SENTINEL

Safeguarding Your Success

CYBER LIABILITY QUICK GUIDE

Why Buy Cyber Liability Insurance?

In today's world, Information Technology (IT) is an essential tool for businesses of all sizes. IT is used in several ways, such as communicating through email, providing information or services via a website, storing, and utilizing customer data, and more.

Cyber Liability risks are rapidly evolving due to technological advancements and new regulations. Businesses can be held liable for compromised data, and insurance experts consider the risk of Cyber Liability losses to exceed those of fraud or theft.

Did You Know?

- Cybercrime is predicted to cost businesses more than $10.5 trillion annually by 2025
- Data breaches can come from external and internal sources:
  - Outsiders: 70%
  - Organized Criminal Groups: 55%
  - Internal Bad Actors: 30%
- Business Email Compromise (BEC), Funds Transfer Fraud (FTF), and Ransomware attacks accounted for approximately **60%** of all Cyber incidents in 2022[1]
- Ransomware attacks now occur every 11 seconds, down from 40 seconds in 2016
- Ransomware and FTF claims averaged $303,000 and $198,000, respectively in 2022[2]
- 60% of businesses affected by a ransomware attack will close within 6 months
- 43% of Cyberattacks target small businesses (companies <$25M)[3]

[1] Coalition Inc., NAIC
[2] Coalition Inc., NAIC
[3] Coalition Inc., NAIC

How Can You Prevent Cyber Incidents?

1. Multi-Factor Authentication (MFA)
2. Endpoint Detection and Response (EDR)
3. Secured, encrypted, and tested backups
4. Privileged Access Management (PAM)
5. Email filtering and web security
6. Patch management and vulnerability management
7. Cyber incident response planning and testing
8. Cybersecurity awareness, training, and phishing testing
9. Hardening techniques, such as Remote Desktop Protocol (RDP)
10. Logging and monitoring network protections
11. End-of-life systems replaced or protected
12. Secure vendor/digital supply chain

How Is Sentinel Dedicated To Safeguarding Your Success?

There are 3 integral parts to Sentinel's Cybersecurity solutions/services:

Pre-Breach

- Helping clients identify risks, understand coverage, and educate employees
- Access to IT security collateral and a network of vendors

Breach Response

- Side-by-side assistance until Cyber incident is resolved

Claims Support

- Claims team at the forefront of defending clients against Cyber incidents

Cyber Liability Claims Scenarios:

Scenario 1 – Ransomware

A firm came to a roadblock when its data was encrypted, rendering it unusable. Back-ups were also corrupted. The threat actor claimed to know the insured had the financial ability to pay and demanded more than $500,000. After consultation with the Cyber claims representative and incident response coach, the decision was made to pay the ransom, which was covered under their existing Cyber Liability policy.

Scenario 2 – Social Engineering

An organization had a $110,000 invoice with one of their third-party vendors. They were advised via email that their ACH transfer had been sent to the incorrect bank. They were subsequently given a different account and instructed to wire the funds. The bank information provided was fraudulently sent to them in a hacked email. The organization's third-party vendor later called them to advise that this was an imposter email. The bank who processed the ACH transfer successfully retrieved approximately $20,000. The organization had a Cyber Liability policy with a $100,000 limit and paid approximately $75,000 after the deductible was applied.

Scenario 3 – Payment Card Industry Data Security Standard (PCI DSS)

A store experienced a data breach that exposed customer credit card information. The store paid to mitigate the breach, including a forensic assessment, network security services, credit monitoring for impacted customers, and a public relations campaign to restore confidence in its brand and reputation. The total cost to mitigate the breach was nearly $500,000.

Sentinel's Cyber Liability Resource:

Reeves Zaytoun, MLIS
Account Executive, Cyber/Technology Errors & Omissions
rzaytoun@sentinelra.com | 919.926.4641

Reeves is a highly detail-oriented professional with extensive experience in the technology industry. As part of our Specialty Lines team, Reeves oversees, manages, and implements various initiatives. With his vast knowledge, he provides technical support to both our clients and internal teams, with a particular focus on Cyber lines of coverage. Reeves is dedicated to addressing our clients' current needs and exploring new opportunities in this field.

CONTACT US TO LEARN MORE
Questions on your Cyber coverage, rates, claims, or more? Call or email our team today!