

EBOOK

Fact or fiction? 10 cybersecurity myths debunked



 **rightworks**

Fact or fiction?

10 cybersecurity myths debunked

Guesswork is dangerous in cybersecurity. Certainty is essential. Cyberattacks present a constant threat to accounting firms and small businesses. Are you doing all you can to protect your organization's data? You might not be if you're laboring under cybersecurity myths.

There are plenty of scary numbers around cyberattacks. The bottom line is that cyberthreats are constant and picking up pace. One study found that **almost 13% of all emails** are malicious. Another found that would-be cybercriminals launch **11 attacks per minute**. Attacks come in **all sort of forms**: fake executive emails, consumer surveys and apparently legitimate URLs that aren't.

And those are just email-based threats. New technologies have led to **new vectors for attacks**, some of them as seemingly innocuous as a voicemail or text message. And the cost of a breach is heavy. In its survey, IBM revealed **data breaches cost the smallest businesses** an average of \$3.31 million in 2023—up 13.4% over 2022. Across all businesses, the average cost was \$165 per record.



Separating cybersecurity myths from reality:

10 facts you need to know

With so much at risk, how can you be certain you're protecting your firm or business from a cyberattack? Consider 10 facts that debunk some common cybersecurity myths.

Myth: You're running applications in a software as a service (SaaS) model, so you have all the backup you need.

Fact: As handy and popular as SaaS apps are, most SaaS providers don't back up your data in any significant way—if at all. In fact, one study from IT network TechTarget comes to a very simple conclusion: It's easy to lose SaaS data. How? The study explains:

"Among the most common reasons: SaaS provider outage or unavailability, malicious deletion from cyberattack, accidental deletion, account closure, insufficient or deficient backup mechanism, current backup vendor not supporting the specific SaaS application(s), misunderstanding of retention/deletion policies, malicious deletion by employee, and schemas misconfiguration or bad schema update."

Unlike a SaaS provider, a third-party cloud partner can protect your critical information from all of those potential data-loss scenarios with managed security services. The right partner will store your data in enterprise-level data centers monitored by experts 24/7/365. Cloud-based managed security services will also back up your data and update your applications automatically while you focus on running your firm or business.

Myth: Protecting your core applications is enough. You don't need to protect devices, too.

Fact: Endpoints are the devices, such as company laptops, that you use to access your data and applications. They're also major vectors for cyberattacks. Network and application protection are critical, but you can't ignore the vulnerability of the devices you use every day. That's especially true in an environment in which many employees work from different locations and use multiple devices.

When you secure your devices, you build on the concept of defense-in-depth, or protecting your data with multiple layers of security. Defense-in-depth is a best practice among security professionals and experts. Simply put, while network security can protect your data in case of a cyberattack, device security can prevent an attack from hitting your network in the first place. You have a critical double layer of protection.

3.

Myth: Your email provider protects you from spam. That's all you need.

Fact: Email is still far and away the most common vector for cyberattacks; 80% of cybersecurity threats start with an email. And the rate of email-based attacks is on the rise. From Q2 2022 to Q2 2023, credential-stealing phishing attacks rose 85%. Business email compromise attacks are an increasing threat—with attackers spoofing CEOs, service providers, attorneys and other close contacts in an effort to steal data.

So, email is a minefield, and your email provider's spam protection doesn't come close to providing adequate protection. More than 1 in 10 emails are malicious, and it only takes clicking one malicious link to cause a data breach—an expensive catastrophe for your firm or business. You need a third-party security provider that goes far beyond offering spam protection.

The right managed security partner will offer secure email services that do more than just filter out malicious emails. Cloud-based services can stop malware from doing damage to your organization before it starts. In the cloud, you also have access to a secure online environment where you can collaborate with customers or clients in real time without using email at all.

Another critical capability standard email protection lacks is the ability to restore access to your account if you lose it. A managed security provider can give you your account back if an attacker robs you of access or you lose the ability to log into your email for any other reason. In the cloud, you can be confident that you won't be locked out of your email account.

4.

Myth: Yearly security training is enough for your employees.

Fact: Nearly 75% of all data breaches involve someone in the victim's organization taking action to make the breach successful. That can involve an employee accidentally clicking on a malicious link in an email, opening a toxic attachment or even responding to what looks like an innocuous text message. Most data breaches aren't possible without someone in the targeted organization launching them.

Your employees are your first and best line of defense against data breaches. Cyberattacks and cybersecurity change constantly. The nature of attacks changes rapidly as cyberthieves embrace new technologies and develop new tactics. And the number of attacks only continues to increase. Your employees need regular training—at least quarterly—from experts on how to detect and avoid cyberattacks. Anything less leaves you wide open for data theft.



5.

Myth: You don't use artificial intelligence (AI) apps like ChatGPT so there's nothing AI can do to hurt your business.

Fact: If you do use AI, you need to be careful not to divulge confidential data. Even if you don't, you still need to be careful—because cyberattackers are using AI to try and steal your data. In fact, AI is helping cyberthieves big time. They're using it to write malicious code they can incorporate into malware, for example.

But perhaps most strikingly, cybercriminals are using AI to develop phishing emails that look more real and credible than ever before. Gone are the days when phishing emails looked almost immediately suspicious—replete with grammatical errors and other obvious mistakes. Modern phishing emails are almost impossible to distinguish from legitimate emails thanks to ChatGPT's content-creation capabilities.

Your firm or business needs to double down on cybersecurity in the era of the AI-aided cyberattacks. Protecting both your network and your endpoints is critical, as is training employees to recognize and avoid malicious messages. This is a challenge that will only become more difficult to manage.

6.

Myth: Antivirus is pretty much all you need to protect your devices.

Fact: Antivirus is important, but its supposed infallibility is one of the most common cybersecurity myths. Most notably, antivirus can do little to stop attacks on

zero-day vulnerabilities, which is when cybercriminals find a way to get around security weaknesses in applications that developers have not had a chance to fix. Essentially, when a zero-day vulnerability exists, attackers exploit it before software developers can fix it. That includes antivirus software.

That means antivirus is fairly useless against most zero-day attacks. Endpoint detection and response (EDR) is a technology that combines both AI and human expertise to identify and thwart zero-day attacks before they can do any harm to your organization. Again, protecting endpoints proves to be critical, as stopping a zero-day attack at the endpoint can prevent it from ever reaching your network. The right managed security partner will offer EDR-based endpoint protection.



7

Myth: Your business is too small to need an outside security partner.

Fact: Don't be fooled by one of the most dangerous cybersecurity myths. The fact is that small businesses are under attack. About 30% of ransomware attacks target small businesses. In one recent survey, 62% of smaller businesses reported experiencing a ransomware attack in the last year, and 36% of those businesses ended up paying the ransom to get their data back. Accounting firms in particular are targets for cyberattacks because they deal with their clients' most critical and confidential information.

Many cyberattacks target small businesses because smaller organizations often don't see the value in investing in cybersecurity. But the fact is that security is paramount for companies of all sizes. The right partner can protect your organization with enterprise-level security for an affordable, fixed monthly fee that easily fits into your budget.

The cost of a data breach could destroy your business altogether. The cost of managing your own security in time and risk alone is high. With experts running a fully managed security service for you, all you have to do is focus on running your firm or business. Trusting a partner ultimately saves you both time and money—and lets you sleep at night.



8

Myth: Your data is more secure in your office than it would be in the cloud.

Fact: This is a dangerous myth on many levels. When you run your own server, you're in charge of application updates, server maintenance, data backup and cybersecurity. Unless you have a highly skilled and dedicated IT staff, there is no way you can build an infrastructure in your office that compares to what a cloud-based managed security partner can provide.

A managed security vendor will update your applications, perform server maintenance, back up your data and secure your network while you go about your business. The right vendor will store your data in enterprise-level data centers (Tier 3 and 4—the highest tiers) and offer support 24/7/365. You'll also enjoy 99.999% uptime, meaning your data and applications will virtually always be available. No small or even midsize firm or business can match that level of service.

9

Myth: You have basic security measures in place, so you don't need cyber insurance.

Fact: Cyber insurance is essential to organizations of all sizes. Unfortunately, it's not necessarily cheap, and it's getting more expensive. Premiums rose by 20% in 2022. But operating without cyber insurance is like failing to insure your car or home. The cost of suffering a data breach would be catastrophic.

Fortunately, a cloud partner can help with the challenge of finding and paying for cyber insurance. The right preventative cybersecurity and comprehensive cyber insurance coverage go together. Underwriters might require you to have certain solutions in place to get coverage. Your managed security provider can provide those services for you. Plus, your organization might pay lower premiums with comprehensive managed security services in place.

Beyond all that, even the most reliable filing system is inefficient if not everybody in your organization knows how to use it. You need a system that's simple and universal and provides secure and consistent access to files for everybody in your organization who needs it. Your business or firm needs document management. With document management running in the cloud, you can be sure that the people who need access to critical files have it—and those who don't, don't.

You can set up access so that employees only see the information that's relevant to their jobs. You can also create workflows so that staffers know exactly what to do and how to do it when taking on a task. With document management in place, running in a secure cloud environment, you can eliminate confusion, increase efficiency and even make employees' jobs easier to do—all while protecting your data.

10

Myth: I can keep everything I need in file cabinets and on devices.

Fact: Storing critical files on paper is not only inefficient, it's insecure. Paper files, after all, aren't recoverable. But even if you moved on from paper a long time ago, not all electronic storage is the same. Keeping files on devices is dangerous. Theft is a real possibility, but perhaps a greater threat is a fire or disaster that destroys your office or even home computers. The same goes for storing data on an in-office server.



Rightworks delivers the cloud-based cybersecurity you need

You need to be sure that you're getting cybersecurity right. With Rightworks, you can. Rightworks provides managed security services that can keep your business-critical data safe on all workstations. Managed security provides the protection your business needs 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 multi-factor authentication (MFA), a VPN, mobile device management (MDM) and endpoint detection and response(EDR).**
- **Provide a secure email service that protects your inbox from malicious messages.**
- **Train employees to identify and avoid cyberscams.**
- **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.**

The underlying fact about cybersecurity is that half-measures aren't enough to protect your data. You need to know that you're doing absolutely everything you can to keep your information safe. The best way to do that is to trust security professionals. Rightworks has the expertise, the team and the technology you need to take your cybersecurity operation to where it needs to be.

Want to learn more?

Contact us today at **888.210.0237**

 **rightworks**

rightworks.com