequently spoof the communication resulting in a change of bank account information pertaining to large payments. This type of incident is also known in other industries, but was first reported in the maritime sector in late 2014.

In addition to identifying actual attacks, CyberKeel made a simple investigation of the 50 largest container shipping lines who collectively control 94% of the global container vessel fleet (CyberKeel, 2014a). The investigation was simple in the sense that only two aspects were tested. One test was for potential SQL injection vulnerabilities; the other was a simple Shodan search for accessible hardware running a systems version with known exploits available. The results were that 37 out of the 50 carriers exhibited vulnerabilities.

Who Performs the Attacks

The motivations of the attackers in the maritime sector appear no different than in a number of other industry sectors. Some attacks are motivated by financial gain, though from various angles. Some, as illustrated earlier, aim at stealing money directly from the targeted companies. Others are aimed at, for example, contraband cargo. A widely publicized cyber-intrusion enabled a drug smuggling operation through the port of Antwerp (Bateman, 2013), where the terminal operation system had been penetrated, allowing smugglers to extract containers from the terminal using manipulated data.

Another type of attack is aimed at potentially infiltrating, controlling, or damaging critical infrastructure. The global shipping industry is undeniably an element of critical infrastructure to all nations, given that a disruption could have a significant impact on national economies – not to mention the ramifications of disrupting shipping services related to military operations. The report from the US Senate inquiry described earlier documented 50 intrusions into suppliers for the United States Transportation Command in a span of one year (United States Senate, 2014). In terms of shipping, the report also noted that commercial vessels handled 95% of all military dry cargoes in 2012.

Conclusion

In the context of cyber-crime related to the theft of money, the maritime industry is fundamentally no different from other industries. Criminals will use weaknesses to obtain a financial payoff, and the main victim of such attacks is the company losing the money. However, the nature of shipping also results in a situation where cyber-attacks, even those “only” aimed at a single company, can have significant ripple effects into entire national economies. As an example, a ransomware attack against a few key container terminals can

Challenges in Maritime Cyber-Resilience

Lars Jensen

cripple an entire national or regional supply chain, resulting in losses significantly out of proportion with the loss suffered by the company under attack. Or, even worse, remote tampering with on-board vessel systems – something that has been demonstrated as feasible – can result in catastrophic effects with not only economic but also significant environmental impacts.

In order to improve the situation, it is important that the maritime industry rapidly develops a set of best practice guidelines to improve the situation, while at the same time working on a longer-term plan to introduce global cybersecurity standards. National governments in many places need to increase their awareness of the critical vulnerabilities of their port infrastructure systems and provide the necessary support to allow for an improvement in cybersecurity.

The current challenge is that no practical guidelines are in place for the maritime sector, and given the global nature of the maritime industry, nationally mandated guidelines are highly likely to become conflicting and hence counterproductive as vessels move across different national jurisdictions.

Reaching a consensus on standards would require the involvement of the International Maritime Organization (IMO; www.imo.org); however, this process will likely take many years to come to fruition. In the interim, a practical approach would be the rapid establishment of voluntary global guidelines that heighten security industry-wide, and such an approach could be beneficially anchored with industry-wide best practice forums such as the Baltic and International Maritime Council (BIMCO; bimco.org). Such anchoring would allow maritime companies to pool their resources related to the necessary analysis and research, as well as attract the attention of IT companies towards dedicated maritime cybersecurity solutions. This approach would further support the adoption of voluntary guidelines.

Maritime organizations should then be encouraged to adopt these voluntary guidelines using three principal tools: i) informational campaigns directed at the maritime companies in terms of the cyber-risks they face; ii) pressure from customers who are made increasingly aware of the risk to their cargo in cases where maritime companies lack cyber-defenses; and finally iii) "cyber-premiums" on insurance policies that reflect the degree to which maritime companies adhere to the voluntary guidelines. Also, national governments could play a key role in helping identify and map out the cyber-risks faced by maritime companies within their own domain, and make such analyses readily available to maritime companies. Additionally, governments could emphasize collaboration with the IMO to fast-track the development and adoption of more binding cyber-standards in the future. Together, these steps would bring us greater cyber-resilience for the efficient functioning of the maritime industry, upon which we all depend.

About the Author

Lars Jensen is CEO and Co-Founder of CyberKeel, an international maritime cybersecurity company based in Copenhagen, Denmark. He is a recognized global expert in container shipping markets, having worked initially working for Maersk Line, where he was responsible for global intelligence and analysis as well as e-Commerce. In 2011, he founded SeaIntel Maritime Analysis, and he is currently the CEO of SeaIntel Consulting in addition to being CEO of CyberKeel. He holds a PhD in Theoretical Physics from the University of Copenhagen, and he has received strategy and leadership training from the London Business School and the Copenhagen Business School.

References

Bateman, T. 2013. Police Warning after Drug Traffickers' Cyber-Attack. *BBC News,* October 16, 2013. Accessed April 1, 2015: http://www.bbc.com/news/world-europe-24539417

Cohen, S. S. 2002. *Economic Impact of a West Coast Dock Shutdown.* Berkeley, CA: Berkeley Roundtable on the International Economy. http://www.brie.berkeley.edu/publications/ships%202002%20final.pdf

CyberKeel. 2014a. *Maritime Cyber-Risks: Virtual Pirates at Large on the Cyber Seas.* Copenhagen: CyberKeel. http://www.cyberkeel.com/images/pdf-files/Whitepaper.pdf

CyberKeel. 2014b. Shipping Companies Successfully Penetrated for Money Transfers. *Marine Cyberwatch,* October: 1. http://www.cyberkeel.com/images/pdf-files/Oct2014.pdf

ENISA. 2011. *Cyber Security Aspects in the Maritime Sector.* Heraklion, Greece: European Union Agency for Network and Information Security. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/dependencies-of-maritime-transport-to-icts/cyber-security-aspects-in-the-maritime-sector-1

Challenges in Maritime Cyber-Resilience

Lars Jensen

IMO. 2015. Frequently Asked Questions on Maritime Security. *International Maritime Organization*. Accessed April 1, 2015: http://www.imo.org/OurWork/Security/Guide_to_Maritime_Security/Pages/FAQ.aspx

Kramek, J. 2013. *The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities*. Washington, DC: Brookings Institution. http://www.brookings.edu/research/papers/2013/07/03-cyber-ports-security-kramek

Lloyds List. 2014. *One Hundred Ports*. London: Informa Publishing. http://europe.nxtbook.com/nxteu/informa/ci_top100ports2014/#/6

United States Senate. 2014. *Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors*. Washington, DC: United States Senate Committee on Armed Services. http://www.armed-services.senate.gov/imo/media/doc/SASC_Cyberreport_091714.pdf

Citation: Jensen, L. 2015. Challenges in Maritime Cyber-Resilience. *Technology Innovation Management Review*, 5(4): 35–39. http://timreview.ca/article/889

Keywords: maritime, cyber-resilience, cyber-risk, cybersecurity, CyberKeel, container, terminal, vessel