ProWriters
Professional & Management Liability Insurance

Why the Logistics and Shipping Industry Needs Cyber Insurance

Fast, efficient distribution networks are a staple of the global economy. During the COVID-19 pandemic, logistics and shipping networks were literally lifesaving. However, this also paints a target on the back of an ill-prepared industry.

According to research by cybersecurity services firm BlueVoyant, ransomware attacks on shipping and logistics increased by a factor of three between 2019 and 2020. These attacks are now the #1 threat to distribution networks, but companies still lack adequate protection.

Effects of an attack could include:

- Lost revenue due to downtime
- Damaged digital assets
- Lawsuits from customers, employees, and third parties
- Hurt reputation from the attack
- Misappropriation of sensitive data

These costs are **not covered by typical CGL policies**. In such turbulent times, logistics and shipping companies need a comprehensive cyber coverage plan that includes risk management and preventative measures, as well as liability coverage.

The Cost of a Breach

The cost of a ransomware attack will vary depending on a variety of factors including the size of the company, whether they choose to pay the ransom, and the extent of the hack.

Additionally, ransom and lost revenue are not the only costs associated with a breach. Asset repair, negligence lawsuits, and government fines can pile up on companies handling sensitive shipping data.

For major hacks in the past few years, total costs are regularly in the millions of dollars, with the largest attacks costing tens and even hundreds of millions of dollars:

- A December 2020 attack on shipping giant Forward Air cost **$7.5 million dollars**
- A September 2020 hack cost logistics titan CMA CGM **$50 million dollars**
- A 2017 attack on global shipping firm Maersk cost between **$250-300 million dollars**

ProWriters
Professional & Management Liability Insurance

The Power of Comprehensive Coverage

With every company a target for ransomware, the question is not if, but when. Solid cyber insurance can alleviate the damage caused by hackers by providing specialized coverage for a wide array of damages. This includes:

First-Party Coverage

- Hiring forensic IT consultants to determine the origin of the breach
- Repairing digital assets
- Alerting affected customers and personnel
- Establishing a hotline to answer questions from affected parties

Third-Party Coverage

- Legal representation
- Document preparation
- Regulatory fines
- Payouts to affected customers

Some firms also provide risk management services to enhance a company's preemptive measures against ransomware. This strengthens their cybersecurity, making them a harder target for cyber crime, and landing them better insurance terms from carriers.

A Real World Example

In August of 2020, a ransomware attack hit four Canadian courier divisions of transport and logistics company TFI International. With their systems offline, the subsidiaries resorted to manually sorting, costing the company about $6 million in lost revenue.

TFI refused to pay the ransom, and as a result, the hackers leaked the stolen data onto the darkweb. While the company claims to not be aware of any misuse of client information, they alerted clients to the breach. They also launched an investigation into the origins of the data breach.

TFI did not sustain significant damages from this attack. However, not every company is so lucky. Without comprehensive coverage, companies, customers, and business partners are all at risk. Get cyber insurance today.