Cyber Threat on the High Seas. A Growing Threat to Infrastructure.

James Cummins
Old Dominion University

Cyber Threat on the High Seas. A Growing Threat to Infrastructure.

James Cummins
Old Dominion University

Abstract

In a growing digital and cloud-connected world, all aspects of our lives are becoming interconnected. All these interconnections breed a possibility for ever-increasing cybersecurity threats. The oceans are not impervious to these attacks. In this research paper, we address the following questions.

What threats do commercial ships face today?

What actions are necessary to mitigate these threats?

A Growing Threat to Infrastructure.

The digital age is clashing with an ancient and stubborn trade. The maritime industry has been around for centuries and is crucial to global supply chains and leisure activities. As in other industries, technological and telecommunication updates and other advancements in the maritime industry increase exposure to cybersecurity threats. As a result, once an afterthought, cybersecurity is now an integral part of this industry. The problem, however, is that implementing security measures has high costs, and are those costs worth it to the organizations operating without them for centuries? Are the threats to their infrastructure that tangible? How much security is required, and does it matter?

Research Methods

This brief review of maritime cybersecurity used the following approach.

1. Reviewing other articles and journals published on the maritime industry, questions they address, and conclusions. More specifically, this involved many short informative articles on maritime cybersecurity's advances and current state. The primary source was the 2015 *cyber-resilience in supply chains* by Carleton University.

2. We review requirements or recommendations from the International Maritime Organization and other industry organizations.

3. Conduct an in-depth interview with someone operating in the heart of this field. Talk to a subject matter expert on the feasibility and effectiveness of various approaches to cybersecurity.

Results

Typically, when people refer to cybersecurity in a business sense, it relates to Information Technology (IT). However, the maritime industry has a complex balance of three areas to protect and manage. Their cyber security program must address IT, Operational Technology (OT), and Entertainment Technology (ET).

With growing digital and increasingly cloud-based technologies, the maritime industry is connected and sometimes even controlled via remote sources. Any connection, especially

those that allow navigation features, poses an entry angle for a cyber-attack. What is the importance of distinguishing between the three different types?

They all have distinct differences in their impact on the company. Entertainment technologies are an aspect of the pleasure side of the maritime industry. Smart devices with internet connectivity are replacing their less capable counterparts in many aspects. Even washers and dryers are connected to monitor detergent levels and the number of cycles to track maintenance. Soda machines monitor syrup levels. While seemingly benign to target these systems, they pose a financial and operational risk to the company. Every ET that can be affected is a potential effect on company brand integrity and revenue.

IT breaches, as shown above, typically will affect revenue or reputation as personal and professional information can be breached or leaked.

The cost can be much more drastic for the operational side. Ship's control systems and navigation are increasingly linked to "off hull" (external to the ship) sources. The potential vulnerability of these systems is the control of the ship, which can result in collisions that cause damage to the vessel and equipment, the environment, and worst, loss of life.

Industry Today (Demboski) poses a pungent issue on the ever-growing integration between IT and OT systems. She poses that to provide the necessary level of cyber security, we

must focus more on "security by design." Security by design means implementing cyber security as part of initial design and construction, not simply an afterthought.

Ships are old, and their average age is only increasing. The average container ship is 14.1 years old, up from 11.6 in 2017 (Mcfarlane). In the last decade, ships' available systems and integrations have seen drastic changes. Every aspect of the ship links to off-hull locations. Each of those connections, as discussed, poses a potential threat. With ships being responsible for about 90% of the world's trade (Demboski) and the average ship age being older than the technology, we can see that the maritime industry is currently adding these systems and their security as an afterthought. Unfortunately, these systems being an afterthought, comes at a high price.

The maritime industry is not in the software business. Most new systems and their security are contracted out to software development companies specializing in those areas. To integrate these new systems, there is a growing need to develop APIs (Application Programming Interfaces) specific to each ship. These integrations take time and money away from the company in both actual cost and the opportunity cost incurred while the ship stays in port, losing potential revenue. The pressure is then to implement these systems as quickly and economically as possible to minimize losses after commissioning improvements. After ensuring proper integration of the new technology, we worry about protecting it.

Obviously, in a perfect world, the most desired approach is to prevent the ability to attack by securing all connections. However, each level of added security can cost significant amounts of money. One example is end-point detection and response. That process can be run remotely from an office. To increase the level of security, create hardened networks with micro-segmentation that involves going to the ships to install hardware. With ships all over the world, that cost is not small. Depending on the level of implementation, the ship can be stranded in port for a while. A ship stuck in port is not making any money resulting in even more revenue loss. Earlier, we mentioned how so many systems are moving towards off-hull capability and trying to cover all those systems is just not financially feasible. "The vast number of things that have to be covered, it's like looking at Mount Everest." (Mills)

We have seen that protecting every system to be impenetrable is not feasible or even possible in an ever-evolving field. How do we protect ourselves in the maritime industry? While this is not unique to the maritime industry, "cyber resiliency" plays a significant role in the cyber defense plan. *Cyber resilience* is "the capability of a supply chain to maintain its operational performance when faced with a cyber risk" (Davis). In an interview with a cyber security executive at Royal Caribbean, he laid out three main facets of their cyber resiliency:

- "Contain the blast"
- Back-ups
- Eliminate a "flat network"

This approach is not all-encompassing but rather a good look into the practical applications utilized today.

"Contain the blast" involves monitoring software, scans, and alerting software. These tools' goals are to get the response as quickly as possible. The faster the breach is found, the faster the response. Faster detection allows containment of affected portions, thus minimizing the affected systems of the breach. These two aspects have a significant impact on recovery time.

Backups are also not a new concept but are imperative in defense. Frequent and proper backups allow for faster recovery and minimize loss of data. "Making backups of collected data is critically important in data management. Backups protect against human errors, hardware failure, virus attacks, power failures, and natural disasters. Backups can help save time and money if these failures occur."

Eliminate a "flat network." "Traditional flat networks, including network-based segmentation or micro-segmentation techniques, cannot detect and prevent many of today's more sophisticated attacks. Many of these networks still provide single-time authenticated users and devices with unfettered access to virtually any application. Such an implicit trust policy provides free rein across permitted segments and reduces the visibility across the network, especially into encrypted paths." (Fortinet)

While OT is essential to ship operation Entertainment Technology (ET) is essential to some aspects of the maritime industry. Cruise lines and other pleasure craft operate with ET as an integral part of their business. Satellites and other off-hull communications is how this ET is functioning in this modern age. On pleasure craft Television and internet services have become a requirement. The expectation of these inherently connected services paired with technology updating and being serviced off-hull proves a very wide angle of attack as well. These systems may not be directly integrated with the ships operations and IT systems but crippling ET has a major impact on guest experience which directly impacts revenue.

Tacit Knowledge

With the increase in functionality of off hull facilities we are seeing an apparent lack of need for the tacit knowledge that was integral to the maritime industry.

Why is this tacit knowledge so crucial to cyber security and safety? We have shown that IT and OT system integrations that have been implemented pose potential security threats. Ships are also becoming much more reliant on these integrations and implementations. With these new advancements, however, we often fail to capture the "tacit knowledge" gained by veteran employees, thus reducing the opportunity for new sailors to learn from this experience. Currently, we have manual backups on almost every OT system in case of any cyber attack or

malfunction. However, that ability may soon pose a more significant threat to the ship and its operations.

Human interaction on normal day operations is dwindling. This year we had a ship complete a 500-mile journey 99% without human intervention (Doll). The removal of the ability to gain the experiences and the lack of sense of need to pass down this tacit knowledge will worsen the effects of any cyber attack threatening OT systems. Professor Torger spoke out about this issue. He states, "It is the combination of formal and tacit knowledge that produces excellent results in the shipping industry." Further, he says that we "cannot run ships safely and efficiently from skyscrapers in Manhattan" (Emeritus).

Discussion

The most challenging question is: Are we doing enough for cyber security, or do we need to improve?

This is answered on a per-company basis. However, the IMO (international maritime organization) has been increasing the requirements for cyber security in the maritime community; however, currently, it needs to be more specific and are considered more recommendations than requirements (Maritime cyber risk). The joint product by BIMCO and others is *The Guidelines on Cyber Security Onboard Ships. T*his 50-page document further

expands on IMO's guidelines and spells out all aspects of the maritime cybersecurity model. Their recommended process is found in the following model:

Figure 2(BIMCO)

Currently, the main discussion in the maritime industry is the impact to operations. The operational impact is the single most unique aspect of maritime cyber security from the rest of the world. As discussed earlier, modern technology poses a possibility to remotely access and control ships with ill intent. Thankfully, most ships have manual overrides and can operate without reliance on internet connections. This simple mitigation, paired with the fact that there has yet to be a reported successful cyber takeover of a vessel, has led to a certain level of resistance to further funding maritime cybersecurity programs.

The industry recognizes that the need for some level of cybersecurity is essential due to the potential impact on operations. How much security is needed is variable, as the threat likelihood is considered low. Once ships successfully start being controlled or ransomed by cyber-attacks, that may cause a reconsideration of the allocation of resources.

Ultimately the maritime industry should address two areas to improve its cyber defense posture.

- OT integration
- Knowledge management

OT integration needs to be part of the security by design. Realizing that IT, ET and OT overlap is necessary, ships must be designed with cyber integration in mind and a significant focus on protecting inevitable integration points.

Retaining tacit knowledge should be a priority for maritime companies. With how much of a potential threat cyber attacks pose on ships, competent and experienced operators are needed to mitigate the effects of these attacks.

References

Balman, S. (2021, January 28). *The importance of retrieving tacit knowledge in the marine industry*. GMBA. Retrieved November 10, 2022, from https://www.gmba.blue/the-importance-of-retrieving-tacit-knowledge-in-the-marine-industry/

BIMCO. (2018). *The Guidelines on Cyber Security onboard ships*.

Davis, A. (2015). Building Cyber-Resilience into supply chains. *Technology Innovation Management Review*, *5*(4), 19–27. https://doi.org/10.22215/timreview/887

Demboski, M. (2022, February 9). *Transportation hazards driven by IT/OT convergence*. Industry Today. Retrieved November 10, 2022, from https://industrytoday.com/transportation-hazards-driven-by-it-ot-convergence/

Doll, S. (2022, May 13). *Autonomous cargo ship completes 500 mile voyage, avoiding hundreds of collisions*. Electrek. Retrieved November 10, 2022, from https://electrek.co/2022/05/13/autonomous-cargo-ship-completes-500-mile-voyage-avoiding-hundreds-of-collisions/#:~:text=The%20%E2%80%9Cworld's%20first%E2%80%9D%20autonomous%20commercial,for%2099%25%20of%20the%20trip.

Fortinet. (2022, February 4). *Flat Networks Inevitably Fall Flat When Attacked — Using Secure Segmentation To Protect Your Business*. Fortinet.com. Retrieved November

5, 2022, from https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-flat-networks.pdf

Maritime Cyber Risk. International Maritime Organization. (n.d.). Retrieved November 5, 2022, from https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

Maritime Cyber Security. DNV. (n.d.). Retrieved November 5, 2022, from https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/index.html

Mcfarlane, S. (2022, July 12). *Ships get older and slower as emissions rules bite*. Reuters. Retrieved November 10, 2022, from https://www.reuters.com/business/sustainable-business/ships-get-older-slower-emissions-rules-bite-2022-07-11/#:~:text=The%20average%20age%20of%20bulk,2017%2C%20according%20to%20the%20data.

Mesich, M. (2021, June 11). *Understanding the importance of operational technology security in the Maritime Industry*. OT & ICS Cybersecurity Solutions. Retrieved November 10, 2022, from https://www.industrialdefender.com/blog/understanding-importance-of-operational-technology-security-maritime

Mills, S., & Cummins, J. (2022, November 4). Cyber security and how it applies to the maritime industry. personal.

Reve, T. (2016, November 17). *A knowledge based shipping industry*. BI Business Review. Retrieved November 10, 2022, from https://www.bi.edu/research/business-review/articles/2014/09/a-knowledge-based-shipping-industry/

US Geological Survey. (n.d.). *Backup & Secure*. Backup & Secure | U.S. Geological Survey. Retrieved November 5, 2022, from https://www.usgs.gov/data-management/backup-secure