Cyber risks in the transport and logistics sector

The increasing digitalisation and automation of the transport and logistics sector means that this industry, too, has become a target for cyber crime. The existence of many links in the logistics chain and the large number of small players handling goods on behalf of third parties also make the sector particularly vulnerable.

When it comes to cyber attacks on the transport and logistics supply chain sector, the most obvious consequences are the loss of products, cargo and freight and any direct repercussions for the client.

However, the impact of a cyber attack can be much more extensive and diverse than this. Unauthorised use of the freight forwarder's logistic planning system, misuse of the goods tracking system, the introduction of viruses into the recording applications of radar systems, or even the disruption of nautical navigation systems can all have enormous financial consequences for clients or suppliers, as well as for the company being hacked itself.

Just think of all the costs involved in investigating and rectifying the problem, the interruption to your operations, the expense of avoiding or limiting reputational damage, the costs relating to a loss of encryption to your data – including confidential data – and so on.

Classic insurance policies such as fire and operational insurance offer clients financial security in case of material damage to their real property. Liability insurance can reimburse damage to third parties that is causally linked to an error committed by the insured party.

However, classic insurance policies date from a pre-digital era, and focus on material and physical damage. This means that these classic policies do not (or only partly) cover financial losses connected to a loss of data or network connections.

There is thus a need for a comprehensive insurance solution.
High-quality information security

Cyber risks are inextricably linked to the **Confidentiality (C)**, the **Integrity (I)** and/or the **Availability (A)** of data – the so-called CIA triad.

The CIA triad provides the different criteria used in high-quality information security:
- The stored data must be **available** when required.
- The **integrity** of the data is ensued if the right data are linked to the right records.
- The **confidentiality** of the information ensures that the only persons who can access the information are those for whom it is intended.

The management and government of this CIA triad is made possible by the **Law on Privacy** (8 December 1992), which protects personal privacy in the context of the processing of personal data. This is further supported by the introduction in December 2015 of a **new European regulation: the General Data Protection Regulation Act**, which governs data processing on a European level and sets the obligations and sanctions imposed in case of data leaks.

A cyber policy insures against the **financial consequences** of data loss or a breach to the CIA triad.

Causes of damage

There is a wide range of possible causes for a loss of confidentiality, integrity or availability – ranging from a mistake made by an employee to malicious intent (hacking, malware) or an accident affecting data. Most of these causes can be insured against through a cyber policy.

Just like any other policy, cyber insurance also comes with a few exclusions – such as a general breakdown of service from an internet provider or an energy supplier (since in cases like this a large number of simultaneous claims may ensue, which insurers would not be able to reimburse in full).

Consequences of a cyber incident

We can assign the financial consequences of a cyber incident to three broad categories:
- operational impact;
- extra costs, rectification;
- legal consequences.

Depending on the type of incident, it is possible that multiple risk categories will be triggered.

The publication online of a database containing personal data may result in legal costs, while extra costs will also be incurred as the victims of the breach will need to be informed.

A denial-of-service attack that paralyses a company for an entire week will primarily have a large impact on its business activity.
Examples of cyber attacks

There are countless examples of and motives for cyber attacks in the transport and logistics sector:

- Cyber hacking in two terminal operators in the Port of Antwerp in order to steal containers full of drugs before the legal owner could collect them;
- Hacking a freight forwarder’s system in order to steal login details and sell them to the highest bidder, or in order to gain unauthorised information on where and when particular transports are planned;
- A DDOS (Distributed Denial of Service) attack can paralyse a company in order to make an ideological or a politico-economic statement;
- Installation of ransomware, which encrypts data and makes it unusable, in order to extort money from the company;
- ‘Portables’ (mobile phones, tablets etc.) fall into the wrong hands with a view to gaining access to company systems;
- Espionage and competition: an attack on the systems for managing loading, unloading and storage can result in delays to the shipment or delivery of a new product model, causing reputational damage and financial losses;
- AIS (Automatic Identification System) hack: a ship’s location coordinates are no longer transmitted, meaning that it officially disappears from radar. However, the hackers can keep tracking the ship and can cause it to take another course (e.g. allowing it to be hijacked in Somali waters);
- ...

Insuring cyber risks

A thorough analysis of your current insurance policies is required in order to understand what risks you are already covered against.

The table below offers an overview of the covers included in a cyber policy. Compare for yourself with a classic fire or civil liability policy.
We also recommend making a separate analysis for policies tailored to the transport and logistics sector. You should take the following points into account:

- **Cargo insurance**: this is a so-called ‘all-risks’ policy (insuring against damage to or loss of cargo). It also includes theft of cargo, but the BVT (Koninklijke Belgische Vereniging van Transportverzekeraars, or the Royal Belgian Association of Marine Insurers) specifically excludes ‘cybernetic attacks’ from its standard policies — meaning any loss or damage that is directly or indirectly caused by a computer, virus etc. is not covered.

- **CMR policy**: this is a non-mandatory liability policy providing compensation of up to around 10 euros per kilo of freight. As this is a liability policy, however, no cover will be provided in case of hacking or cyber attack if the insured party is unable to demonstrate that they were at fault.

### Next steps

1. **Put your affairs in order**
   - Bring both your general and your specifically IT-related security processes into line via audits and systematic updates or monitoring.
   - Gain an understanding of what data your company handles or comes into contact with, and what processes are performed on that data.
   - Analyse your own contractual liabilities towards suppliers and clients, and require your partners to also take any necessary steps themselves. After all, you are only as strong as your weakest link!
   - Map out potential problem areas within your company.
   - Make cyber risk a common topic of conversation throughout your company instead of restricting it to your IT department. After all, resources are assigned from the top down, so raising awareness among all your employees is essential to ensure the success of the overall process.

2. **Set up a business continuity plan**
   If a problem occurs, you will need to be able to act extremely efficiently with an understanding of who is responsible for the consequences of the damage (IT, legal, communication, engineers etc.). You should thus ensure that you know what measures need to be taken in the event of a crisis.

3. **Analyse your current insurance portfolio**
   Seek out expert guidance here — perhaps you are already well covered?

### Need more information?

**Annelies Helsen**  
Product Manager  
Tel. +32 3 217 54 13  
annelies.helsen@vanbreda.be

**Cécile Vassart**  
Product Manager  
Tel. +32 3 217 55 20  
cecile.vassart@vanbreda.be