The SMB Owner's
Cyber Insurance Checklist

www.the20.com

The SMB Owner’s

Cyber Insurance Checklist

Purchasing a cyber insurance policy for your small to medium-sized business (SMB) can go a long way in ensuring that you’re equipped to endure a cyberattack. But a rushed decision can do more harm than good. So, before you go shopping for a policy, work through this checklist — ideally, with the help of trusted IT professionals — so that you’re positioned to find affordable and suitable coverage for your organization.

#1: Turn on Multi-Factor Authentication (MFA)

MFA is one of the simplest, easiest-to-use, and most cost-effective cybersecurity tools available to SMBs — not to mention a requirement for many cyber insurance carriers. So, before you even think about purchasing a cyber policy, enable MFA for email, accounting software, and remote access tools (at the bare minimum!).

#2: Conduct an Inventory of Personally Identifiable Information (PII) at Your Organization

You can’t protect what you don’t know about, and nothing needs protecting more than the PII that flows through your company. Conducting an inventory of your organization’s PII helps you create a ‘map’ of an area of your attack surface that requires particularly strong cyber defenses, and shows cyber insurance carriers that you’re serious about protecting your digital assets.

#3: Hold Regular Employee Cyber Awareness Training Sessions

Ideally, employee cyber awareness training should be something you already do on a regular basis, as 85% of data breaches involve a human element (*Verizon*) — or more simply, people getting tricked. When your staff is well-trained to spot suspicious activity in your IT environment, your chances of suffering a devastating cyberattack drop considerably. So, hold training sessions on an annual basis at the very least, and depending on the size and nature of your business, as frequently as every quarter.

#4: Start Using a Password Manager

If you don’t already use a password manager to store usernames and passwords at your organization, start doing so ASAP. A password manager is an inexpensive and highly effective cybersecurity tool that can keep your business’s online credentials from falling into the wrong hands.

#5: Update Your Anti-Virus and Anti-Malware Software

This one should go without saying, but a surprising number of businesses are lax when it comes to updates. The threat landscape is constantly evolving, with new viruses emerging every day. Without the latest software, your organization is a sitting duck for crafty hackers with novel viruses at their disposal. If you’re unsure about which software is optimal for your organization, check with your IT provider to ensure that your tools are not only up to date, but the right ones for your business.

#6: Build Better Backup Solutions

Your business should have backups of its data, but not all backups are created equal. How often are you backing up data, and how often are you testing your backups? The appropriate frequency is directly tied to how much time in data loss you can afford to lose: a minute, an hour, a day, etc. And remember, deploying backups in the event of a data breach — who’s responsible and how it is to be done — should be a cornerstone of your cyber incident response plan (*see item #11*). Work with a trusted IT partner to develop a backup strategy and business continuity solutions that will impress carriers and help your company avoid costly downtime.

Continued >

The SMB Owner’s

Cyber Insurance Checklist

#7: Make a List of Third Parties

Your organization does not exist on an island. You’re connected to your customers at the very least, along with any vendors, business associates, and other third parties that you do business with. It’s important, when shopping for cyber insurance, to know who is — and isn’t — going to be covered by a particular policy. Making a list of third parties is the first step in answering this vital question.

#8: Determine Your ‘Must-Haves’

Every business has unique needs when it comes to cyber insurance, because every business has a slightly different attack surface. Maybe you need a policy to cover social engineering attacks, or maybe it’s vital that your coverage extends to remote workstations. Work closely with your IT provider or insurance agent to figure out what you require from a cyber insurance policy, so that later, when it’s time to purchase a policy, you can spell out your needs clearly to carriers. The more detailed your demands are, the more confident you can be about selecting the right policy for your SMB.

#9: Update Your Employee Handbook

Put it in writing. Regularly updating your employee handbook to reflect your latest cybersecurity policies and commitments to data protection will impress cyber insurance carriers, help keep your staff from engaging in risky cyber behaviors, promote compliance with relevant laws and regulations, and may even offer legal protection if you’re faced with litigation stemming from a data breach.

#10: Know Your Potential Losses

Determine how much you could lose per day from IT downtime:

- Revenue lost
- Production lost
- Productivity lost

And remember, downtime often lasts multiple days. Recent studies found the average length of downtime following a ransomware attack to range from 15 to 22 days (*Statista*). Work with your IT staff or IT provider to get a more precise idea of how long it would take your business to recover from a ransomware attack and other common disruptions. When you know how much you stand to lose in the event that your IT infrastructure becomes unavailable, you can budget more intelligently for cybersecurity and cyber insurance.

#11: Create a Cyber Incident Response Plan

When it comes to responding to a cyberattack, time is of the essence. You and your team need to spring into action like firefighters to minimize losses. To that end, create a cyber incident response plan — a clearcut plan of action that identifies who is responsible for what in the event of a breach. Who’s in charge of contacting service providers, insurance agents, clients, etc.? A short document that answers these questions costs hardly anything to create, but it can help save your business thousands of dollars.

THE 20