ProWriters
Professional & Management Liability Insurance

Managing Cyber Risk in the Logistics Industry

The Danger: Ransomware Threatens to Hold Logistics Hostage

According to cybersecurity service provider BlueVoyant:

- Ransomware attacks against logistics and shipping companies tripled from 2019 to 2020, confirming ransomware is the #1 threat this sector faces.
- Of the 20 top global shipping and logistics companies BlueVoyant assessed, all saw evidence their networks had been targeted, yet 90% have open remote desktop or administration ports and insufficient email security—the main ways ransomware infiltrates networks.
- The logistics sector relies too often on out-of-date processes and technologies, creating needless exposure to cyber attacks.

Ransomware attacks can lead to:

- **Interruption of operations**
- **Financial loss**
- **Reputational damage**

The Solution: Robust Cyber Protections and Strong Cyber Insurance

The good news is logistics companies can take several immediate, practical steps to make their networks more secure. Some important measures include:

- **Multi-factor authentication (MFA)**—Requiring credentials beyond a user name and password helps limit who can access protected data.
- **Managed detection and response (MDR) services**—Outsourcing continuous, real-time monitoring of a network and its endpoints (servers, computers, and devices) increases a company's ability to successfully identify and respond to threats.
- **DMARC and SPF controls**—Domain-based Message Authentication, Reporting & Conformance allows email domain owners to decide how mailbox providers deal with incoming unauthenticated messages. A Sender Policy Framework identifies IP addresses authorized to send messages on a domain's behalf. Both give companies greater control over email traffic, reducing ransomware's opportunities to enter their networks.
- **Secure email gateways (SEGs)**—Monitoring incoming and outgoing email for spam, phishing attacks, and other malicious content helps prevent ransomware's entrance into a network.

- Patching procedures—Distributing and installing software updates in a consistent and timely way, reducing criminals' chances to exploit software vulnerabilities.
- "3-2-1" backup protocols—Creating one primary backup and two copies of data, on two different media, and keeping at least one backup off-site protects the information and makes it easier for companies to recover in the event of a cyber attack.

Logistics companies must also invest in a comprehensive Cyber Insurance policy.

General Liability policies won't cover the costs of:

- digital forensics investigation
- notifying vendors and customers of a data breach
- crisis and reputation management
- restoring operations and rebuilding a network

Case Study: Forward Air

In December 2020, the Hades ransomware gang targeted trucking and logistics company Forward Air. The company had to take all its IT systems offline, causing a communications blackout that significantly disrupted and delayed the flow of freight—and at the height of the holiday shipping season. For some tasks, such as tendering, logistics providers were forced to resort to expensive manual processes.

The attack ultimately cost Forward Air $7.5 million in lost revenue. It also allowed hackers to steal Forward Air employees' personal information, including Social Security numbers, driver's license numbers, passport numbers and bank account numbers.

While Forward Air's SEC filings about the attack don't state whether the company paid the ransom or relied on a Cyber Insurance policy, the incident "shows once again why most security researchers have been preaching prevention rather than a cure for the ransomware problem," according to ZDNet.