

# The Ins and Outs of Cyber Insurance

A Brief Overview for SMBs



## What is Cyber Insurance?

Cyber insurance (also referred to as cyber liability insurance or cybersecurity insurance) is a type of insurance that an organization can purchase to help mitigate or cover the financial risks of a possible cyberattack. In exchange for a monthly or quarterly fee outlined in a cyber insurance policy, the cyber insurance provider absorbs some of the financial risks of a cyberattack.

## Why Should SMBs Invest in Cyber Insurance Coverage?

SMBs should secure cyber insurance coverage due to the statistical risks to their business:

20%

Every five years, 20 percent of small and medium-sized businesses suffer from data loss due to a significant disaster.

60%

According to Datto, ransomware remains the most common cyberthreat to SMBs, with 60 percent of MSPs reporting that their SMB clients have been hit as of the third quarter of 2020.

75%

In 2019, three in four SMBs in the U.S. had reported a digital attack in the preceding year, according to the Ponemon Institute.

43%

According to Accenture's Cybercrime study, 43 percent of all cyberattacks are on small businesses.

14%

Accenture's Cybercrime study shows that only 14% of SMBs are prepared to face cyberattacks.

95%

According to the World Economic Forum, 95 percent of cybersecurity breaches are attributed to human error.

\$653k

SMBs spend, on average, \$826 to \$653,587 on cybersecurity incidents, according to 2021 SMB Data Breach Statistics.

\$10.5T

Cybercrime is estimated to increase by 15 percent, with costs reaching \$10.5 trillion by 2025.

The average cybersecurity insurance claim cost for a small to medium enterprise is \$345,000. *2023 Cyber Claims Study*



## What Are the Benefits of Cyber Insurance for SMBs?

Here's what SMBs can expect to get out of investing in cyber insurance coverage:



### Cyber Risk Remediation

Cyber insurance coverage protects businesses against the risk of cyberattacks, cyber incidents and major cyber events linked to terrorism.



### Financial Protection

Cyber insurance reduces the financial impact of cyber incidents. These expenses can include investigation fees, credit monitoring services, legal fees, costs for data breaches, business interruption, revenue loss and computer system restoration.



### Legal Support

Cyber insurance helps pay for the costs of legal counsel, legal compliance with regulations and potential lawsuits due to data breaches or privacy violations following a cyber incident.



### Peace of Mind

Cyber insurance lets businesses focus on day-to-day business operations without nonstop worry about shouldering all the possible financial consequences of a cyber incident.



### Secure Reputation

Cyber insurance coverage helps SMBs look committed to cybersecurity due to the security requirements needed to get coverage.

## What Does Cyber Insurance Cover for SMBs?

Cyber Insurance is as dynamic as the companies it protects and is far from standardized. However, areas SMBs can typically expect coverage in these areas:



### Cyber Extortion



### Data Loss, Recovery, and Re-creation



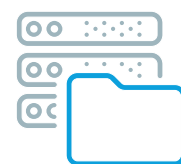
### Computer Fraud



### Business Interruption and Loss of Revenue Due to a Breach



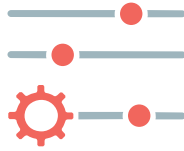
### Loss of Transferred Funds



### Digital Asset Management

## What Does Cyber Insurance Not Cover for SMBs?

Cyber Insurance policies typically exclude preventable security issues caused by humans, including the following:



**Poor Configuration Management**



**Mishandling of Digital Assets**



**Preexisting or Prior Breaches that Occurred before the Policy Purchase**



**Intentional Cyber Incidents Initiated by Employees**



**Infrastructure Failures not caused by Purposeful Cyberattacks**



**A Breach as a Result of a Known Vulnerability within the Company that was not Addressed**



**The Cost to Improve Technology Systems, including Security Hardening in Systems or Apps**



**Intellectual Property Loss (Proprietary Information, Trade Secrets or Intangible Assets)**

## What Types of Cyberattacks Does Cyber Insurance Cover for SMBs?

Cyber insurance providers typically offer coverage for, but are not limited to, these common cyberthreats:



**Malware Attacks**



**Password and Phishing Attacks**



**Ransomware Attacks**



**Man-in-the-Middle (MitM) Attacks**



**URL Interpretation and Poisoning**



**SQL Injection Attacks**



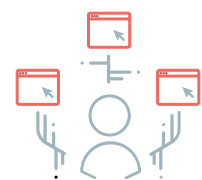
**Distributed Denial of Service (DDoS) Attacks**



**DNS Spoofing**



**Botnets**



**Watering Hole Attacks**

## What Do Cyber Insurers Look for Before Insuring SMBs?

Insurance providers can deny coverage to companies not meeting minimum standards to prepare for and defend against cyberthreats. Specific criteria may vary slightly by provider, but typically, four types of security controls are required:



### Multi-Factor Authentication (MFA)

MFA protects data or applications by requiring a user to present two or more credentials to verify user identity at the time of login.



### Security Awareness Training

User training is vital to educate staff on proper cyber hygiene and the ways to identify cyberattacks that may be encountered via email and the web.



### Encrypted Backups

Businesses need encrypted backups to minimize downtime in a systems crash, natural disaster or security event.



### Endpoint Detection & Response (EDR)

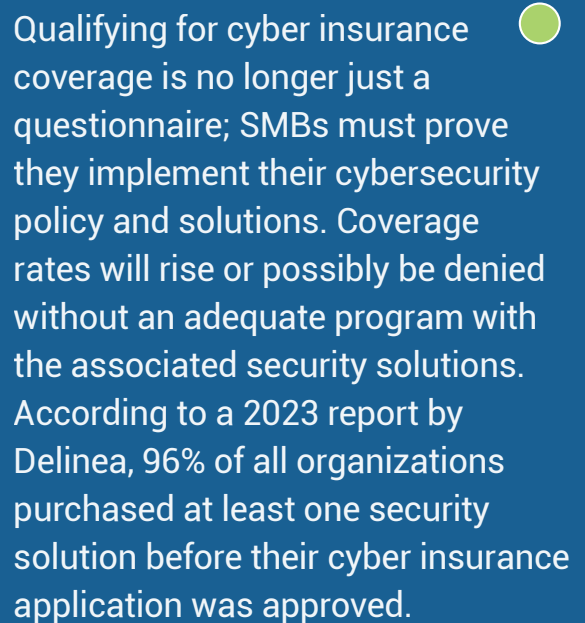
With EDR, you can monitor, detect, and mitigate any threats on your endpoints (computers, laptops, servers, etc.) regardless of whether your employees are in the office or working remotely..

## What Does Qualifying for Cyber Insurance Coverage Look Like?

Cyber insurance carriers are ultimately looking for maturity in the company they're insuring, including:

- A robust patching schedule to patch known vulnerabilities, including the Common Vulnerabilities and Exposures (CVE) catalog sponsored by the United States Department of Homeland Security (DHS)
- Consistent data governance across the organization

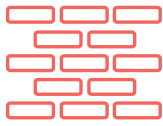
The underwriter will frequently bring a Chief Information Security Officer (CISO) or equivalent member of the organization responsible for security into an interview to cover every system and procedure the company has in place before implementing the policy. Cyber insurers will also conduct regular vulnerability scans to detect open ports and send them to the organization seeking coverage to shut them off. It gets more challenging for companies to get their desired low rate when they lose defensibility.



Qualifying for cyber insurance coverage is no longer just a questionnaire; SMBs must prove they implement their cybersecurity policy and solutions. Coverage rates will rise or possibly be denied without an adequate program with the associated security solutions. According to a 2023 report by Delinea, 96% of all organizations purchased at least one security solution before their cyber insurance application was approved.

## How TPx Helps Businesses Acquire & Maintain Cyber Insurance

TPx provides key solutions that cyber insurance companies look for before approving businesses for coverage.



### Managed Firewalls

TPx offers a next-gen firewall (NGFW) with unified threat management (UTM), virtual private network (VPN) and managed detection and response (MDR). A firewall on your network blocks malicious traffic from entering your network, reducing your threat risk.



### Inbox Detection & Response (IDR)

TPx's Managed IDR service allows users to easily report suspicious emails with an Outlook plug-in to quickly determine if the emails are safe or malicious.



### Backup and Disaster Recovery (BDR)

We help organizations quickly recover from system downtime and data loss caused by cyberattacks, human error, system failures and natural disasters. Using advanced hybrid local/cloud technology and skills management resources, TPx delivers a turnkey BDR solution that will meet recovery objectives and give peace of mind to your cyber insurance provider.



### Security Awareness Training (SAT)

TPx provides regular training courses with phishing simulations, following NIST guidelines. These help your employees conduct themselves with proper cyber hygiene best practices to minimize the risk of phishing and ransomware attacks.



### Virtual Compliance Officer (VCO)

TPx's endpoint security services leverage remote monitoring and management (RMM) and patch management to keep your servers and workstations secure and optimized.



### Managed Detection and Response (MDR)

Discover, prevent and recover from cyber threats faster. TPx's MDR helps you identify more threats, reduce attack dwell time, and proactively mitigate attacks. We offer managed detection and response for both firewalls and endpoints.



### Endpoint Management & Security

TPx protects endpoints with patch management, next-gen antivirus, remote monitoring and management (RMM), managed detection and response (MDR) and more.



### Security Advisory Services

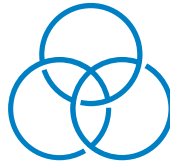
TPx advisory services provide comprehensive security consulting that can help improve your security posture and protect your business. Our services include network vulnerability and penetration scanning, cybersecurity plans and policies (such as incident response plan), network security assessment, wireless security assessment and ransomware readiness assessment. Insurers often require an incident response plan and cybersecurity risk assessment to determine premiums and coverage levels.

## Why TPx?

You have enough business challenges. Partnering with TPx provides the support it needs so you can focus on core business goals. At TPx, we have the products, services, experience and certifications to keep your network and applications running smoothly and safely.



**Our mission is to be the easiest MSP to do business with**



**We solve the biggest IT issues – cybersecurity, connectivity, and collaboration – under one umbrella**



**We have 120+ certifications across 60+ competencies, like CompTIA, Cisco, Fortinet, Microsoft, SMC and more**



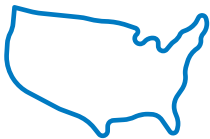
**We offer HIPAA, PCI DSS and SOC 2-compliant solutions**



**We offer different service levels and highly customizable solutions**

24  
7  
365

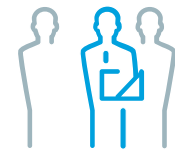
**We provide enterprise-class, 24/7 support**



**We have a national footprint with multi-site, multi-carrier, partner coverage**



**With thousands of customers nationwide, we're big enough to get the job done and small enough to be agile**



**We have various dedicated teams to ensure service excellence**



**We continuously invest in automation, self-service innovation, and back-office transformation**



**We are committed to the most densely monitored service delivery platform in the industry**



**We understand and embrace the criticality of our customers' performance analytics**



**Ready to Secure Your Business?**

**Contact TPx today. Visit [tpx.com/contact-sales](https://tpx.com/contact-sales) or call 866-706-7441.**