Insurance for cyber risks in the port sector

I. Introduction.

Cyber risks have increased in the port sector in recent years due to the increase in automation, the use of disruptive technologies and the use of information exchange and communication platforms. These risks refer to threats that can compromise the security, integrity and confidentiality of information and computer systems in ports and port terminals.

The International Maritime Organization (IMO) mentions that cyber risk is the level of threat of a technological asset due to an event derived from the corruption, loss or endangerment of information or systems, which can cause operational, security and protection failures. to maritime transport.

Currently, there is an increase in the possibility of suffering economic or reputational damage or loss as a result of a cyberattack involving computer systems, digital platforms and networks. For example, we can list some ports or port terminals attacked with ransomware: in 2018, the Long Beach terminal, the port of Barcelona and the port of San Diego; in 2020, the Port of Kennewick; and in 2021, the port of Cape Town.

Cyber risks can manifest themselves in a variety of ways, including malware, phishing, ransomware, and denial-of-service attacks; each of these methods can cause a variety of problems, from the theft of sensitive information to disruption of port operations and port terminals.

In 2023, port terminals in Melbourne, Sydney, Fremantle and Brisbane suffered cyberattacks that halted port operations for four days and allowed sensitive information to be stolen. There is no transparency about the impact on the economic cost and data breach by DP Word. But, we can point out that the cyberattack affected the main Australian ports, which dispatch 40% of the merchandise that enters or leaves that country. Additionally, Australian government authorities changed their protection and risk management policies to address future cyberattacks of this magnitude.

The United States Federal Bureau of Investigation (FBI) mentions that there is no reliable statistic on the number of cyberattacks, since the majority of victims do not report these incidents. However, IBM's cybersecurity report estimates that at least 4% of ransomware-related attacks were directed at the transportation sector during 2022.

II. Cyber threats to critical infrastructure.

National regulations classify certain services or infrastructure as critical, because their functions are vital for society, the economy and/or the government. These infrastructures include energy supply systems, transportation networks, health facilities, and water services, among others. Ports and port terminals are classified as critical infrastructure by most countries. Countries establish stricter and more rigorous security standards and guidelines for ports and port terminals.

It is important to highlight that insurance companies offer more limited policies and coverage for this type of critical infrastructure, taking into account the cyber threats they face, as well as the high economic costs that a cyber-attack against ports or port terminals would produce.

For example, AXA no longer covers payments related to ransomware and Lloyd's of London no longer covers country-sponsored cyberattacks. The limits on commercial insurance coverage and the possible national economic losses generated by a cyber-attack on a port have caused the United States government to analyze the possibility of offering additional coverage as is the case with *Terrorism Risk Insurance Act of 2002* (GAO-22-104256. Cyber Insurance).

III. The insurance contract for cyber-attacks.

As cyber threats evolve, so do the solutions to protect against them. One of the tools to mitigate the economic cost associated with cyber-attacks is cyber risk insurance, which has become a key element within cyber risk mitigation and management strategies in the port sector.

The cyber-attack insurance contract is an agreement between a company and an insurer that provides financial coverage against losses arising from cyber incidents, these may include, but are not limited to, data breaches, ransomware attacks, interruptions of operations and legal liabilities arising from the exposure of personal and confidential data. For their part, insurance companies ask ports and port terminals to adopt minimum cybersecurity standards to contract or maintain insurance coverage for cyber-attacks, such as multi-factor authentication, data encryption or zero trust, among others.

The importance of having this type of insurance is that, as ports and port terminals digitize their operations, they also increase their vulnerability to these attacks, which can result in significant financial losses and damage to their reputation. Therefore, one of the most relevant characteristics of an insurance contract for cyberattacks is the variety of coverage that insurance companies can offer.

V. Coverage.

Insurance companies offer different coverages to mitigate the financial losses and expenses associated with a cyber-attack. Mainly, policy coverage can be divided into the following three items:

1. **Data violation:** generally cover the costs, expenses and fines derived from violations of regulations regarding the protection of personal and confidential data, as well as legal damages, judicial defense expenses and computer forensic expenses. IBM notes that the average cost of a cyberattack of this type was $4.2 million in 2021.

2. **Ransomware:** cover payments related to ransom and extortion to prevent the disclosure of data, recover information and/or eliminate the break-in or suspension of computer systems of the port or port terminal. A Palo Alto study mentions that the average ransom amount requested was $3 million during 2021. Likewise, the United States Cybersecurity and Infrastructure Security Agency indicates that the most used ransomware in recent years is LockBit, generating losses for 91 million dollars as a ransom payment during the years 2020 to 2022.

1. **Interruption of activities:** they mainly cover losses generated by disruption of operations, property damage, civil liability for property damage, costs to recover the operation of the systems and crisis management expenses. The cyber-attack that occurred in Australian ports in 2023 affected the clearance of 30,000 containers over four days.

VI. Limits of coverage and exclusions.

The insurance market is constantly changing, derived from the increase in cyber risks and cyber-attacks in the world. Consequently, insurance companies have significantly reduced the maximum coverage limit. Ports and port terminals should be aware of the limits on insurance coverage to primarily address events related to kidnapping or cyber extortion.

Along the same lines, cyber insurance policies may contain exclusions from the payment of economic losses derived from low levels of cybersecurity; errors, omissions or breaches of cybersecurity standards; cyberattacks carried out by employees; terrorism; cyber warfare; interruptions of services of other critical infrastructures such as electrical failures or telecommunications networks; natural disaster; as well as injuries or material damage. Particularly, this last scenario can considerably affect a port or port terminal, since a cyber-attack can cause physical damage, which could be excluded from some policies.

VII. Insurance is part of the cyber risk management and mitigation plan.

The contracting of cyber insurance in ports and terminals is a link in the risk mitigation strategy, which must also be accompanied by infrastructure and equipment, training, policies and risk management plans. Well, ECLAC indicates that the main triggering elements of a cyberattack are: phishing (31%), vulnerabilities (30%), theft of credentials (29%) and various causes (10%).

In conclusion, ports and terminals must take into account the increase in the number of cyber-attacks in the port sector and the decrease in the limits of insurance policy coverage when carrying out their cyber risk management plans. In addition, ports and terminals must invest in the training of their staff, since several of the cyberattacks had their origin in an omission, a human error or a failure to comply with cybersecurity standards, which can generate an exclusion from the payment of compensation. by insurance companies.