MOVER'S CHOICE

CYBER RISK – TRUCKING & TRANSPORTATION

Cyber-crime now costs the world over $1 Trillion – More than 1% of global GDP, up 50% from two years ago.[1] In the first half of 2021, the average ransomware payment climbed to $570,000.[2] Cyber criminals have become increasingly bold, sometimes resorting to harassing a business's customers, partners and employees to secure their ransom payment.

2021 has further proven to insurance and security professionals that not one business is immune to cyber-attacks. With 53% of claims affecting businesses with less than $50M in revenue, small businesses struggle to cope with an uninsured cyber loss.[3]

In partnership with BIZLock Cybercrime Protection, Mover's Choice is happy to offer coverage for the following cyber threats:

- **Breach Response:** Call our Incident Response On-Demand™ 24-7. Coverage is provided for forensic experts, legal support/law firm, PR, consumer notifications, and identity protection remedies. Getting your business back in operation is priority #1.
- **Privacy & Security Liability:** When you have a cyber or privacy related incident, a lawsuit can be catastrophic. Cyberspace exposures and the legal landscape continue to evolve rapidly. Covering litigation expenses and plaintiff claims is the primary goal of cyber liability coverage.
- **Ransomware:** Coverage is provided for costs to investigate and terminate cyber extortion threats, including reimbursement of money and cryptocurrencies paid to recover from the incident.
- **Business Interruption:** Loss of income following a cyber-attack or from operational or technical failure is a real and complex threat.
- **Data Reconstruction:** Costs to restore, replace or re-create digital assets when lost or corrupted as the result of a breach or virus.
- **Regulatory Fines & Penalties:** Coverage is provided for defending against regulatory actions and resulting fines and penalties arising from a covered privacy event.
- **Multimedia Liability:** Coverage for wrongful acts (defamation, libel, slander, infringement of copyright) in connection with material on an internet site owned by the insured or related social media.
- **Employee Protection:** Your employees are covered with automatic identity protection, including unlimited access to our team of experts, risk management education and personal identity insurance.

BIZLOCK

MOVER'S CHOICE

CYBER RISK – TRUCKING & TRANSPORTATION

LOSS & INCIDENT EXAMPLES

Example 1 RANSOMWARE

A Texas-based trucking firm was the victim of a ransomware attack and corporate identity theft, which started when the VP of the company opened a seemingly harmless email attachment which described itself as a "resume" for an applicant who was applying for a job-opening. Upon clicking on the "resume" document, a malware virus was introduced onto the system and quickly went to the main server's shared files, which locked up all the servers and displayed a ransom message on every computer.

After paying the ransom and gaining access to their systems, the firm thought the case was closed. That was, until the phone calls started coming in from clients. When the ransomware encrypted the servers, the hackers had also stolen all of their customer data, employee data, SSN's, etc., and started calling brokers on the company's list, booking loads under their name and insisting on cash advances, which totaled up to $800/load in some cases. When the loads never got picked up, customers started calling. As highlighted by this event, cyber-attacks can disrupt goods and services, divert finances, and hurt a company's reputation.[4]

Example 2 PHISHING

An unauthorized actor used a phishing email campaign to gain access to certain employees email accounts. Upon further investigation, it was found that the attacker had also gained access to the company's HR platform, compromising personal information of the company's employees.[5]

Example 3 EMAIL SPOOFING

A trucking dealer was the victim of an email spoofing attack by an individual pretending to be the owner of the company requesting a copy of employee W-2 information from an employee of the company. The employee was duped by the scam and sent documents containing W-2 information to the fraudster.[6]

Example 4 CYBER EXTORTION

A 25-truck company was hacked after downloading a malicious file. All of their data was encrypted and they received a $300,000 ransom demand to retrieve their files. After they refused to pay the ransom, the hackers released sensitive customer information to the public.[7]

1 Allianz Risk Barometer, 2021

2 Palo Alto Networks, Unit 42 Ransomware Threat Report

3 Net Diligence Cyber Claims Study 2020 Report

4 https://www.fleetowner.com/technology/battling-hack-one-fleet-s-story

5 https://www.doj.nh.gov/consumer/security-breaches/documents/roadrunner-transportation-20180713.pdf

6 https://www.freightwaves.com/news/inside-a-ransomware-attack-on-a-small-trucking-company

7 https://www.databreaches.net/wp-content/uploads/BentleyTruckSvces.pdf

Summary information only. Please refer to the policy for full terms/limitations.

BIZLOCK