

rewind

Strategies to Enhance Data Security

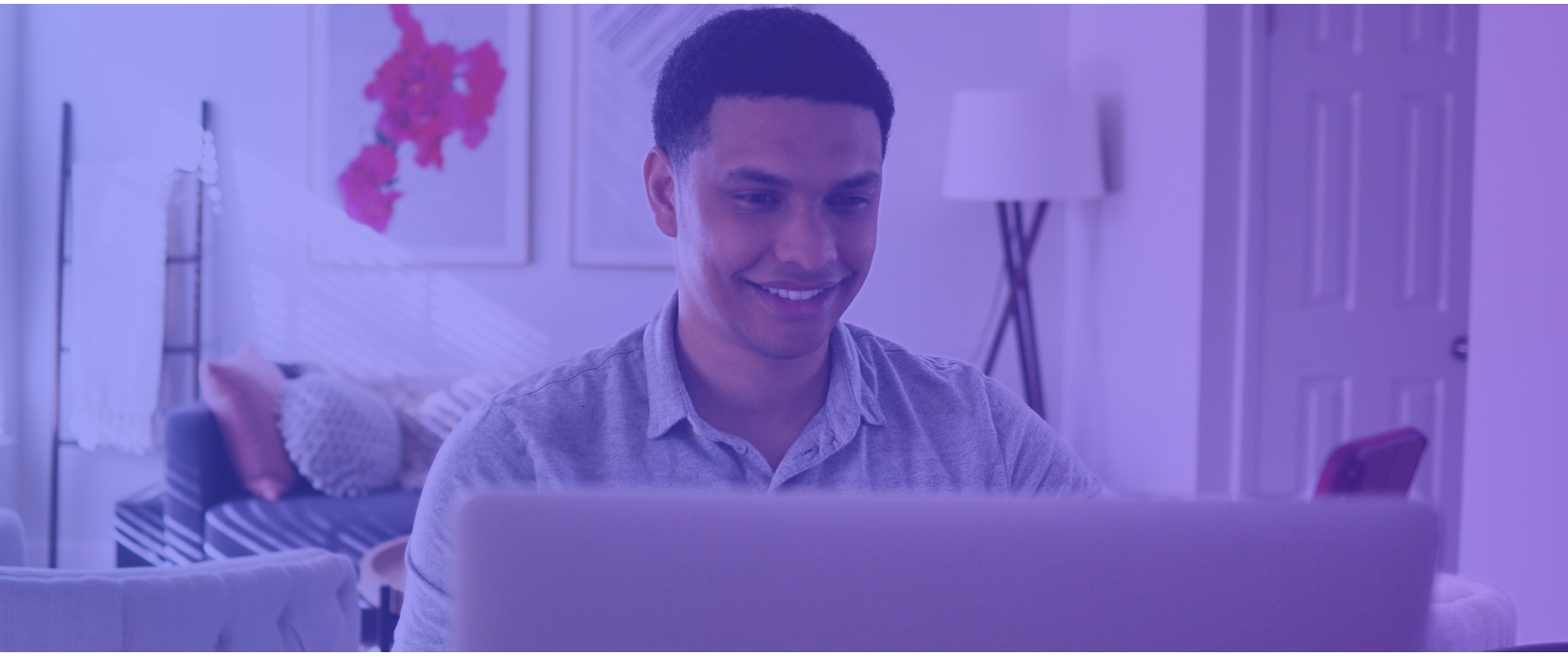
A deeper dive into smart security protocols for CAS practices.

Introduction

Accounting firms constantly import massive amounts of financial information and data from clients, but not all firms practice handling data securely. When many transitioned to working from home at the beginning of the COVID-19 pandemic, the risk of leaked or damaged data skyrocketed for firms lacking an established security protocol for work outside the office. According to research published in peer-reviewed journal ScienceDirect, "Moving millions of employees, their computers and their data away from a secure office environment presents tremendous data security risks, ranging from simple technical glitches to full-scale ransomware attacks." While working from home certainly compounds the risks, the truth is that no firm—regardless of working location—is immune from lost, damaged, or stolen data.

Accounting firms must take proactive action to ensure that the amount of sensitive information and data they house as part of their CAS practice is stored and maintained securely. Accountants have a duty to their clients—not only is trust on the line, but professional reputation and federal compliance rules as well. Since the Gramm-Leach-Bliley Act was passed by the Federal Trade Commission in 1999, all financial institutions are required, through the Safeguards Rule, to maintain a written information security plan that "describes their program to protect customer information."

Use this guide as a resource to develop security protocols for your firm.



Tone Starts at the Top

Executive-level commitment to security is imperative to establish, and sets a precedent for the rest of the company. The saying "lead by example" applies here as much as anywhere–if employees don't see the leadership team prioritizing security, it won't get the attention it deserves.

Security expert Nick Norton, co-founder of Geels Norton, illustrated this concept best in a scenario he introduced during his recent webinar, *Building Out Security Protocols for Your Practice*. He describes a situation in which a partner at a firm neglects to follow the established security policy for emailing about sensitive information with a client. "Copied on that email are also members of their team—managers, associates, supervisors—who are watching the partner... communicating sensitive data in [a manner that isn't allowed]." Norton explained. "Now, what does that show to the rest of the employees? It shows that we understand security protocols, but we're not following them."

Norton went on to describe an ever-spiraling situation in which more and more employees start sending sensitive information in plain text over email, without using the secure email platform the firm had already set up.

Developing a risk-aware culture will drive adoption and commitment to security practices. Make sure to lead by example—just because you're on the leadership team does not mean you can shirk protocols. They're established to protect everyone involved, from clients to team members.

Reduce the Risk of Human Error

Firms should seek out and adopt technology that mitigates the risk of data mishaps.



"Human error is the biggest culprit resulting in data loss and unfortunately, there is very little control over it. Whether it's by you, your client, or your staff, there is no option to undo a minor setback or a major security breach. You are responsible for recovering the data. If the compromised data contains personally identifiable information you might also have to report the breach to the affected clients and possibly regulatory bodies."

— Mike Potter, co-founder and CEO of Rewind,
Building Your Firm's Backup Strategy: Accounting Today

According to an analysis by the UK Information Commissioner's Office and CybSafe, a UK-based analytics company, human error was found to be responsible for around 90% of cyber attacks in 2019. Using the appropriate technology can reduce the risk of accidental data loss dramatically. Here are a few areas of implementation:

Use a Virtual Private Network

Using a Virtual Private Network, commonly known as a VPN, is one simple way to enhance security tenfold—especially for teams working from home, or anyone who occasionally works at a cafe. At its most basic level, a VPN service creates a more secure network that is much less susceptible to hacking and identity theft.



There are many VPN providers on the market, but they all function the same way. Using a VPN occludes your true IP address, which is literally the "address" to your computer. If someone knows your IP address, they can access your browsing history among other sensitive areas. "VPNs use encryption to scramble data, making it unreadable for people trying to access it. Data security is especially important when using a public Wi-Fi network, because it prevents anyone else on the network from eavesdropping on your internet activity." (NortonLifeLock, *What is a VPN?*, 14 Jan 2021).

Device Oversight

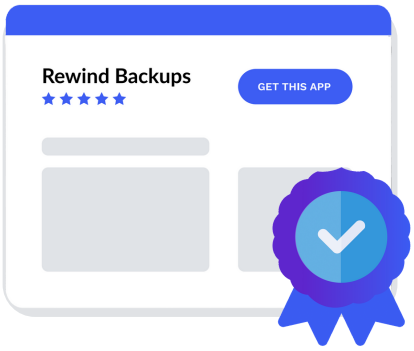
Mobile Device Management (MDM) has become increasingly more important given how widely dispersed we have become—not only because of remote work during COVID-19, but it's a reality of globalization that large firms and successful companies often have office locations across the world. Having personnel working from various locations created a need for a systematic oversight tool: enter MDM. The acronym refers to a range of available softwares that all assist in the management and oversight of company devices that employees are using for work.

Mobile device management offers a centralized way to manage all devices—from laptops to phones and tablets, using MDM software allows insight into all devices from a singular dashboard that an IT manager or another leader oversees. This is the most comprehensive and practical method to ensure all team members who use company devices also use safe networks to connect to Wi-Fi, access the company domain securely, keep anti-virus software up-to-date, monitor security issues and threats, and enforce any other company-wide policies regarding technology.

Maintain Backups of Client Files

Practicing a regular backup strategy is one of the most important security steps a firm can take, because even the most comprehensive security protocols in the world can't completely prevent data loss—they only mitigate the risk. The best step to take is to be proactive and continuously back up important data in the (very real) off-chance that anything happens that results in data damage or loss. It's imperative to backup stored data regularly and on a secure system as a safeguard against loss, damage, or tampering.

There are three main ways to backup data and files. Choose a technique that works best both for the firm's needs and the client's peace of mind:



Local Storage

One example of backing up data using the local storage method is exporting raw data as a .CSV file and placing that on a USB drive or an external hard drive. A plus side of this method is that external hard drives or thumb drives are inexpensive. However, it's not particularly secure, and this method requires someone to remember to manually back up the data regularly. While many people feel that being able to physically hold the data and "see" it as an object that can be stored in a safe place, that very aspect carries significant risk. The data is lost immediately if something happens to the storage device—whether it's misplaced, damaged in a flood or fire, or stolen. And even if nothing happens to the device, restoring the backed-up data with this method can be error-prone and labor intensive.

Physical Server

This method is similar to the previous in that it involves a physical object. A physical server is located on-premise at the firm's main location. It's more secure than local storage, and it's more accessible from company devices. However, it requires expensive hardware that relies on technical knowledge and time to maintain. And like the local storage option, this method also requires someone to manually backup the data on a regular basis.

Cloud-based

For any firm lacking an in-house IT team, cloud-based backups are the way to go. These services are affordable, and typically paid as a monthly subscription. Not all cloud-based backups are created equal, however. A good cloud backup system will be secure and automated, meaning it doesn't take extra time and to-do lists for firms to maintain accurate, timely backups. Additionally, the service is only useful if users can quickly recover and reconstitute lost data whenever necessary.



The cloud tools that many accountants use, such as QuickBooks Online or Xero, are not obligated to protect or restore the data kept on their systems. However, due to the FTC's Safeguards Rule and the expectations of clients, accounting professionals are obligated to protect it in any way possible.

Make sure your firm is equipped for any data loss scenario by implementing a backup plan ahead of time. Avoid future disruptions and unnecessary embarrassment by taking precautionary steps today. One of the easiest and most cost-effective ways to put a backup strategy in place is to use an automated backup and recovery service like Rewind.

Stop Using Email for Sensitive Data

Not only is email a productivity killer, it's a major source of accidentally leaked information and an extremely vulnerable point of cybercrime. Phishing, one of the most common methods of online scamming, occurs almost entirely through email—when the victim of the scam opens an email and unsuspectingly gives away sensitive information, typically usernames and passwords.

Phishing attacks can be costly for firms, with the average scam costing "a mid-size business $1.6 million in damages and recovery costs," according to secure client communication service Liscio. "As these low-cost, high-reward crimes grow in success and popularity, it's no longer a matter of if you'll be targeted, but when."

Using a platform like Liscio for client communication allows firms to streamline many services in a secure way. For example, Liscio makes it easy for clients to use their phones to safely and simply send PDFs of documents that they formerly emailed pictures of. It also enables accountants and clients to exchange text messages, which has the double effect of creating a better client experience while being more secure than emailing.

Consistent Training and Education

You can bend over backwards to be secure, but if your employees, vendors, and clients aren't playing along, they're just as vulnerable. Consistently train, educate, and communicate with your team about cyber security, and make it a point to discuss security with clients as well. Educate consistently on team expectations using strategies such as phishing testing, security awareness training, and sharing any examples of risks team-wide. As Rewind co-founder and CEO Mike Potter advises, "Be proactive and make sure everyone understands the firm's data security policies. Staff should have a good understanding of how and why data is backed up, and know where to access the information they need to implement security measures. Regularly run detailed training sessions with the team on your firm's responsibilities and compliance requirements when backing up your client's data."



Curious to learn more about strategies to enhance data security? Learn more about implementing Rewind for your QuickBooks Online clients.

About Rewind

Since 2015, Rewind has been on a mission to help businesses protect their SaaS and cloud data. Today, over 80,000 customers in more than 100 countries use Rewind's top-reviewed apps and support to ensure their software-as-a-service applications run uninterrupted. The Rewind platform enables companies to back up, restore and copy the critical data that drives their business.

rewind