How have major cybersecurity challenges in the global maritime shipping industry evolved, especially in the aftermath of the Ragnar Locker cyber-attack in September 2020?

Louis Septier

IDS 300: Interdisciplinary Theory & Concepts

Dr. Kat LaFever

March 23, 2024

Abstract

The worldwide shipping industry can be classified as a high-profile target of cyber-attack. In an ever-growing world becoming more and more digitalized, it is clear the risk of new attacks grows larger every day. The challenges this industry faces need to be understood to prevent further damage from being done. With a detailed analysis of Cybersecurity, the worldwide economy, and the shipping industry, this paper explores the potential damages and risks cyber-attacks can have on worldwide trading. A strong emphasis on the Ragnar Locker cyberattack of September 2020, is made in this paper, as it allows for a clear and detailed understanding of the problem. Amidst the COVID-19 pandemic and the following lockdown as a result, the industry saw its revenue drop, as demand decreased. The already chaotic situation saw the rise of ransomware with the goal of extorting large sums from shipping companies. Detailed sources and insight are used to provide the most comprehensible explanation of the issue. Some conflict between these sources is found, but the overall subject does not suffer from it, as the mixture of all this information can be used to our advantage in getting a better understanding of the issue.

Keywords: Ransomware, Maritime Industry, International Relationship

Introduction

In an era marked by rapid digitalization and technological advancement, an industry as old as the age of sailing stands at the center of innovation and vulnerability. While the integration of digital technologies has revolutionized the efficiency and connectivity of the maritime field, it has also exposed it to unforeseen cybersecurity threats. The emergence of technology like Global Positioning System (GPS), Electronic Chart Display and Information System (ECDIS), or Radio Frequency Identification (RFID) helped the industry not only sustain itself through the ages but also become the largest and most common means of transporting goods around the globe. However, this kind of technology has allowed a certain amount of malicious actors to thrive and seek to exploit potential weaknesses, for financial gain, or simple disruption. History showed us how this kind of behavior could cripple this industry with a certain severity. A good example of this is the Ragnar Locker cyber-attack in September 2020, proving to the world that technical innovation and cyber threats are bound to coexist.

Seeing such an issue arise, the worldwide shipping community needs to address the potential problem linked to cybersecurity and the possible solution that can help mitigate the damages caused by problems of this kind. We could study this issue with the question; How have major cybersecurity challenges evolved, in the global shipping industry? This paper dives into the evolution of the difficulties and challenges linked to major cybersecurity the global maritime shipping industry is facing, with a strong focus on the aftermath of the Ragnar Locker attack. From defining the terms related to our topics of interest to the analysis of the cause and result of

these cyber threats, we are aiming to understand how cybersecurity and the global trading economy are linked. Finally, we will discuss how these changes have impacted the economy connected to the shipping industry and the possible solutions to prevent further damage.

To clearly understand the extent of the issue, some key terms and concepts need to be defined. This is a good way of clearly understanding how the different disciplines linked to the problem are associated. *Ransomware*, *maritime industry*, and *International cooperation* are among the key terms recurring within the topic. *Ransomware*, a type of cyber-attack, is defined as a seemingly harmless file attached to an email, which initiates a denial of access to a system (Mrakovic et al., 2019). These forms of malware can be fixed by paying a ransom, which will, allegedly, return control of the system. *Maritime industry*, while being a field in itself, can be used as a term for this analysis. The term *maritime* refers to ships, yachts, or other kind of activities taking place in a large body of water (Mrakovic et al., 2019). Any kind of business conducted surrounding these said activities is classified as the maritime industry. This includes, but is not limited to, trading, construction, travel, or resource gathering. In his paper, we refer to the *Maritime Industry* as the *Shipping industry*, as the two terms carry a very similar definition. According to the San Francisco State University, *International Relationships are* the "relations across boundaries of nation-states", in simpler terms, the relations between one country to another. As it is stated later in the article, as the world grows more and more connected through trade and commerce, understanding how these relations between sovereign states work becomes a necessity.

Shipping Industry

The worldwide shipping industry was, according to the OECD and European Union Intellectual Property, an industry worth over 19 trillion US dollars in 2019 (2021). The transporting of goods across the oceans plays an important role in worldwide supply production and consumption. The introduction of containers was a revolutionary change that brought many logistical possibilities and boosted the revenue of trading by a large margin. The use of this practice is essential to the well-functioning of our society, as it allows for goods from all around the world to be sent to many destinations, all in a timely manner. The importance of this industry in the global market makes it a primary target of all kinds of attacks and fraud, as it sits on a significant amount of wealth. The disruption of logistics on a large scale can bring a country's economy down and put the living conditions of its citizens in jeopardy. Furthermore, a worldwide pandemic, such as the COVID-19 one, can lead to a large amount of loss in the sector. As Kuhn et al. (2021) articulate it in their article, the lockdown following the rise of the virus led to a $5 trillion loss for the industry. The prolonged confinement of individuals within their homes resulted in a diminished demand for international goods, subsequently precipitating a decline in the necessity for cargo freighter movement. However, it also changed the relationship between the field and IT systems, increasing its dependency on connected technology. “The COVID-19 crisis has transformed how we do work, trade, and crime; and the way these will continue to be done in the future” (Kuhn et al. 2021, 195).

Cybersecurity

As technology evolved throughout the ages, the way we interacted with the world was followed by new sets of morals and habits. This led to a great amount of progress, made in a

wide range of fields, but also led to new ways of abusing society with a wide range of new crimes. Cybersecurity focuses on the security linked to digital technology and works to prevent IT crimes from happening. “Cybersecurity is a user-centric notion that necessitates the implementation of secure behavior to protect against online vulnerabilities and assaults” (Asan, 2023, p.26). To determine how ransomware, or other kind of cyberattack, is perpetrated, a strong understanding of cybersecurity and its many strategies is required. Understanding how, why, where, and when a crime is committed is a good way to mitigate and potentially totally prevent damages. If a crime was to be committed, this discipline is also specialized in combating its effect. A strong comprehension and allocation of means in cybersecurity is required to prevent potential disasters but it is not always enough. As technology evolves, so do the ways of committing crimes, thus explaining why staying top. As stated in their analysis, Baig et al. (2023) observed that techniques surrounding ransomware attacks keep on improving, consequently, prevention has to keep up and always know how to react.

Global Economy

An economy that is well-balanced and operating effectively is very important for the good functioning of our society. Major events such as cyber-attacks or a global pandemic have the ability to diminish the returns on countries’ investments. In our case, the “COVID-19 pandemic led to a massive disruption to economic activity” (Kerr, 2020, p. 225). Furthermore, adding to the original problem of the economic disruption of the pandemic, the Ragnar Locker attack of September 2020, added oil to an already raging fire, and the economy slowed down by up to 30%, according to the OECD (2021). By working on improving cybersecurity in the

shipping sector, an emphasis needs to be placed on the economic factor. Protecting the assets from further damages would lead to a more stable economy overall, as it will prevent potential loss in the future.

Common Ground

The three disciplines of interest in this paper share a common ground. The maritime domain has seen many improvements during the previous decades, especially in technologies touching the field of navigation. Such technologies are a great enhancement and addition to the already existing methods. They allow ships for a better understanding of their surroundings and area of navigation, leading to faster and safer travel. In the past, ships were afraid that the calculations made about how the weather would be on the way, but with these improvements, it is possible to know in real time where and when a storm is a threat. Today, even if the threat of a storm is greatly reduced, this kind of improvement brings another type of challenge to the industry. When the ships are rigged with top-of-the-line electronic equipment, the threat is less physical and more online. The digital age brought a ton of new threats in the realm of cybersecurity. A ship is not always safe from a potential hack, leading to the malfunctioning of its navigation system, thus removing all these new safety features. As Asan states in his text, "Accidents that may result in injury or death may occur due to the steering of ships for malicious purposes, or the deactivation or steering of machinery" (2023, p. 25). This is why the cybersecurity and shipping industries are both working in unison to ensure maximum security and mitigate potential losses.

Any cyber threat to the maritime industry puts it at great risk of economic loss. According to Kuhn et.al (2021), a collision involving two cargo freighters following a cyber-attack, which crippled their navigation system, could lead to a loss of up to $4 billion. A good example of this is the Ragnar Locker attack which happened in September 2020. The ransomware targeted high-profile targets like the CMA CGM, one of the leading companies in the sector. This attack crippled the entirety of the companies it targeted system, rendering their operation ineffective for a prolonged period. Furthermore, Ragnar Locker adopted a double-extortion method, meaning that not only did it disable systems, but it also extracted a large amount of sensitive data that can be sold for an increased profit. The malware had a long dormant period during which it analyzed how it could infect the system for maximum damage. Ransoms going up to $11 million were requested for the control of the system to be returned (Baig et al., 2023). Not only was the ransom for the malware a large hit on the company's economy but the lack of ship movement during this period also greatly decreased the amount of revenue during the period. Additionally, the economic demands companies were contractually obligated to fulfill could not be honored, which led to shortages. While most companies were able to recover from the malware, it clearly put a dent in their reputation and exposed their lack of preparation for this kind of scenario. A case like the Ragnar Locker is proof that first, no field is spared by cybercrime, and such crime can lead to a decrease in growth for the economy. Any damage done by ransomware can be devastating for a company or a country with a low GDP.

The link between the shipping industry, cybersecurity, and the worldwide economy proved how much damage a well-placed and assembled ransomware attack can cause. While the damages are mostly financial, they can also be physical, as stated in Kuhn et al. article, “Cyber

risks to vessels include physical damage or loss of hire" (2021, p. 200). A well-developed cybersecurity system and a good learning program for company employees can help prevent this kind of attack. Nevertheless, staying on top of the technology and ransomware method will always be the best solution to counter potential damages in the future. As the risks linked to the shipping industry shift from mostly physical threats to digitalized threats, the fields keep their technology up to date to mitigate all the potential risks.

Disciplinary Conflict

While all of the sources used in this paper brought thoughtful and detailed insight on the issue, as well as providing numbers and scientific facts, some conflicts between the insights can be found. The biggest conflict between the sources is related to the effects caused by the 2020 COVID-19 pandemic. While some of the sources exploring the subject agree that this event hurt the shipping industry in some ways, these damages done are not all the same in every insight. For example, the OECD is talking about a slowing of the industry, however, Kuhn et al. article explains a rise in cyber-attacks, and Kerr's article talks more about the financial loss linked to the pandemic. These differences in insight may seem like they can hurt the overall accuracy of the research, but the mixture of results can be used effectively to have a better understanding of the overall issue. Having an idea of the damages caused by the pandemic in all of the disciplinary fields we are exploring in this paper is a good way of drawing a clear conclusion about what happened following this crisis.

Constructing a More Comprehensive Understanding or Theory

Understanding an issue like this one can be a difficult task, especially when multiple disciplines are linked together. Applying a different approach to the initial question will allow for a better comprehension of the subject. From a broader perspective, the problem of cybersecurity linked to the shipping industry can be seen as follows; The evolution of technologies led to a boom in cyber-attacks toward shipping companies and the industry in general, disrupting the economy in the process. Understanding how these attacks are being carried out and what are the priority targets, is a good way of preventing them. Always being on top of the technology, industry innovations, and emerging trends in cybercrime is paramount for determining the efficacy of a defense strategy.

Reflecting On, Testing, and Communicating the Understanding or Theory

This research had the goal of understanding how cybersecurity became a major part of the shipping industry. However, even after exploring a large part of the problem, a good number of questions can be raised. For example, what led to the increase in cyber-attacks against this industry, or was a change of trend in criminal activity against the industry the source of cyber-attacks? This kind of question requires a more detailed description of the discipline used in the paper and additional discipline to grasp a better understanding of the potential issues. A better understanding of the past, present, and future cybersecurity trends in each discipline can be achieved by providing a description and history of each of them. Disciplines like maritime navigation, international laws, or criminology would make for a great addition to this kind of research. Future research could use this as a base for a greater dive down on the subject, combining the disciplines from this paper with new ones that can be related to the topic.

Conclusion

The rise of cyberattacks against the shipping industry has been a growing problem in the last two decades. The shipping industry, cybersecurity, and the global economy are all linked to this issue and are all suffering from it. While damages are guaranteed to happen, a good understanding of the trends and actors of cybercrime can help mitigate potential damages, as well as completely prevent them. The Ragnar Locker attack in September 2020 demonstrated how the chaos of an already installed issue can lead to a bigger problem. A good understanding of cybersecurity, frequent training, and a constant emphasis on security will prevent such damage from happening.

References

AŞAN, C. (2023). THE ROLE OF CYBER SITUATIONAL AWARENESS OF HUMANS IN SOCIAL ENGINEERING CYBER ATTACKS ON THE MARITIME DOMAIN. Mersin University Journal of Maritime Faculty, 5(2), 22-36. https://doi.org/10.47512/meujmaf.1370274

Baig, Z., Mekala, S. H., & Zeadally, S. (2023). Ransomware Attacks of the COVID-19 Pandemic: Novel Strains, Victims, and Threat Actors. IT Professional, 25(5), 37-44. https://doi.org/10.1109/MITP.2023.3297085

European Union. Intellectual Property Office. (2021). Illicit Trade Misuse of Containerized Maritime Shipping in the Global Trade of Counterfeits. https://doi.org/10.1787/e39d8939-en

Kerr, W. A. (2020). The COVID-19 pandemic and agriculture: Short-and long-run implications for international trade relations. Canadian Journal of Agricultural Economics/Revue canadienne d'agroeconomie, 68(2), 225-229. https://doi.org/10.1111/cjag.12230

Kuhn, K., Bicakci, S., & Shaikh, S. A. (2021). COVID-19 digitization in maritime: understanding cyber risks. WMU Journal of Maritime Affairs, 20, 193–214. https://doi.org/10.1007/s13437-021-00235-1

Mraković, I., & Vojinović, R. (2019). Maritime cyber security analysis–How to reduce threats?. Transactions on maritime science, 8(01), 132-139.https://doi.org/10.7225/toms.v08.n01.013