2021-11-10

Is cyber-security a value added service for maritime transport sector?

Karamperidis, Stavros

Is cyber-security a value added service for maritime transport sector?

Stavros Karamperidis
Department of International Shipping, Logistics and Operations, University of Plymouth, United Kingdom
stavros.karamperidis@plymouth.ac.uk

Extended Abstract

The average total cost of each data breach worldwide in 2020 for transportation sector was $3.58million, which is slightly below the global average cost of data breach worldwide ($3.86 million) (Statista, 2021). That is nearly half of the cost related to sectors like healthcare and energy ($7.13 and $6.39 million respectively) (Statista, 2021). That cost of such data breaches in transportation sector is still low, as the level of technology implementation and digitalization is limited. Shipping, which composes a large part of the transportation sector, is a late adopter of technology, as it is not following the new trends and innovations (Papathanasiou et al, 2020). However as shipping is a key component of logistic systems (Song, 2015), therefore other parts of the logistics system as forcing shipping towards smart technologies application. The reason for that force is that logistics companies want to be transformed to Logistics 4.0 that will help them to reduce costs and improve supply chain visualization (Acciaro, 2020; Küpper, 2020). With the digitalization of ships and ports the concept of "Physical Internet" (PI) (global cargo handling system similar to the Internet) will be materialised (Montreuil, 2011). That will help to add value to services offered from maritime transport sector. To achieve that we need to securely implement technology to maritime transport sector. If that is not achieved, we will increase the level of risk, as the increase of technological solutions application into the maritime sector will "expose" the sector to cyber criminals who can operate on a global scale from remote locations. As the maritime sector risk management falls behind technological developments, that will generate the rise of an urgency to improve managerial visibility and cooperative cybersecurity research between maritime and Information Communication Technologies (ICT) professionals (Kalogeraki, 2018). With the aforementioned in mind, that cybersecurity is an emerging issue and the costs and inefficiencies that could be caused by a cyber-breach to maritime transport sector could spread to the overall logistics systems, the IMO requires immediate attention to the MSC-FAL.1/Circ.3 (IMO, 2017). According to the MSC-FAL.1/Circ.3 all ships are encouraged to have a process in place within their safety management systems for tackling cyber security risk issues, after their first annual verification of the company's Document of Compliance after 1 January 2021. As it is demonstrated cyber risk is recognized and shipping companies have to tackle it as it would cost them money and reputation. Therefore, cyber-security should be considered as a value added service, as

according to the experts participated in the research demonstrated that it is very important in their daily operations. Finally, we could say that cyber-security could on the one hand secure maritime transport companies primary business while on the other hand is offering competitive advantage in a market that still lags cyber maturity; which could be considered to add value in the overall operations.

Objective

In business, every process that is added (invested) should add value, so it could "payback" the investment and improve operations. Therefore, recently maritime transport sector started to invest in digitalisation (e.g. smart ports and shipping) to enhance efficiency, productivity, reduce costs, optimise operations, improve safety and boost trade with e-commerce and supply chain integration. The aforementioned actions will help maritime transport to sustainably grow. However, to achieve those benefits from digitalisation, cyber-security should be enhanced to minimise risk of disruptions (e.g. affect personnel, ship, port, environment, company and cargo) caused by a cyber-incident. In addition, ship-owners not accessing cyber risk are not only exposed to disruptions, but may have their ships detained by Port State Control Authorities that would need to enforce this requirement since 1 January 2021. According IMO all ships are encouraged to address the MSC-FAL.1/Circ.3 (IMO, 2017) after their first annual verification of the company's Document of Compliance after 1 January 2021. In maritime sector cyber risks are considered as simple security challenges, but as it demonstrated they are not, as they are business challenges that require leadership's involvement.

The purpose of the research is to identify if the investment requested to reduce cyber risks on vessels and ports is adding value to the maritime transport sector. As it was demonstrated in recent studies cyber-breaches increase and they will increase in future because maritime ecosystem becomes more digitalised, due to the need for global supply chain integration. That need in conjunction with the current pandemic has accelerated cyber-breaches. Therefore, there is a need to provide evidence to C-level (top-level management positions in a company) about the need for investing in cyber security in maritime transport.

Data/Methodology

To tackle the aforementioned research topic, minimise bias and triangulate the findings, mixed-method research was applied. First step was a literature review, which demonstrated deep insights for emerging topics (therefore, it was extremely beneficial for the present research), was conducted and combined with key reports related to maritime transport digitalisation and cyber security. Findings were used to develop a questionnaire, which was distributed to collect the views of maritime transport and cyber security experts. Data collected were analysed with thematic analysis. Experts validated the findings and helped to create a tool that would demonstrate to C-level the importance of cyber security in short and long term period for maritime transport sector.

Results/Findings

A good understanding was gained based on experts' views on the value that they allocate to events as; loss of confidential information, vessel unable to operate, non-compliance with GDPR, affecting the supply chain due to ceased operations, etc., which could be caused by the risk of compromising operations due to a cyber-breach . By understanding that value and exposure to cyber-criminals, C-level could take actions to mitigate that. The level of actions is something that C-level could estimate based on the individual business operations and willingness to take risk. The findings from the survey are demonstrated in Figure 1, where the importance of cyber security to managers' daily job and activities is highlighted.

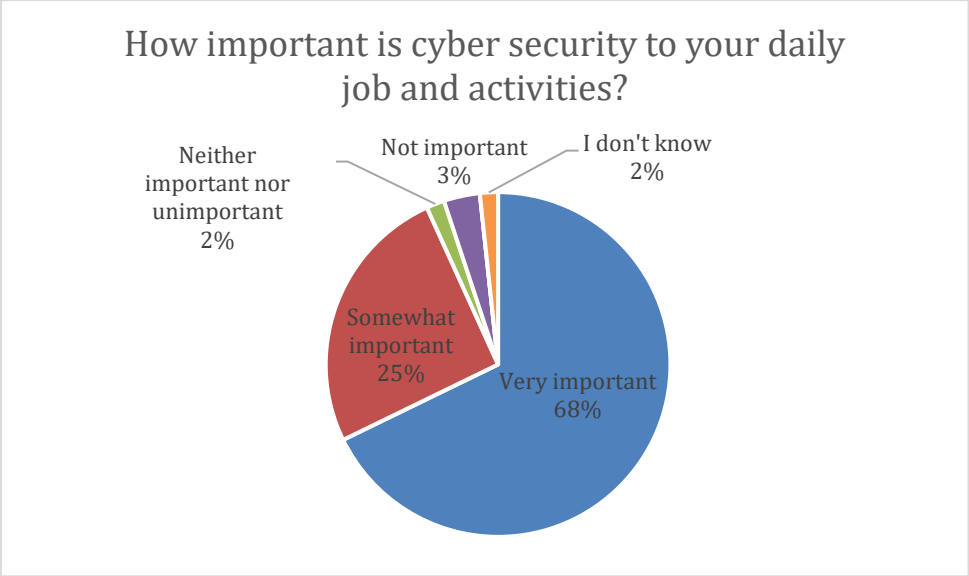

Figure 1 How important is cyber security to your daily job and activities?

As it is demonstrated, cyber security is very important and somewhat important to 93% of maritime and cyber experts participated in our survey. That demonstrates the importance of cyber security under the current digitalized environment that maritime sector is asked to operate. Therefore, C-level managers should take actions, not only to comply with the IMO MSC-FAL.1/Circ.3, but also to avoid instances of loss of confidential information, vessel unable to operate, non-compliance with GDPR, affecting the supply chain due to ceased operations which could cost approximately $3.58million.

Implications for Research/Policy

The aim of the undertaken research is twofold to demonstrate the importance of maritime cyber risk management both in terms of research but also in terms of policy. In terms of policy it was examined the application of the IMO MSC-FAL.1/Circ.3 guideline by maritime transport companies. That will demonstrate the effectiveness of IMO guidelines implementation to

maritime sector. In terms of research, we will get a better understating of the actions required by C-level managers for the cyber defense of their maritime operations during the digitalization phase that they are undertaken. That will help them to understand that cyber defense it is not just an additional guideline that they have to comply with but it is really adding value to their operation as it increases the supply chain robustness against criminal activities. Increasing the robustness especially in the post Covid-19 era where several workers work remotely and increase their exposure to cyber breaches is something important.

Keywords: *cyber-security, value added service, maritime transport sector, physical internet, digitalization*

References:

Acciaro, M., Renken, K. and El Khadiri, N., 2020. Technological change and logistics development in European ports. *European Port Cities in Transition*, pp.73-88.

IMO, 2017. Guidelines on Maritime Cyber Risk Management. Available at: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf, accessed 10/2/2020

Kalogeraki, E.M., Papastergiou, S., Mouratidis, H. and Polemi, N., 2018. A novel risk assessment methodology for SCADA maritime logistics environments. *Applied Sciences*, *8*(9), p.1477.

Küpper, D., Kuhlmann, K. Pieper, C., Burchardt, J. and Schlageter, J., 2020. The Green Factory of the Future. Available at: https://www.bcg.com/publications/2020/green-factory-of-future, accessed 10/6/2021

Montreuil, B., 2011. Toward a Physical Internet: meeting the global logistics sustainability grand challenge. *Logistics Research*, 3(2), pp.71-87.

Papathanasiou, A., Cole, R. and Murray, P., 2020. The (non-) application of blockchain technology in the Greek shipping industry. *European Management Journal*, *38*(6), pp.927-938.

Song, D.W. and Panayides, P. eds., 2015. *Maritime logistics: A guide to contemporary shipping and port management*. Kogan Page Publishers.

Statista, 2021. Average total cost per data breach worldwide 2020, by industry. Available at: https://www-statista-com.plymouth.idm.oclc.org/statistics/387861/cost-data-breach-industry/ accessed 11/6/2021