2020-10-16

Building a digital armour for the maritime sector against cyber-attacks

Karamperidis, Stavros

Dr Stavros Karamperidis
Plymouth Business School
University of Plymouth
United Kingdom
Tel: +44 1752 585589
E-mail: stavros.karamperidis@plymouth.ac.uk

Georgios Koligiannis
Hellenic Navy
Greece
Tel:+306940103646
Email: gkoligiannis1@gmail.com

Dr Fotios Moustakis
Associate Professor
Director of Dartmouth Centre for Sea Power & Strategy
School of Government, Law, & Criminology
University of Plymouth
Email: fotios.moustakis@plymouth.ac.uk

Building a digital armour for the maritime sector against cyber-attacks.

Extended abstract

Objective

Numerous cyber-attacks against high profile companies during the last decade across several sectors has proven that cyber-security should be a primary concern. In relation with the aforementioned, previous research highlighted that cyber incidents are the leading risk for business in the USA during the current year compared to other risks such as market volatility, natural catastrophes (i.e., earthquake, flood and storm), climate change, shortage of skilled workforce and changes in regulation (Allianz, 2020). Research by Zurich and Advisen (2018) has demonstrated that companies purchase cyber-liability insurance recently, in order to mitigate risk (e.g., reputation harm, breach notification costs, fines and penalties). On the other hand, Ipsos MORI (2019) has revealed that some organisations do not apply cyber-security countermeasures even though they have been exploited by a breach attack. Recently, the maritime transport sector is among the sectors that try to tackle cyber-risk due to the digital solutions applied in several ports and vessels. However, the challenges are countless, and there seems to be not only a gap in information technology solutions but also in academic research related to maritime cyber-security. The purpose of the research is to present evidence related to anticipated future maritime incidents,

maritime cyber risk insurance, and provide a minimum of countermeasures that support maritime cyber-hygiene.

Data- Methodology

The authors adopted the pragmatist philosophy, as the topic under survey is novel; thus, primary and secondary data were gathered from scholars and practitioners coming from several sectors and having an expertise in cyber-security. After conducting an in-depth literature review, an internet-based survey was conducted in order to collect up to date primary data. More specifically, a questionnaire was structured by using a sophisticated online survey software (i.e., Qualtrics) which was published in LinkedIn in two discreet groups (i.e., Maritime Cyber-Risk and Cyber-Security for Financial Institutions) and was also sent to high profile cyber-security companies. Even though more than 100 respondents accessed the survey online, overall 72 responses were completed in full and we were able to use for our study. More than 52% of the respondents had at least five years of experience in the cyber-security sector,. Thus, the majority of the participants could be characterised as senior cyber-security experts, and it could be argued that a representative sample was surveyed which further strengthens the validity of the research. Anonymity was provided to the participants in order not to be identified and freely express their opinion.

Results/ Findings

According to the survey, almost 93% of the respondents highlighted that maritime incidents will increase in the future. The aforementioned findings mainly could be attributed to the increasing attack surface due to the digitalisation of the sector and the low level of cyber-security culture. The remaining 7% represents the “traditional” view which the maritime sector has that it will not have face many cyber-incidents in the future. Surprisingly, this group of the respondents argued that hackers cannot gain money from the industry and that IMO prepares a new cyber-security framework to help the maritime entities in terms of cyber-security. Furthermore, the authors investigated if social media consist of a cyber-threat for the maritime entities, and the evidence revealed that respondents evaluate social media with scepticism in terms of cyber-security. More specifically, almost 74% of the respondents strongly or somewhat agree that social media could be a source of cyber-attacks. This could be attributed to the fact that social media helped malicious actors to mount spear-phishing e-mails and extort entity’s critical data. The survey has also shown that almost 87% of the respondents strongly or somewhat agree that mandatory reporting

of cyber-incidents could protect the maritime sector from cyber-attacks. The aforementioned numerical result is of high importance because, even nowadays, international entities do not know how many incidents have occurred, due to the absence of mandatory reporting. Little attention has been paid to cyber-insurance in the maritime sector until recently, thus the authors included in the questionnaire the question "*Should the maritime entities be insured against cyber-threats*"? The findings revealed that maritime entities should be insured against cyber-risks as almost 95% of the respondents highlighted the need to pay a premium for cyber-liability insurance. The findings could be attributed mainly to the fact that cyber-risk insurance is a way to transfer the risk to a third-party organisation. Furthermore, the results imply that the sector will witness increasing demand for cyber-security insurance. Therefore, the market could start preparing several frameworks of cyber-insurance in case of a ransomware attack which sometimes is not covered from P&I Clubs. The survey has also highlighted a minimum of countermeasures that could help the maritime entities maintain the cyber-security battle against potential malicious actors. More specifically, with regard to the IT countermeasures, the survey has shown that a company's IT department should keep authorised users to minimum software privileges, implement a white list policy for external device (i.e., deactivate unauthorized external devices) and prioritise the segmentation of IT network in order to protect critical systems and devices in case of a cyber-intrusion (e.g., ransomware). Furthermore, the IT department should conduct penetration testing before investing in IT systems, maintain up to date security patches for the IT systems, review policies in a regular basis and put in place business continuity plans. The survey has also proven that the sector will be more prepared against cyber-attacks if cyber-threat intelligence is optimized by sharing the incidents occurred and by training people to act responsibly and in a cyber-hygiene friendly manner. The survey has also shown that entities could provide insurance to existing critical assets by paying any premium required in cyber-liability insurance. However, further research needs to be conducted in order to quantify cyber-risk, which will help insurance companies to cover several exposures efficiently (e.g., data recovery and reputation harm).

Implication for research/ policy

Cyber-threats seem to be a high risk for the maritime industry which will endanger several entities if it is not addressed properly and on time. Recent incidents across the world have proved that vessels are not "*isolated islands*", and a simple malicious file could cause significant business disruptions, financial losses and reputation damage in case it infiltrates a company's network. As it was revealed by the research, a holistic

approach could help the industry to be less vulnerable to cyber-attacks. Thus, maritime entities should not only invest in IT systems but also to transparency, forensic analysis and employees' education on cyber-resilient practices. The limitation of the research includes the number of respondents that completed the online survey as it is a new topic for the maritime industry, which has been under researched until recently. Further research could be focused on P&I clubs that cover cyber-security exposure in order to extract useful data related to cyber-risk and the challenges that need to be addressed when the theft of trade secrets and human safety are triggered.

Keywords: *Maritime transport sector, Cyber-insurance, Cyber-security, Cyber-threats.*