9 Things SMBs Need to Know About Cyber Insurance

Cyber insurance protects SMBs from costs your company incurs due to cyberattack. While cyber insurance can help mitigate some of the risks of cyberattacks, it's not a silver bullet for cybersecurity and obtaining and maintaining cyber insurance coverage requires some level of cybersecurity protection.

Here are nine things you need to know about cyber insurance.

1 Third-Party Cyber Insurance Covers Breaches on Other Organizations' Networks

Cyberattacks are on the rise, with **ransomware-related data breaches having doubled** in each of the past two years, according to Identity Theft Resource Center's (ITRC) 2021 Annual Data Breach Report. 43% of attacks are aimed at SMBs, but only 14% are prepared to defend themselves. Your business should consider acquiring cyber insurance; **a single cyberattack costs companies of all sizes an average of $200,000**. Getting reimbursed for damages incurred if you're breached can be vital to financial recovery.

2 To Obtain Cyber Insurance, You Need to Implement Cyber Defenses

You can purchase cybersecurity insurance through most business insurance providers, but **cyber insurers consider organizations with poor security practices as an unwanted,** and potentially dangerous, liability to their business model. Improving your cyber defenses will improve your chance of qualifying for cyber insurance coverage, as well as obtaining the best rates.

3 Cyber Insurance Benefits Businesses of All Sizes

Your business isn't too small to be a target of cyberattack. According to Hiscox, an international cyber insurer, **23% of small businesses suffered at least one cyberattack in the past year**. If you handle or use digital information, you need to mitigate your cyber risks and protect your company, your employees and your customers. In fact, 99% of all cybersecurity insurance claims come from small to medium-sized enterprises (SMEs). According to a 2023 Cyber Claims Study, **the average cybersecurity insurance claim cost for a small to medium enterprise is $345,000**.

4 Cyber Insurance Varies, But Typically Covers Six Key Areas

Cyber Insurance is as dynamic as the companies it protects and is consequently far from standardized. However, some things that it typically covers include:

- **Cyber Extortion**
- **Data Loss, Recovery & Re-Creation**
- **Computer Fraud**
- **Interruption/ Revenue Loss Due To Breach**
- **Loss Of Transferred Funds**
- **Digital Asset Management**

5 First-Party Cyber Insurance Covers Breaches on Your Own Network

First-party cyber liability insurance addresses the financial fallout associated with cybersecurity breaches on your own network and can include:

IT Forensic Costs

To determine what information may have been breached and how

Notification Costs

To notify all individuals and businesses affected

Credit Protection Costs

To provide credit monitoring services to all parties affected

Crisis Mgmt Costs

For media relations for reputation management

6 Third-Party Cyber Insurance Covers Breaches on Other Organizations' Networks

Third party coverage helps pay for lawsuits caused by data breaches on clients', vendors', regulatory bodies', service providers' and other organizations' network systems and can cover:

Privacy Lawsuits

These suits would be brought by customers or employees who allege you were responsible for data loss.

Regulatory Fines

In some cases, you may need to pay authorities or compliance regulators and agencies as a result of the loss.

Claims

Claims could be brought that allege a breach of contract or negligence on your part.

7 Cyber Insurance Requires Security Controls

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

Multi-Factor Authentication (MFA)

TMFA 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 important to educate staff on proper cyber hygiene and the ways to identify cyberattacks encountered via email and the web.

Encrypted Backups

In the event of a systems crash, natural disaster or significant security event, businesses need encrypted backups to minimize their downtime.

Endpoint Detection & Response (EDR)

You can monitor, detect, and mitigate threats on computers, laptops, servers, etc., regardless of whether your employees work in the office or remotely.

8 Get Help from an MSP Like TPx with Your Cyber Insurance Needs

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

Managed Firewalls

TPx cybersecurity experts will configure, deploy, manage and monitor your next-generation firewalls to block any unsolicited traffic from your network

.Security Awareness Training (SAT)

TPx's security awareness training includes monthly phishing simulations and courses with automated reporting to track results.

Managed Detection & Response (MDR)

TPx's MDR helps your business identify more threats, reduce attack dwell time and proactively mitigate attacks on your firewalls/endpoints.

Backup and Disaster Recovery (BDR)

With ransomware on the rise, TPx's managed backup can help you restore your system to a point before data is held hostage.

Virtual Compliance Officer (VCO)

Specialized support so you adhere to legal standards and industry regs, safeguard against penalties, and bolster your reputation.

Security Advisory Services

Improve your security posture with network vulnerability and penetration scanning, plus cybersecurity gap, network security, and ransomware readiness assessments.

Endpoint Mgmt & Security

Endpoint security services leverage remote monitoring and management (RMM) and patch management to keep your servers and workstations secure and optimized.

Inbox Detection & Response (IDR)

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

Incident Response Plan

TPx experts will help your business create an Incident Response Plan, a documented process to respond to and recover from any cybersecurity breach event.

Plus, TPx offers multi-factor authentication (MFA) under Microsoft 365 and Firewall solutions.

9 Consider TPx

SMBs like to choose TPx to meet their cybersecurity needs because:

- TPx's mission is being the easiest MSP to do business with
- TPx solves the biggest IT issues – cybersecurity, connectivity and collaboration – under one umbrella
- TPx has 120+ certifications across 60+ competencies, like CompTIA, Cisco, Fortinet, Microsoft, SMC and more
- TPx offers HIPAA, PCI DSS and SOC 2-compliant solutions
- TPx provides enterprise-class, 24/7 support
- TPx offers different service levels and highly customizable solutions
- TPx has a national footprint, with multi-site, multi-carrier and partner coverage
- With thousands of customers, TPx is big enough to get the job done and small enough to be agile
- TPx has various dedicated teams to ensure service excellence
- TPx continuously invests in automation, self-service innovation and back-office transformation
- TPx is committed to providing the most densely monitored service delivery platform in the industry
- TPx understands and embraces the criticality of our customers' performance analytics

TPx takes the worry out of IT services and cybersecurity for businesses. We can help your company qualify for and maintain your cyber insurance coverage while reducing real-world risk of cyberattacks.

Download

Learn More About Cyber Insurance in TPx's eBook

Contact TPx at 866-706-7441 or visit tpx.com.