



Cyber Liability Insurance: What You Need to Know

72% of SMB companies expect an unauthorized attempt on their data this year.

Ransomware attacks are skyrocketing in frequency and severity, driving companies to consider cyber insurance for needed protection. Our guide will help you understand cyber insurance, how to choose a policy that adequately covers your business, and what it takes to qualify for coverage.

01 Understand the types of cyber insurance

Forensic Investigation

Covers forensic, technical, or legal services to assess if a cyber attack has occurred.

Theft & Fraud

Covers impacted data from criminal or fraud event, including theft and transfer of funds.

Computer Loss & Restoration

Covers damage & restoration of hardware and software, and data, due to a cyber attack.

Hacksurance

Insurance against cyber and hacking attacks.

Business Interruption

Covers lost income and loss of production costs due to a cyber event or data loss.

Extortion

Covers cost of investigating attack threats and extortionist payments to protect sensitive information.

Reputation Insurance

Mitigates against reputation attacks and cyber defamation.

02 How company size impacts your risk

Small to Mid-sized Businesses

- Most successfully hacked
- Less in-house IT security budget/expertise
- Need outside security help
- Use cyber insurance to reduce risk
- Coverage through agencies

Large Corporations

- Most targeted
- Have in-house IT expertise
- Coverage generally direct from insurer

03 What you need to cover



Expenses can add up rapidly once a breach is exposed and reported. Most SMB companies with cyber insurance only cover liability (\$50K), which isn't enough when the average cost begins at \$120,000.

Here's what you need to consider covering:

- > Customer Loss
- > Business Disruption
- > Regulatory Fines
- > Legal Costs
- > Public Relations
- > Direct Financial Loss

04 What influences cyber insurance costs

Policy pricing has increased sharply since 2021. Be financially prepared for higher rates or a rise in current policy costs. The advantages still far outweigh the cost.

These six elements that influence insurance costs:

- 1 Size and Complexity:** The more devices, users, and systems involved, the larger the threat surface and possibility of becoming a victim.
- 2 Industry:** Some are targeted more than others, like healthcare, manufacturing, and public administration. Attack frequency and damage payouts, as in the financial industry, are factors.
- 3 Company Revenue:** Revenue determines the potential losses from a cyberattack, and impact policy costs.
- 4 Coverage Type:** Policies are based on frequent or dangerous risks that need to be covered. Highly sophisticated attacks cost more than threats like credential or employee identity theft.
- 5 Geographic Presence:** International operations increase risks and require layers of security and data protection adapted to local regulations.
- 6 Remote Workforce:** Remote working requires VPNs and extends an organization's surface outside the perimeter, increasing risk.



Did you know? General business insurance *doesn't* cover cyber attacks?

05 Understand how to qualify for cyber insurance

To get coverage, businesses applying for cyber insurance must show they are implementing a long list of cybersecurity technologies and practices including MFA and an incident response plan. Use this checklist to evaluate your cybersecurity practices and determine which insurance types are right for you.

Cyber Security Practices	Yes	No
Formalize your security policies and procedures		
Institute cybersecurity awareness training for employees		
Update your incident response plan		
Ensure compliance with GDPR, HIPAA, and PCI DSS, as they apply		
Establish role restrictions for sensitive information		
Appoint a position responsible for your cyber security		
Set up a patching schedule and controls		
Document procedure for testing network security controls		
Test and document backup procedures		
Ensure redundancy of all critical systems		
Update encryption processes		
Document your disaster recovery plan		
Have AV active on all servers, computers, and endpoints		
Put endpoint detection and response (EDR) in place		
Have a third-party security assessment completed		
Require MFA to ensure secure email access		
Require MFA for remote access to company network		
Limit remote access to VPN		
Ensure active, updated firewall protection		
Replace EOL hardware and systems		
Prepare to have your systems tested		

Want to learn more?

Insurance companies are requiring a Security Risk Assessment and MFA to qualify for coverage – we can help you with that!

Schedule a time to talk