

EBOOK

3 major security threats to small businesses



 **rightworks**

Introduction

Small businesses just can't get any relief. COVID repercussions caused problems for businesses of all kinds. And accounting firms and their clients struggled to keep up with Paycheck Protection Program regulations and other pandemic-related programs.

As if that weren't enough, the trend toward working at home hasn't eased security concerns; if anything, it's made them more pressing. No less an authority than INTERPOL—the intergovernmental organization that fights crime in 194 countries—noted in the summer of 2020 that **COVID had led to a spike in cybercrime.**

It's a spike small businesses might not be as prepared to handle as well as they think they are. A 2020 report from BullGuard revealed that one-third of companies with 50 employees or fewer rely only on free—mostly inadequate—cybersecurity applications intended for consumers and that **43% of SMB owners have no cybersecurity defense plan in place.** Perhaps more worrisome, 60% of respondents to BullGuard's survey said they didn't think their businesses were likely to be targets for cybercriminals.



60% of SMB owners think their business is unlikely to be targeted by cybercriminals.

43% of SMB owners have no defense plan in place.

One-third of SMB owners rely on free cybersecurity apps.

Small businesses are frequent victims of cyberattacks

That's a dangerous assumption to make. Verizon's 2020 Data Breach Investigations Report revealed that **small businesses were victims** in more than 1 in 4 reported security breaches—a frighteningly large number, considering that the generally low-profile nature of most small businesses would seem to make them less obvious targets than bigger companies.

Each breach costs small businesses \$2.98 million. One-fourth of SMBs reported security breaches in 2020.

Not surprisingly, the cost of data breaches to small businesses is devastating. On average, according to a 2021 Cost of a Data Breach report from IBM Security and the Ponemon Institute, **each breach costs a small business \$2.98 million**. Very few small businesses can absorb that kind of financial blow. That's why handling security in-house is so risky for firms and small businesses.

Security is not only critical—it's complex. Small businesses and firms face a series of different threats, each requiring a particular method for either eliminating risk or mitigating damage. Gearing up to take care of all those threats in-house can be prohibitively complex and expensive—and there's no room for error. This eBook looks at the most common and dangerous security threats to small businesses and delves into how the cloud helps firms and small businesses deal with them effectively.

The 3 biggest security threats to small businesses (and how the cloud helps businesses deal with them)

The biggest security threats to small businesses break down into three overlapping categories: **phishing, malware and internal threats**. All three can—and often do—work together, but this eBook specifically breaks down phishing as an attack to steal user data. It's important to understand that cybercriminals can also use phishing attacks to install malware and that internal security threats can take all kinds of forms.



Phishing



Malware



Internal threats

Phishing and spear phishing

for data theft

Most owners of small businesses—in fact, most people who use computers, period—should be familiar with phishing by now. Often performed with, but not limited to, a rogue email, **phishing attacks** trick a user into entering private information into a fake website, an editable PDF or some other form that accepts data entry. Attackers steal the information entered, including passwords and other account credentials, as well as financial information, like credit card or bank account details. With that information, attackers can clean out a bank account, make fraudulent charges on a card, or even infiltrate a company's entire network...and all of its critical data.

Phishing can go *beyond* email to social networks or text messages and can come in different forms. Spear phishing, for instance, targets one person or company very specifically and appears to come from a trusted contact. And phishing happens all the time. According to the Verizon Data Breach Investigations Report, it's the method most employed for attacking small businesses, used in more than 30% of all attacks in the report's period.

Cybercriminals are becoming increasingly more adept at making their attacks look like legitimate communication.



Phishing accounts for more than **30%** of all SMB attacks.

Phishing is dangerous because it's not only common but also because many attacks look credible—and cybercriminals are becoming increasingly more adept at making their attacks look like legitimate communication. Plus, major news events such as COVID generally lead to a rise in phishing schemes, with emails that promise (fake) news updates or (also fake) critical information from official authorities.

The cloud helps prevent phishing attacks by employing technologies that recognize phishing attacks and isolate them before they ever reach employees. By using **email security gateways and post-delivery protection**, cloud providers can stop phishing attacks before they start. And, as is the case with any technology, a cloud provider will be better able to update security applications and successfully deploy them than a small business will be able to do in-house.

Malware and ransomware attacks

Cybercriminals use ransomware to steal a company's data and essentially hold it hostage.

Some phishing attacks do more than just entice users to enter information attackers can steal. They install malware on a user's computer that attackers can use to infiltrate a company's entire network and steal data, including passwords, client financial records and other business-critical information.

Malware comes in many forms, some more insidious than others. It can launch via a link a user unknowingly clicks on in a phishing email or text. It can find a network through a user's cell phone or mobile device. It can also hide behind an advertisement online that looks completely legitimate but launches malware when a user clicks on it.

It also does all sorts of damage. Spyware gathers user data, often using keyloggers that record every keystroke a user types to swipe passwords, private information about clients and other critical details. Some malware gives cybercriminals administrator access—in other words, complete control—of a business's system without anybody realizing it's happening. There's even a form of malware that forces a user's computer to undertake the extremely electricity-intensive process of mining Bitcoin.

One particularly nasty version of malware is ransomware. Cybercriminals use ransomware to steal a company's data and essentially hold it hostage, forcing the company to pay a large sum of money—a literal ransom—to get it back. And it's not just for big organizations. The Verizon report found that ransomware was present in about 20% of attacks on small businesses.

What's worse is that malware can spread. Computer viruses, well known for decades among just about all computer users, are a form of malware. A trojan can also move from one machine to another. Once infected, businesses can unknowingly spread malware to their clients and turn them into victims of cyberattacks as well.

Businesses can unknowingly spread malware to their clients and turn them into victims of cyberattacks as well.



Ransomware was used in about **20%** of attacks on SMBs.

But that's not likely to happen if a business runs critical applications in the cloud with a cloud provider. That's because a cloud provider can catch malware as soon as it enters a network and stop it from deploying any malicious applications that would give attackers the control they seek. Even if a cloud provider doesn't stop the malware itself, it can stop the attack from doing any damage. Either way, the business is safe.

Real-world example

How the cloud eliminates damage from malware attacks

Our advanced cloud security recently saved two accounting firms victimized by a malware attack—targeted at accountants—from experiencing extensive damage. Had those firms not been running applications in a secure cloud, they almost assuredly would have suffered prolonged and extensive damage to their systems, possibly resulting in downtime and stolen data. All it took was one user clicking on a single link.

When Rightworks learned of the attack at both firms, our anti-malware system and security protocol sprang into action, isolating and shutting down the affected server and removing the victim as a user. Rather than cause immense disruption for the entire firm, the security protocol disabled the server the individual victim was using, knocking only a few users offline while other workers continued...unaware of any issue.

Within minutes, the user who had clicked on the malware file was back up and running, and the rest of the firm continued to work unimpeded. Meanwhile, Rightworks was running security diagnostics on the attack.

Had the impacted firms not been running applications in the cloud, the attack would almost assuredly have succeeded and could have lasted for weeks or months. It's almost impossible for businesses to keep up with security developments themselves—traditional antivirus software wouldn't have caught the attack on the two accounting firms.

A cloud provider that constantly updates security definitions and can spot and disable malware is a much safer option than running and trying to manage antivirus applications in-house. Cybercrime is everywhere. Being able to stifle attacks—before they start—is critical to avoiding expensive damages caused by a major breach.



As a cloud provider, Rightworks has been through this before.

Internal threats

Attackers aren't always faceless threats in some far-off location. Sometimes, they're on the payroll.

While business owners might think their employees are beyond reproach, the numbers suggest otherwise.

The fact is that employee fraud can be a costly problem. The Association of Certified Fraud Examiners' **2020 Report to the Nations**—the most comprehensive study of employee fraud available—lays out a scenario that should cause even the most cautious firms to review their anti-fraud policies.

The report reveals that organizations lose an estimated **5% of revenues to fraud each year**. While that might sound like a small number, it adds up to a **median loss of \$125,000 per case and an average loss of \$1.5 million**. Not many businesses can afford that hit, particularly in a fragile economy. And once that money is gone, it's likely gone forever—**54% of companies surveyed in the Report to the Nations did not recover any money lost to fraud**.



Organizations lose an estimated **5%** of revenues to fraud each year.

Internal cybercriminals can use any of the tools of their trade to steal from their employers, including phishing and malware. And they can do it with exceptional credibility because they actually work for the business. Fraud is the most insidious type of attack and often both the most effective and the hardest to detect. But the cloud can help companies prevent fraud and avoid damage from would-be fraudsters.

In general, as the Report to the Nations reveals, physical documents are a major vector for fraud. Virtual documents stored in the cloud with a cloud provider are much safer. The report shows that **40% of fraudsters created fraudulent physical documents** in attempting to steal from their employers, while **36% altered physical documents**. By contrast, only 27% altered virtual documents, and 26% created fake virtual documents. Physical documents are generally easier to fake, alter and pass off as legitimate. With good controls in place, and critical business applications running in the cloud, electronic documents offer an added element of security.

The cloud offers other advantages in the battle against fraud. First, firms can track exactly who accesses which systems and which documents, and when—providing insight into employees who might show a pattern of accessing certain forms at unusual times or spending more time with a particular form than they should. Backups and archives in the cloud can reveal *how* documents have changed, *when* they changed and *who* changed them. Effectively, the cloud can play a critical role in helping a firm build a case against a fraudster.

Other benefits of moving

accounting operations to the cloud

As highlighted, the cloud can play a critical role in keeping businesses secure. But what exactly does moving to the cloud involve? The journey to the cloud is short, simple and inexpensive. First, it's important to know what the cloud is.

What is the cloud, exactly?

Simply stated, the "cloud" is a metaphor for the internet. And, like the internet, the cloud is:

- A place where people go to store information.
- A place where people go to find information.
- Accessible from any internet-connected device, including desktops, laptops, tablets and smartphones.

No matter where employees are, if the devices they're using can connect to the internet, they can connect to the cloud. So, when someone says, "My QuickBooks® Desktop is in the cloud," that really means: **"I can open the full-featured desktop version of QuickBooks from any laptop, desktop, smartphone or tablet."**

What does it take to move to the cloud?

Not much, actually. The idea behind moving to the cloud is, in part, to simplify access to critical applications. A move to the cloud is easy. It's as simple as an email or phone call to sign up for service with a cloud provider. After that, the provider takes care of everything.

- Once a provider sets up access, all employees have to do is log out of applications once and log back in. That's it.
- The whole move to the cloud takes place off-site, with no involvement from the firm other than signing up for cloud service. The provider's professionals move data to servers in world-class, secure data centers.
- Moving to the cloud doesn't affect software licenses at all. There's no need to get in touch with software vendors or anybody else, for that matter.
- The cutover to a cloud service is nearly immediate and completely painless. It's so quick and seamless that employees probably won't even know it has happened. There is no business disruption.
- And the cloud is not expensive. Moving accounting and business applications to the cloud can cost less than \$2 per day.

What are some of the other benefits of the cloud?

The Rightworks cloud offerings deliver a variety of other benefits:

- Access to QuickBooks Desktop, along with more than 250 other business-critical apps, from any internet-connected device.
- Real-time collaboration with clients and colleagues on the same, live QuickBooks Desktop files.
- 24/7 US-based support with specialists trained in accounting and tax application best practices.

Plus, Rightworks:

- Is 100% focused on accounting—and has been for more than 20 years.
- Offers a deep understanding of accounting tools and system best practices.
- Delivers experience in determining the best technology stack to support a firm's CAAS (client accounting and advisory services) practice.



A cloud provider is the **best protection** against security threats

Security is becoming more critical for small businesses to manage and more difficult to control. The threats to businesses will likely increase as remote work becomes the norm in the post-COVID era. When facing the three major threats to their operations, the safest play for companies is to let a cloud provider like Rightworks host critical business applications and handle security.

Want to learn more?

Contact us today at **888.210.0237**

 **rightworks**
rightworks.com