



6 things you can do to **protect your clients' data**



Cyberattacks never stop. It's very likely that right now, a cyberattacker is trying to steal your clients' data. If the attack succeeds, it can put your whole operation in peril. That's why cybersecurity is so difficult to manage, and also so important. It's a constant battle—one you can't afford to lose.

Cyberattacks can take a number of forms and originate from a variety of devices. **One of the most common data breaches is a ransomware attack**, in which cyberattackers steal your data and literally hold it for ransom.

Other attacks slow the response time of your website or attempt to steal your employees' usernames and passwords. **New threats involving texting and artificial intelligence (AI)** are also emerging and evolving.

A few numbers illuminate why cybersecurity is both so critical and so worrisome to deal with:

- Attacks occur at a pace of more than **11 per minute**. The pace of attacks is increasing.
- The median ransom payment was **more than \$190,000 in Q2 2023**, up 20% from Q1. That number includes even the smallest businesses. Could your firm take that kind of hit?
- About 30% of ransomware attacks **target small businesses**. Being small doesn't make you safe.
- Cyber insurance premiums **rose by 20%** in 2022, so even those companies that haven't been hit by ransomware yet are still paying for it.

How you can protect your organization from cyberattacks

Despite the persistent threat of cyberattacks, you don't have to be a victim of a data breach. There are six essential measures you can take to protect your clients' data. They're not necessarily simple, however, so finding a partner to implement and manage them for you is essential.

1. Update your software and devices. The pace of change in cybersecurity is extremely fast. Zero-day vulnerabilities offer vectors for cyberattacks to strike very quickly. In an attack on a zero-day vulnerability, cybercriminals find a way to get around security weaknesses in applications that developers haven't yet had a chance to fix.

Software developers can only combat zero-day attacks with application updates, which means **it's essential that you update your apps as quickly and thoroughly as possible**. That's not necessarily a simple task. Updates can come in bunches and without warning.

For example, in late summer 2022, Microsoft released 64 fixes for zero-day vulnerabilities, one of which attackers were actively exploiting. In just one week last year, Google released six updates targeting zero-day vulnerabilities. Failing to install those updates leaves your network wide open for data theft.

That's why automatic updates for software in computers and mobile devices are so essential. Attackers know which patches developers are releasing and exploit those vulnerabilities even after patches are available, knowing that many organizations don't update software automatically. You can't afford to let your firm fall behind.

2. Enforce modern password policies. No, "password!" and "password123!" are not strong passwords. Hopefully, most of your employees know that by now. But there's more to a wise password policy than just requiring employees to add a number of special characters to their credentials. Yes, passwords should be long and complex—and perhaps better expressed as passphrases with numbers and characters worked in.

But one of the most common habits is also one of the worst: using the same password across multiple accounts. Each application or account should have its own password. Why? If a cyberattacker manages to steal the credentials of one of your employees, and the employee uses the same password across accounts, the attacker gains access to all the accounts that use that password. If passwords are different from one account to another, the attacker only has access to one account.

Of course, attackers shouldn't have access to any accounts at all, but it's also true that passwords are a hassle many users would rather not deal

with. In fact, it's safest to sign into an application every time you use it, rather than saving a password in each individual app as many users do. That's why password managers or wallets are so useful. They store all your individual passwords in one place and let you access all your accounts securely with one master password.

3. Adopt multifactor authentication. In addition to a password manager or wallet, multifactor authentication (MFA) is essential to maintaining a modern password policy. With MFA, a second "factor," usually another device, is required for sign-in to an account. So, if you enter your username and password into, say, a laptop, you'll have to confirm your identity on another device, often a mobile phone.



With MFA, you have a layer of protection that a password alone doesn't provide. If an attacker does manage to steal your password, your account still won't be accessible because the attacker would also need to confirm identity on another device. Unless the attacker has your cell phone, for example, confirming on the second factor is impossible. Your data remains safe even if your password is compromised.

Remember, also, to terminate a user's login credentials immediately after the person leaves the company. **Old credentials provide an easy attack vector**, particularly for employees who did not leave on good terms. A departed employee with active credentials and an MFA-enabled device renders the protection MFA provides ineffective, so dealing with employee exits quickly is essential.

4. Allow only trusted users to connect to IT resources. By now, many or all of your employees may work from home. However, you don't know what kind of security setup they have in their homes—if any. That's why it's important for them to connect to your network through a virtual private network, or VPN. A properly configured VPN, professionally installed and maintained, gives you control of remote security settings.

The same goes for employees who work remotely from a coffee shop, hotel or even a client's office. **Connecting via a VPN is essential.** It's also essential to train your employees to connect through the VPN at all times when they're not in the office. Employees bypassing the VPN or simply forgetting to use it leave your data exposed.

At the outset of COVID shutdowns, many businesses began using **Windows Remote Desktop Services (RDS)** or **Remote Desktop Protocol (RPD)** to allow users to connect remotely. Unfortunately, cyberattackers jumped all over those services and turned them into major vectors for attacks. You need to disable both RDS and RPD and make sure your employees connect through a VPN instead.

Along those same lines, you need to make sure mobile devices such as cell phones and tablets are safe to use. The best way to do that is to implement **mobile device management (MDM)** or **endpoint detection response (EDR)**. Those technologies ensure that each mobile device is authenticated by your firm for use and that devices run the latest and most secure versions of software and operating systems.

5. Train employees to avoid risky behavior. Your employees are your last and best line of defense against a cyberattack. Most attacks cannot succeed without someone letting them happen. Nearly three-quarters of all data breaches **include a human element**, such as an employee clicking on a malicious link in an email or responding to a rogue text.

That's why training your employees to recognize and avoid potential cyberattacks is so important. Cyberattackers are constantly **developing new ways to steal data**, some of which start with a simple text or even a voice mail. It's nearly impossible for employees to do their jobs and keep up with cybersecurity trends on their own. They need help.

With the advent of AI, ransomware emails are no longer clunky and awkwardly worded. Many look legitimate and fully professional. Your employees should never open an email unless they've verified directly with the sender via a method other than email that the message is legitimate. They should absolutely never click on a link within an unexpected email. The same goes for text messages, voice mails and even videos. Employees need to connect with the sender via another method to ensure legitimacy.

Your best option for safe communications is to use a managed cloud service that protects your email client and prevents malicious emails from ever hitting your inbox.

Aside from educating employees, which is necessary no matter what, your best option for safe communications is to use a managed cloud service that protects your email client and prevents malicious emails from ever hitting your inbox. Also, a cloud provider can deliver a secure online environment where you can communicate with clients without using email, text or voice mail at all.

6. Verify that you're backing up your data effectively. Even when you're doing all you can to prevent data loss, you need to make sure your data will still be available in a worst-case scenario. As such, you need to completely back up your data on a regular basis and ensure that your information is always quickly recoverable.

If you're trying to do this on your own, it can be a challenge. You need to make hourly shadow copies of your data that capture any changes to information that have taken place within the previous hour. You need to perform daily full-system backups, with backed-up information stored offsite in case of damage to your servers.

And you need to make sure that your backups are comprehensive and accurate. Have a qualified person review your backup logs and identify errors, which can be difficult to spot. Randomly restore files from time to time in order to ensure that your system is working. Just trusting data backup isn't enough. You have to verify that it's working.



Why you should let experts manage cybersecurity

If all of that sounds like a lot of work, it is. Protecting your firm is a full-time job. It's unlikely that you want to be in the cybersecurity business. The best way to secure your operation is to work with a partner that handles security full-time.

Cybersecurity is so risky and changes so quickly that it's almost impossible for non-experts to manage it. The expertise, technology and equipment required to properly handle security are prohibitively expensive for most companies to acquire. And then there's the work of keeping your firm secure, which is complex and can be all-encompassing.

What managed security services from Rightworks can do for your firm

Rightworks provides **managed security services** that can keep your business-critical data safe on all workstations. Managed security provides the protection your firm needs at a fixed monthly cost that can scale as your business grows. You can trust Rightworks to:

- Update applications without having any impact on your daily business activity.
- Implement and maintain essential technologies such as MFA, a VPN and MDM/EDR.
- Provide a secure email service that protects your inbox from malicious messages.
- Train employees to avoid cybersecurity risks.
- Back up and protect your data offsite for maximum availability.
- Protect your data in enterprise-class facilities and provide US-based, 24/7/365 support.

Cyberattacks never stop—and cybersecurity can't, either. With Rightworks providing managed security, you can minimize the amount of work you need to do to protect your critical information and rest assured that your data is safe and available.

Talk to our sales team today at **866.931.6254**

 **rightworks**

rightworks.com