

EBOOK

How a strong **cybersecurity plan** could save your business



rightworks

Your business probably has a plan for just about everything.

Whether it's marketing, financial planning or revenue generation, you have a roadmap laid out to get you where you want to go. How about cybersecurity? If you don't have a cybersecurity plan, all of your other plans could crumble in an instant.

A cyberattack always seems like some distant, unlikely, worst-case scenario, like damage from a tornado or a broken pipe. The problem is that **cyberattacks aren't unlikely at all. In fact, they happen constantly, as often as 26 times per minute.** Cybercriminals desperately want your data so they can hold it for ransom and then maybe never give it back to you whether you pay or not.



Cybercriminals love to attack smaller businesses

Ransomware and other types of cyberattacks can do some serious damage. **The average cost to resolve a data breach for smaller businesses was \$3.3 million in 2023, up 13% from 2022.**

Overall, cleaning up a breach costs \$165 per record, or effectively \$165 for each client or customer in your database. Extrapolate that cost across all of your entire collection of data, and recovering from a breach gets expensive quickly.

If you think your business is too small to suffer an attack, it isn't. Cybercriminals love to go after small and midsize businesses (SMBs). Research shows that **61% of SMBs suffered a cyberattack in the last year.** Of those, 40% lost customer or client data to cybercriminals. And lightning can strike the same place twice or even more often: 87% of IT decision makers said their businesses had suffered two or more successful cyberattacks in the last 12 months.

Too many small businesses don't have an adequate cybersecurity plan

Scary stuff, right? Every business should have a plan for preventing and responding to cyberattacks. Unfortunately, many small businesses don't, and many that do have either potentially outdated or plainly insufficient plans.

After all, a plan is only as useful as its ability to work. Consider the results of a recent study of cybersecurity plans among SMBs:

- 30% of SMBs do not have a written plan for responding to a cyberattack.
- Of those that do have a plan, 35% haven't tested it in six months or more.
- Three out of four small businesses would only survive for three to seven days after a ransomware attack. Almost half would survive only three days.

Not having a plan is very, very bad. Having one that might or might not work isn't so great, either. But what about businesses that have plans that aren't comprehensive enough to help them actually survive a cyberattack? The same survey reveals that 21% of SMBs do not back up data to protect it from ransomware attacks. And 34% don't train employees to avoid phishing attempts.

Whether those businesses have plans or not is somewhat irrelevant if they're simply not prepared to protect their clients' data—whether they've created a cybersecurity document or not. Take, for instance, accounting firms. They're doing well coming up with plans—as **is required by law.** Only 14% of firms don't have plans.

But the effectiveness of those plans is questionable at best, with 31% of firms failing to effectively back up data and 27% not training employees to spot phishing attacks. The bottom line? While 86% of firms have a cybersecurity plan, only 29% would survive for more than seven days after a ransomware attack.

Why is developing a cybersecurity plan so difficult?

What stops SMBs from being ready for cyberattacks? It's not necessarily laziness or ignorance. The fact is that managing cybersecurity is hard, and most SMBs don't have the resources to do it well—or, in some cases, at all.

In one recent survey, almost 40% of respondents said their business had zero employees dedicated to security as all or part of their job descriptions. Another 42% had only one employee dedicated to security even part-time. Only 6% had increased headcount or a cybersecurity budget in the last year. And what was their top concern regarding cybersecurity? Not data loss or a ransomware attack, but a lack of time to manage security.

Almost 40% of respondents said their business had zero employees dedicated to security as all or part of their job descriptions.

Most small businesses struggle just to keep their heads above water in protecting critical data. Creating, implementing and testing a plan goes far beyond their capabilities. That's true in part because putting a cybersecurity plan in place isn't easy. There are a lot of factors to consider in even a relatively simple plan.

Consider the technology alone you'd need to invest in, implement and maintain as part of a basic template security plan:

- Antivirus software
- Strong firewalls
- Encryption
- Backups
- Software update cycles
- Software swaps (replacing outdated applications with new versions)
- Wi-fi network security
- Password management
- Multifactor authentication
- Protection for Internet of Things (IoT) devices

How much do you and your employees know about those technologies? How much time do you have to implement and manage them? That's just the technology list—one component of a multi-pronged plan that also includes determining which employees have access to which sets of data, identifying and fixing technical vulnerabilities, teaching employees to avoid cyberthreats, and testing to see how well your employees are complying with your security plan.

Oh, and you'll need to test, review and revise the plan at least every six months. That's just the work involved with developing and maintaining the plan itself. Making sure you actually carry out the plan every day is a completely different, massively time-consuming task altogether. Security threats change constantly. Your plan for prevention and response needs to change with them.

Smart SMBs trust security partners to keep them safe

You're going to need help. Small businesses are increasingly turning to security partners for assistance in setting up and implementing security plans, and making sure the plans actually work. In fact, small business owners trust their security partners more than anyone else to provide cybersecurity guidance.

SMB owners, probably wisely, said in a recent survey that they have more **confidence in security partners** than in colleagues, analysts or peers within other organizations. Many seemed to be relatively recent converts to partnering for security, with almost 70% of respondents saying they were more likely to ask a cybersecurity partner about new security applications than they were a year ago. The threat and pace of cyberattacks has brought many SMBs into the security-outsourcing fold.



With owners tied up trying to run their own businesses and lacking expertise in cybersecurity, bringing in an outside expert to protect data just makes sense. It's not enough, though, to simply reach out to a partner that can tackle one or two specific security issues. Businesses need a partner that offers holistic cybersecurity protection, including threat prevention, attack neutralization, backup and iron-clad data storage.

What small businesses need is a security partner that runs a managed service in the cloud. That's a **direct recommendation** from the Cybersecurity and Infrastructure Security Agency, the US government's cybersecurity arm:

"One major improvement you can make is to eliminate all services that are hosted in your offices," the agency says on its website. "We call these services 'on premises' or 'on-prem' services...These systems require a great deal of skill to secure. They also require time to patch, to monitor, and to respond to potential security events. Few small businesses have the time and expertise to keep them secure...We urge all businesses with on-prem systems to migrate to secure cloud-based alternatives as soon as possible."

Businesses need a partner that offers holistic cybersecurity protection, including threat prevention, attack neutralization, backup and iron-clad data storage.

A managed security service can actually be your cybersecurity plan

However, there is a lot more to managing security than just moving away from on-premises servers, although that's an important step. Total security management involves partnering with a provider that offers comprehensive data protection. There's a lot more involved there than just storing information in data centers.

A security partner with comprehensive capabilities will store information in data centers of the highest tier available, but it will also do a lot more than that. The right partner will update servers and applications, offer advanced technologies such as multifactor authentication, deliver a secure online platform for communicating with clients and customers, and provide advanced protection for email systems.

But your cybersecurity partner should also provide protection for the devices you use every day (sometimes called "endpoints"), such as laptops. It should offer rapid data backup and recovery and minimize system downtime to the point where you'll never notice it at all. Your partner should be able to do all of this in the cloud so that you minimize installation of security applications at your own site. And you should be able to benefit from all of this for a manageable monthly fee.

A security partner with comprehensive capabilities will store information in data centers of the highest tier available, but it will also do a lot more than that.

In short, your security partner should be able to not only guide you in developing a comprehensive security plan but to carry that plan out successfully every day with little to no effort on your part. You won't need to test a plan every six months when you have a partner executing it for you every day. Turning security over to experts effectively becomes your plan.

Don't forget about the human element of security, either. Look for a provider that offers cybersecurity training to employees so they can know how to avoid cyberthreats. In fact, the Verizon Data Breach Information Report, probably the most comprehensive cybersecurity report published, says **employee training should be the top priority** in an SMB security plan, even above establishing data recovery. Your employees are your last and best line of defense against attacks, and there is nothing more important to protecting your data than training and testing them.

Another of the top three protections the Verizon report mentions is determining which employees have access to which sets of data. In some businesses, especially the smallest ones, that might not be an issue. But in operations that deal with money, such as accounting firms or financial consultancies, letting employees only see what they need to see is critical. A partner that offers managed security can help with that part of your security plan, too.

Get your security plan right with Rightworks

Rightworks can develop and carry out your security plan in the cloud, with cloud-based **managed security services** that can keep your business-critical data safe on all workstations. **Managed security** provides the protection your business needs at a fixed monthly cost that can scale as your business grows. You can trust Rightworks to:

- **Understand your cybersecurity needs** and develop a comprehensive plan with you.
- **Update technology** without having any impact on your daily business activity.
- **Back up and protect your data** in top-tier data centers for maximum availability.
- **Implement and maintain essential security technologies** so you don't have to.
- **Train and test employees** so they know how to avoid cybersecurity risks.
- **Help determine and enforce data access** among your employees.
- **Protect your data in enterprise-class facilities** and provide US-based, 24/7/365 support.

Most businesses don't have time to manage security, and there's really no reason for them to try. Rightworks can be your security partner from the planning stage through to keeping your data protected every day—while you focus on running your business.

Want to learn more?

Contact us today at **888.210.0237**

 **rightworks**
rightworks.com