El seguro para riesgos cibernéticos en el sector portuario

I. Introducción.

Los riesgos cibernéticos han aumentado en el sector portuario durante los últimos años debido al incremento en la automatización, el uso de tecnologías disruptivas y la utilización de plataformas de intercambio de información y comunicación. Estos riesgos se refieren a las amenazas que pueden comprometer la seguridad, integridad y confidencialidad de la información y los sistemas de computación de los puertos y las terminales portuarias.

La Organización Marítima Internacional (OMI) menciona que el riesgo cibernético es el nivel de amenaza de un activo tecnológico por un evento derivado de la corrupción, pérdida o colocación en peligro de información o sistemas, lo cual puede causar fallos operacionales, de seguridad y protección al transporte marítimo.

Actualmente, hay un incremento en la posibilidad de sufrir daños o pérdidas económicas o de reputación como resultado de un ciberataque que involucre sistemas computacionales, plataformas digitales y redes. Por ejemplo, podemos enlistar algunos puertos o terminales portuarias atacadas con *ransomware*: en 2018, la terminal de Long Beach, el puerto de Barcelona y el puerto de San Diego; en 2020, el puerto de Kennewick; y en 2021, el puerto de Cape Town.

Los riesgos cibernéticos pueden manifestarse de diversas formas, incluyendo malware, phishing, ransomware y ataques de denegación de servicio, cada uno de estos métodos puede causar una variedad de problemas, desde el robo de información sensible hasta la interrupción de las operaciones de los puertos y terminales portuarias.

En 2023, las terminales portuarias de Melbourne, Sydney, Fremantle y Brisbane sufrieron ataques cibernéticos que detuvieron las operaciones portuarias a lo largo de cuatro días y permitieron el robo de información confidencial. No existe transparencia sobre el impacto en el costo económico y en la vulneración de datos por parte de DP Word., Pero, podemos señalar que el ciberataque afectó a los principales puertos australianos, quienes despachan el 40% de la mercancía que ingresa o sale de ese país. Además, las autoridades gubernamentales australianas cambiaron sus políticas de protección y gestión de riesgo para hacer frente a futuros ciberataques de esta magnitud.

El Buró Federal de Investigaciones de los Estados Unidos (FBI) menciona que no existe una estadística fiable sobre el número de ciberataques, ya que la mayoría de las víctimas no reporta estos incidentes. No obstante, el reporte de ciberseguridad de IBM calcula que por lo menos el 4% de los ataques relacionados con *ransomware* fueron dirigidos al sector del transporte durante 2022.

II. Las amenazas cibernéticas para las infraestructuras críticas.

Las normativas nacionales catalogan a ciertos servicios o infraestructura como críticos, debido a que sus funciones son vitales para la sociedad, la economía y/o el gobierno. Estas infraestructuras incluyen sistemas de suministro de energía, redes de transporte, instalaciones de salud, y servicios de agua, entre otros. Los puertos y las terminales portuarias están catalogadas como infraestructuras críticas por la mayoría de los países. Los países establecen estándares y directrices de seguridad más estrictas y rigurosas a los puertos y a las terminales portuarias.

Es importante destacar que las compañías de seguro ofrecen pólizas y coberturas más limitadas para este tipo de infraestructuras críticas, tomando en cuenta las amenazas cibernéticas que enfrentan, así como los altos costos económicos que produciría un ciberataque en contra de puertos o terminales portuarias.

Por ejemplo, la compañía *AXA* ya no cubre los pagos relacionados con *ransomware* y *Lloyd´s* de Londres no cubre los ciberataques patrocinados por países. Los límites en la cobertura de los seguros comerciales y las posibles pérdidas económicas nacionales generadas por un ciberataque a un puerto han generado que el gobierno de los Estados Unidos analice la posibilidad de ofrecer coberturas adicionales como sucede con *Terrorism Risk Insurance Act of 2002* (GAO-22-104256. Cyber Insurance).

III. El contrato de seguro para ciberataques.

A medida que las amenazas cibernéticas evolucionan, también lo hacen las soluciones para protegerse contra ellas. Una de las herramientas para mitigar el costo económico asociado a los ciberataques es el seguro para riesgos cibernéticos, el cual se ha convertido en un elemento clave dentro de las estrategias de mitigación y gestión de riesgos cibernéticos en el sector portuario.

El contrato de seguro para ciberataques es un acuerdo entre una empresa y una aseguradora que proporciona cobertura financiera ante pérdidas derivadas de incidentes cibernéticos, estos pueden incluir, entre otros, vulneración de datos, ataques de *ransomware*, interrupciones de operaciones y responsabilidades legales derivadas de la exposición de datos personales y confidenciales.

Por su parte, las compañías de seguros solicitan a los puertos y terminales portuarias la adopción de estándares mínimos de ciberseguridad para realizar la contratación o mantener la cobertura del seguro para ciberataques, como autentificación multifactor, cifrado de datos o confianza cero, entre otros.

La importancia de contar con este tipo de seguro radica en que, a medida que los puertos y terminales portuarias digitalizan sus operaciones, también aumentan su vulnerabilidad a estos ataques, lo que puede resultar en pérdidas financieras significativas y daños a su reputación. Por ello, una de las características más relevantes de un contrato de seguro para ciberataques es la variedad de coberturas que las compañías de seguro pueden ofrecer.

V. La cobertura.

Las compañías de seguro ofrecen distintas coberturas para mitigar las pérdidas financieras y los gastos asociados con un ataque cibernético. Principalmente, las coberturas de las pólizas pueden dividirse en los siguientes tres rubros:

1. **Vulneración a los datos**: generalmente cubren los costos, gastos y multas derivadas de las infracciones a la normativa en materia de protección de datos personales y confidenciales, así como los daños legales, gastos de defensa judicial y gastos de forense informático. IBM señala que el costo promedio de un ciberataque de este tipo fue de 4.2 millones de dólares en 2021.

2. **Ransomware:** cubren los pagos relacionados con el rescate y la extorsión para evitar la divulgación de datos, recuperar la información y/o eliminar la irrupción o suspensión de sistemas informáticos del puerto o terminal portuaria. Un estudio de Palo Alto menciona que la cantidad promedio de rescate solicitada fue de 3 millones de dólares durante 2021. Igualmente, la Agencia de los Estados Unidos de ciberseguridad y seguridad de infraestructuras indica el ransomware más usado en los últimos años es LockBit, generando pérdidas por 91 millones de dólares por concepto de pago de rescate durante los años 2020 a 2022.

3. **Interrupción de actividades:** cubren principalmente las pérdidas generadas por irrupción de operaciones, los daños a la propiedad, la responsabilidad civil por daños a la propiedad, los costos para recuperar la operatividad de los sistemas y los gastos de gestión de crisis. El ciberataque ocurrido en los puertos australianos en 2023 afectó el despacho de 30,000 contenedores a lo largo de cuatro días.

VI. Límites de la cobertura y excluyentes.

El mercado de seguros está cambiando constantemente, derivado del aumento de riesgos cibernéticos y ciberataques en el mundo. En consecuencia, las empresas de seguro han reducido significativamente el límite máximo de las coberturas. Los puertos y las terminales portuarias deben ser conscientes de los límites en la cobertura del seguro para hacer frente principalmente a eventos relacionados con secuestro o extorsión cibernética.

En la misma línea, las pólizas de ciberseguros pueden contener exclusiones al pago de pérdidas económicas derivadas de bajos niveles de ciberseguridad; errores, omisiones o incumplimientos a los estándares de ciberseguridad; ciberataques realizados por empleados; terrorismo; guerra cibernética; interrupciones de servicios de otras infraestructuras críticas como fallas eléctricas o en las redes telecomunicaciones; desastre natural; así como lesiones o daños materiales. Particularmente, este último supuesto puede afectar considerablemente a un puerto o una terminal portuaria, ya que un ciberataque puede generar daños físicos, que pudieran estar excluidos de algunas pólizas.

VII. El seguro es parte del plan de gestión y mitigación de riesgos cibernéticos.

La contratación de un seguro cibernético en puertos y terminales es un eslabón de la estrategia de mitigación de riesgo, que también debe ir acompañada de infraestructura y equipamiento, capacitación, políticas y planes de gestión de riesgo. Pues, la CEPAL indica que los principales elementos detonadores de un ciberataque son: phishing (31%), vulnerabilidades (30%), robo de credenciales (29%) y diversas causas (10%).

En conclusión, los puertos y terminales deben tomar en cuenta el aumento de el número de ciberataques en el sector portuario y la disminución en los límites de las coberturas de las pólizas de seguros al momento de realizar sus planes de gestión de riesgos cibernéticos. Además, los puertos y terminales deben invertir en la capacitación de su personal, ya que varios de los ciberataques tuvieron su origen en una omisión, un error humano o un incumplimiento en los estándares de ciberseguridad, lo cual puede generar una exclusión del pago de indemnización por parte de las compañías de seguros.

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 cyberattack on a port have caused the United States government to analyze the possibility of offering additional coverage as is the case with the Terrorism Risk Insurance Act of 2002 (GAO- 22-104256.

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.

3. **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.