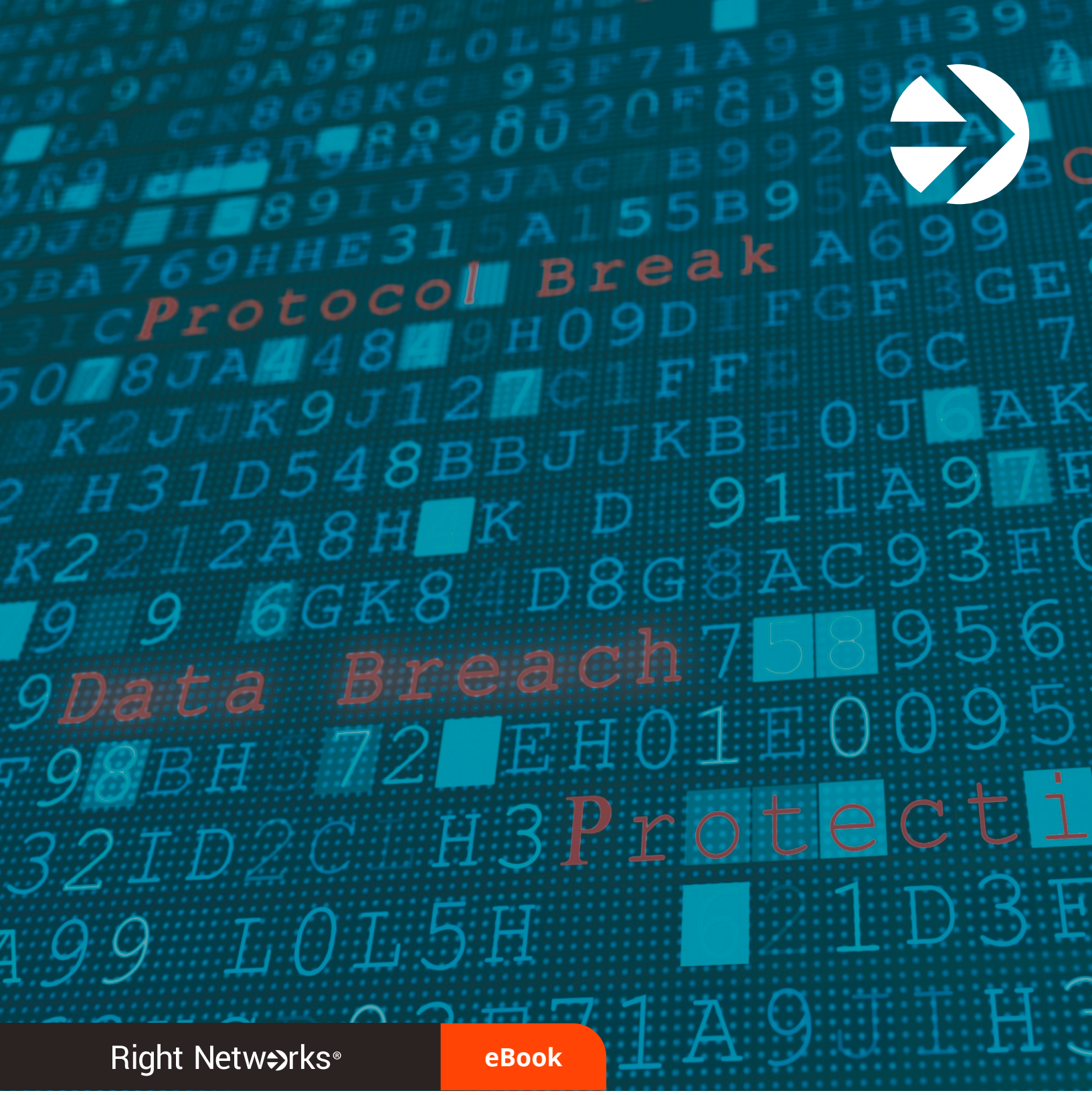
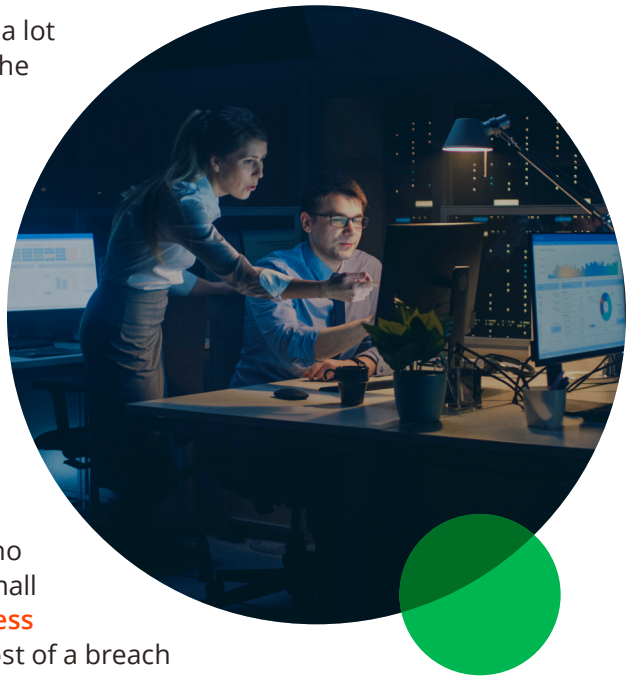


Right Networks®

eBook

5 things you can do right now to **prevent data breaches**

Introduction

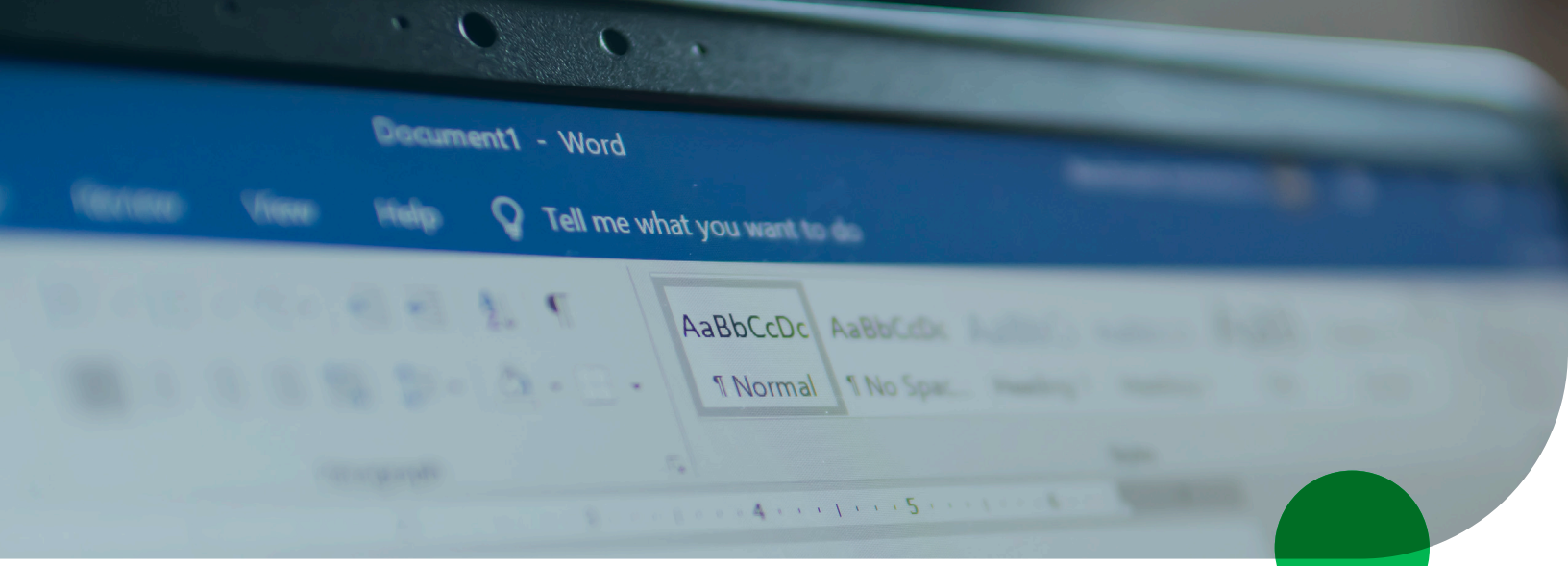


Managing security is difficult—so difficult, in fact, that a lot of accounting firms don't bother to do it adequately. The same goes for most small businesses. One survey indicates that only 8% of businesses with fewer than 50 employees have a dedicated security budget, while almost half have no security budget at all.

Why? More than three-quarters of survey respondents cited the complexity of cybersecurity as a reason for not making improvements in that area. The bottom line is respondents just don't know enough about cybersecurity to manage it, and they can't afford to hire experienced people who can.

That leaves small businesses, firms included, at risk of data breaches that can prove devastating. And make no mistake, a breach can wreck your firm. Fully 60% of small and medium-sized businesses (SMBs) go out of business within six months after a cyberattack. The average cost of a breach for an SMB is $3.6 million, according to cyber security group Cimcor.

Security, then, is quite simply an issue accounting firms must take seriously. Yet, while most firm owners are aware of how important it is to prevent data breaches, many still fail to address security properly. There are a few things your firm can do right now, starting today, to make your operation more secure. Some are relatively simple. Others aren't—cybersecurity, after all, is ever-changing. Ultimately, the best idea might be to have someone else altogether handle security for you.



How you can work with cybersecurity partners to prevent cyberattacks

This list starts with the simplest step your firm can take to up its cybersecurity game and increases in difficulty—until the end.

1. Write a formal security plan.

Your firms should already have one of these since they're required by law for any organization that processes tax returns. So, if you don't have a written plan, you need one. But there are more reasons than just compliance to put a security strategy in writing.

Firms don't always know their data has been breached until it's too late and a cyberattacker is demanding a ransom or menacing the firm in some other way. Then the reaction tends to be panic, and panic often leads to bad decisions.

With a security plan, your firm will have written instructions to follow in case of a security incident. You'll have documentation on how you're securing your firm so that you can cover yourself in the event of client concerns or an IRS investigation. You'll also be able to pass your security strategy on to new employees or partners if your security personnel changes.

Don't worry. You don't have to produce a document on your own. Templates exist for creating written security plans. It's not a bad idea, of course, to get a security expert or partner, or maybe a lawyer, involved in the process of developing your plan. In any case, having a plan is essential—and required.

2. Enforce use of strong passwords and multifactor authentication.

Passwords are ripe for theft. Stolen credentials—in other words, hijacked usernames and passwords—are at the core of more than half of cyberattacks on businesses with 10 or fewer employees and about half of attacks on businesses in general, according to the 2022 Verizon Data Breach Investigations Report (DBIR).

Of course, using strong, complex passwords and not repeating passwords from one application to another are basic concepts of good security practice. Passwords should be complex, with each containing at least 14 characters. When it's time to change a password, simply adding a number to the previous password is dangerous. And using the same password in more than one place just opens more apps to potential attacks.

Employees need to know and respect password best practices, but password discipline alone isn't enough to ensure data security. Firms should also use a password manager, which gives users the convenience of storing passwords in a single place—helping eliminate the inevitable frustration of the forgotten password—and provides password security.

Perhaps most importantly, though, firms need to adopt multifactor authentication (MFA). Yes, that's the system that requires users to sign in on some device other than the one they're using to access data. (For instance, a user signing into QuickBooks® on a computer will also need to verify the sign-in on a phone with the MFA application running on it, or even on a landline that delivers an audio code.)

One extra step can make a massive difference in preventing data breaches. MFA can **prevent 90% of cyberattacks**, including, according to Microsoft, **99.9% of automated attacks**. MFA is experiencing massive uptake around the world, so if your firm hasn't adopted it, you're falling behind—and your data is at risk.

3. Train employees to practice cybersecurity for accounting firms.

This is where things start to get more difficult. All the technology you can implement is only as effective as the people who use it. If an employee bites on a phishing email, that one click could be catastrophic and open your data to theft via a cyberattack. Training employees goes far beyond teaching them how to create passwords.

Employee actions are massive factors in data breaches. The DBIR notes that 82% of breaches involve the "human element": an employee clicking on a malicious link, downloading malware or otherwise unwittingly opening the door to your firm's data. People make mistakes, but the more they're aware of the potential consequences of their carelessness, the more careful they're likely to be.

This element of bolstering security is critical for firms but difficult for them to handle in-house. Your firm probably doesn't have a security expert who can develop a security curriculum for employees. This is one area where a cybersecurity partner comes in especially handy. There are, of course, several large vendors that provide security training. However, quality varies, as does the level of maintenance and interaction the firm itself has to maintain. Your firm needs a set of courses that will be relevant to your employees.

Finding training designed for accountants and accounting firms, then, is a smart move for firms that want to keep their people engaged in security training. For instance, your employees need to know how to identify a breach and what to do if they spot one. If the firm has processed 100 tax returns but there are 130 in the system, it's likely that a breach has occurred and a cyberattacker is stealing data. Catching breaches quickly is essential to mitigating damage, and employees need to be active on the front lines of protecting your firm's data.

4. Update everything all the time.

This is where things get a little scary. Cybersecurity never stops changing because attacks never stop, period. And the tactics cyberattackers use change constantly as well. Big companies such as Microsoft and Google issue security patches based on known vulnerabilities—security weaknesses they've found and need to correct. Firms that don't immediately patch their systems leave themselves open to attack.

What's worse is that tomorrow's attack might be nothing like today's, so a critical patch can come at any time. Most attacks on endpoint devices, such as individual computers, are "zero-day" attacks, meaning they're basically impossible to see coming. Firms are vulnerable to such attacks until they can apply the patches that prevent them. If you're not applying patches regularly, you're constantly vulnerable to multiple types of attacks.

So, what do you need to update, exactly? Everything. What does that mean? Well, Windows for one, as well as any accounting software you might use, such as QuickBooks. Think about all the software applications your firm uses. They all need regular updates. If that sounds simple, it's not. A patch can be released at any time. Does your firm have somebody committed to patching software? If not, you're at risk.

And if so...it's still not enough because a lot of other technologies need constant patching. Think about everything you use every day in both your office and your home office—and in any location from which your employees work. Servers, browsers, antivirus software, printers, scanners, firewalls, routers, individual computers—they all need constant updating. And you need to make sure that the patches you're implementing work and won't cause havoc with any of your other technologies.

It's a big deal—basically, a full-time job. And it's essential. If all of this sounds overwhelming, that's because it is. But it doesn't have to be.

5. Find a trusted cybersecurity partner.

The fifth security step in this list isn't so much a tip as it is a way to address many of the other security imperatives listed in this document. Your job is to run your firm—to serve clients, attract and maintain employees, drive revenue and manage your business efficiently. That leaves little time for dealing with cybersecurity. And unless you can find—and pay—a cybersecurity expert to work for you full time, your firm will be at risk.

So what's the solution? Outsource security. Let experts handle it for you. Find a trusted partner that offers the products and services you need to keep your firm's data safe. Trying to manage security in-house without expertise is a little like having a legal department with no lawyers. It's not going to work. But outsourcing does work.

For what is often a fixed amount of money that's easy to budget, your firm can have comprehensive security protection—and you can focus on running your firm's business. You'll enjoy the same level of security big banks have without having to deal with any of it yourself. And that includes more than just technology.

A trusted provider can help you develop a security strategy and can train your employees to be good stewards of your data. It can also implement MFA and manage updates—along with other essential tasks that would be extremely difficult to deal with in-house.

This is Smart Security Management from Right Networks

Consider Smart Security Management (SSM) from Right Networks, a provider with more than two decades of experience:

- Secure Cloud offers secure and reliable cloud hosting that safeguards your data with end-to-end redundancy across all systems, real-time data replication and enterprise-class multi-layer security systems—24/7/365.
- Secure Workstation is a comprehensive, secure endpoint solution to safeguard your business-critical data. You can have peace of mind with added security for all your employees with one enterprise-level solution.
- Security Awareness Training offers an employee education program that provides best practices for staying safe online using an expert-developed gamified training program.

With SSM, Right Networks offers technology, expertise and training from a single organization that has been at the forefront of securing accounting firms for more than two decades. And if you want to go beyond security, you can outsource many other elements of your firm's IT operation with Right Networks Cloud Premier.

Prevent data breaches today with a cybersecurity partner

Security can't wait. If your firm hasn't taken any of the steps outlined in this document to protect your data, you need to start taking them now. Some you can begin in-house: writing a security document, for instance, or requiring employees to practice good password discipline.

Other tasks are more complex and require more time, as well as a greater allocation of resources. You shouldn't have to take them on yourself for the long term. Updating patches now, for instance, is a necessity, but it's not something you'll likely be able to do in-house for months and years on end.

Finding a trusted partner, such as Right Networks, can relieve you of your firm's security burden while also enabling you to protect your firm's data and minimize damage from cyberattacks. The time to act on security is, as always, right now.