



Right Networks®

eBook

Flirting with disaster: How CPA firms can find the security help they desperately need

Flirting with disaster: How CPA firms can find the security help they desperately need

Accounting firms are major targets for cybercriminals looking to pilfer data, and ultimately money, from clients. Some firms might be tempted to try and ward off threats by tackling cybersecurity themselves. That approach is fraught with danger. Firms of all sizes need help with managing the complexities and risk of cybersecurity. Fortunately, that help exists.

Because CPA firms control the lifeblood of their clients—money—they are frequent targets for data theft. In fact, ITProPortal.com reports that according to CNBC, [accounting firms are the most targeted](#) type of business among small companies.



NUMBERS SHOW DATA BREACHES ARE A CONSTANT THREAT TO ACCOUNTING FIRMS

The [numbers are alarming](#), as reported by The Tax Adviser:

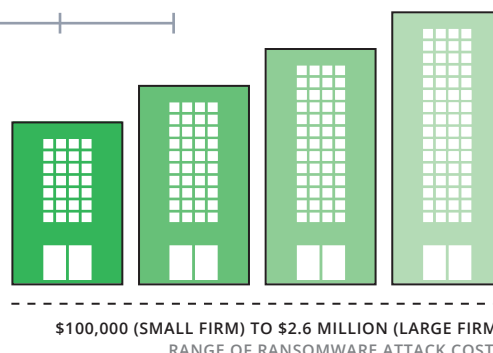
- ▶ Cleaning up after a cybersecurity breach typically costs a firm between \$70,000 to \$300,000.



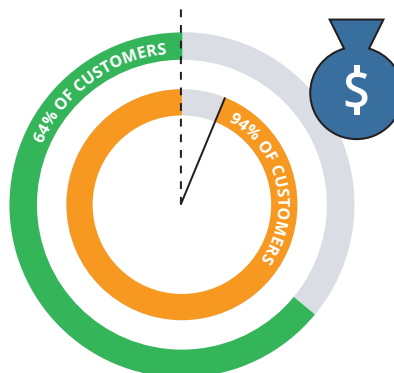
- ▶ Reporting and credit monitoring requirements could cost further \$100,000 to \$300,000.



- ▶ Ransoms paid by firms to recover their data after ransomware attacks—just one type of cybersecurity threat—usually range between \$100,000 for a small firm to \$2.6 million for a large firm
- ▶ Paying a ransom doesn't guarantee data recovery, which can cost tens of thousands of dollars more.



Of course, the cost of a breach reaches far beyond money spent to remedy the breach itself. The losses a firm could incur in fleeing clients and damaged reputation are harder to quantify but potentially much more damaging. In one survey cited in CPA Practice Advisor, 64 percent of customers said they [would cease to work with a company](#) if their personal or financial information were stolen. And 94 percent of those customers would consider taking legal action against the hacked company.



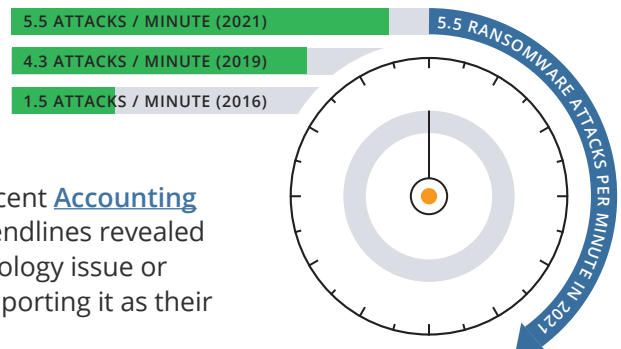


NO CPA FIRM IS IMMUNE TO CYBERSECURITY THREATS

Breaches aren't rare, nor are they a problem only for firms of a certain size or type. Attempts to steal data happen constantly. In reporting from Accounting Today, experts from the Herjavec Group expect ransomware attacks alone to [occur at a rate of 5.5 attacks per minute](#) in 2021—almost 8000 attacks per day. That's up from 4.3 per minute in 2019 and 1.5 per minute in 2016, an increase of 267 percent in just five years.

Firms are, at least, worried about security. The most recent [Accounting Firm Operations and Technology Survey](#) from CPA Trendlines revealed that security and risk management is the biggest technology issue or annoyance for firms, with nearly half of respondents reporting it as their primary concern.

With security such a pervasive and important issue, CPA firms that decide to handle security on their own could be putting themselves and their clients at risk. [Experts recommend that firms seek outside expertise](#), including implementing “a cloud solution to help support . . . legal, regulatory, and risk management obligations.” So, just as companies hire firms to handle accounting, bringing in expertise from a cloud provider to enhance security is a worthwhile and even necessary initiative.



HOW THE CLOUD HELPS ACCOUNTING FIRMS MEET 5 MAJOR SECURITY CHALLENGES

Given their vulnerable position as keepers of critical client data, and given the ever-shifting and increasingly dangerous cybersecurity landscape, accounting firms face security challenges that are daunting, perhaps even scary. The trend toward working from home brought on by the COVID-19 pandemic has only increased the risk of data breaches.

But firms don't have to—and shouldn't—deal with security on their own. A move as simple as running critical business applications in the cloud can enable firms to meet security challenges and protect client data with the help of a cloud provider.

⇒ **CHALLENGE #1: Depth of security expertise.** One major issue facing firms is that not all of them have IT staff to manage security. Those that do need IT professionals to handle just about any technology issue, from lost passwords to printers that blink error messages. There's no getting around the need for that kind of expertise—it's what users need and expect.



But what firms have in breadth of technical expertise, they usually lack in depth. Managing security is a full-time job, with the variety and nature of attacks evolving constantly. There's no way a firm, or any other business without specific expertise, could possibly stay up to date on how to prevent or recover from security threats.

How a cloud provider helps: Providers offer both breadth and depth of security expertise, with professionals who do nothing but manage security for their clients. There's no substitute for deep security capabilities when client data is at stake. Again, clients hire firms for their expertise in accounting rather than trying to handle it themselves. The same principle applies here—the experts handle security, and firms can focus on serving clients.

⇒ **CHALLENGE #2: The need for continual security training.** The economy has been fragile since COVID-19 shut down much of the American economy in March. Instability and uncertainty have led to budget cuts at many firms and businesses, and one of the first casualties of those cuts is almost always employee training. That's business . . . but it's also dangerous.

It's difficult enough, as mentioned earlier, for firms to keep up with trends in security given all of the other responsibilities they have.

If they hope to manage security on their own, they'll need to train somebody in-house. Without adequate training—which is not only a financial drain but time-consuming, too—leaders at firms won't even know what they don't know.

How a cloud provider helps: Providers provide extensive and up-to-date training for security professionals whose job it is to always be on the forefront of security strategies and technologies. Falling behind on security is simply not an option with the growing proliferation of attacks, and it's not a problem when a cloud provider takes care of keeping its experts up to date so firms don't have to make that investment themselves.

⇒ **CHALLENGE #3: Awareness vs. implementation.** It happens in all kinds of companies—intent to invest in new technology turns into a purchase delayed or never made at all. When cybersecurity is at stake, though, awareness and intention aren't enough. Implementation is critical. As is the case with training, failure to keep up with the pace of technology can lead to disaster. Long implementation cycles can rob firms of valuable time, causing them to stay behind security trends even when they're trying to get ahead.

Firms that want to handle security in-house need to make constant investments—in multifactor authentication, antivirus technologies, firewalls, zero-trust networks and more in order to properly ensure the safety of client data. It's a lot to ask of a company that isn't in the business of selling technology or technology services, especially given the current challenges of working remotely. It's also potentially expensive.

How a cloud provider helps: Providers solve the problem of awareness vs. implementation by managing updates, upgrades and other critical security improvements for firms. A provider will handle most of those tasks automatically. Dedicated professionals are in charge of securing client data. All CPAs have to do is run their firms. Nothing slips through the cracks, and client data remains secure.

⇒ **CHALLENGE #4: The complexity of recovery.** Suppose a breach does happen. What next? As noted in the numbers above, the process of recovering data can be staggeringly difficult and

extremely expensive. Even a non-security issue, such as server failure or backup that doesn't work properly, can throw a firm into chaos.

Recovery can be arduous, slow, expensive—and sometimes impossible. Client relationships and the firm's reputation, meanwhile, are on the line while the whole thing plays out. But a cyberattack or technological failure is only as dangerous as the damage it can do. Even a successful attack will have minimal impact if a firm catches it quickly enough to nullify its effect.

How a cloud provider helps: Speed of recovery is a key advantage of outsourcing security to a cloud provider. Professionals who mitigate cybersecurity attacks and other disasters will have a firm back up and running far more quickly than most firms could manage on their own—while also more effectively avoiding problems from the beginning.

⇒ **CHALLENGE #5: Working from home.** The likelihood is that working from home will become far more common in the future than it was before March 2020, even after the COVID pandemic subsides. [Employees like it, as do many bosses.](#) But for firms, remote work still presents many challenges that were less prominent pre-pandemic. For instance, the transfer of client data from one remote device to another can present a major security threat if it occurs outside the cloud—for instance, via email.

Then there are the computers themselves. With children homeschooling, many parents are pulling out old computers and putting them back to work. Those computers could be ridden with malware or all sorts of other viruses just waiting to escape onto a network. Beyond that, kids aren't necessarily trained to avoid cybersecurity attacks such as phishing scams. Remote work multiplies the opportunity for security breaches.

How a cloud provider helps: Professionals who work for cloud providers are capable of managing the complexities of remote work because their business depends on keeping clients up and running. Plus, cloud hosting enables workers to use the same application (such as QuickBooks Desktop) at the same time from anywhere . . . securely.

A NEW ERA FOR SECURITY AT ACCOUNTING FIRMS CALLS FOR THE CLOUD

With the [IRS cracking down on security requirements for accounting firms](#), and with cybersecurity threats constantly evolving, firms must prioritize security now by engaging with a cloud provider. But what does that mean, exactly? As it turns out, the process of shoring up security by moving applications to the cloud is very simple. The journey to the cloud is short, simple and inexpensive. How does a firm move toward the cloud? 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 firm 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," what that really means is: "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 really 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.

- ▶ Starting to use the cloud is simple. 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 cloud is about much more than just security. The [Right Networks 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.
- ▶ US-based support agents trained on accounting and tax application best practices, available 24/7/365.

Plus, Right Networks:

- ▶ Is 100 percent 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 practice;
- ▶ Is an active technology thought leader and influencer within the accounting industry.

Now is the **time to act**. Firms' relationship with their clients' most critical data makes them frequent targets of attacks. They are under fire every day, but they need to focus on accounting rather than managing cybersecurity. For their own peace of mind and that of their clients, firms need to turn to Cloud providers **such as Right Networks** to protect their most valuable asset. ➡