6-PART CLOUD ACCOUNTING SECURITY CHECKUP INCLUDED

How to build a data security stack at your firm

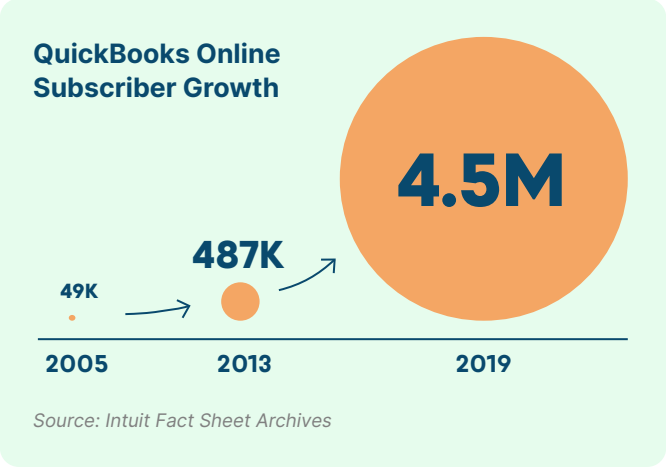
Understand the latest data security risks facing accountants and bookkeepers. Learn how to protect your firm — and your clients' data.

relay Practice Protect MORE TRUST. LESS RISK. rewind

Introduction:

Why firms need to think about data security

In the last decade, the accounting profession experienced a significant shift: it moved online. All it takes to illustrate the scale of this change is to look at the growth of QuickBooks Online subscriptions between 2013 and 2019. The number of paying users rose ninefold — to over 4.5 million businesses globally. This data point alone accounts for 15% of all small businesses in The United States. Post Covid-19, we're safe to assume that this trend has only accelerated.



Source: Intuit Fact Sheet Archives

While the shift to cloud accounting has been a net positive — improving efficiency and flexibility for accountants and their clients — it also transformed the data security landscape.

One of the most distinctive features of cloud accounting software is the ease with which it connects to other applications. Accountants and bookkeepers no longer depend solely on one accounting system. Instead, advisors work inside an "app stack": multiple applications, all integrated with a central general ledger (e.g., QuickBooks Online), each serving a unique business need. And there's a tool for almost everything: payroll, expense management, forecasting, you name it.

As a result, accountants and bookkeepers have also become financial technology advisors. They often decide where financial data is stored, how it flows through different applications, and who can access it.

And as they make these decisions, many advisors start to wonder, "Am I handling my clients' data securely?"

We wrote this ebook to help you answer that question. The companies behind this guide — Rewind, Practice Protect, and Relay — have a few things in common. We all serve accountants and bookkeepers, we deeply integrate with your cloud accounting software, and we share a common mission of helping firms achieve better data security.

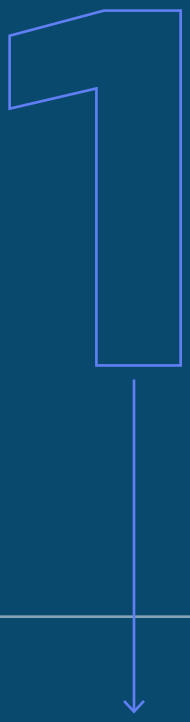
In this guide, you'll find:

- → An overview of today's data security landscape: how data breaches occur, what puts your firm at risk, and your obligations to your clients.
- → A framework for thinking about and creating your data security plan.
- → An overview of what a best-in-class data security stack might look like.
- → A checklist to assess whether you're handling client data securely.

By the end of this guide, you'll have a better understanding of data security risks and be ready to manage them with confidence.

Let's dive in!

Contents



Security and your firm: the landscape today

PART ONE

Let's start by taking a look at the security landscape as it stands today. While accountants and bookkeepers reap massive benefits from cloud accounting software and other online workflow tools, there is a catch. Every time you or your employees access sensitive client data online, you expose your firm to security risks.

Unauthorized access to systems or services (you may think of this as "hacking") is the primary driver behind many breaches. And the number of data breaches has gone up dramatically in recent years. According to a recent report by RiskBased Security, **over 27 billion records were exposed globally in just the first half of 2020** — almost *double* the number of records exposed during the *entirety of 2019*.

What type of information is at risk of being breached? Emails, passwords and social security numbers (SSNs) top the list. And advisors work in a high-risk industry: **finance is the third most frequently breached sector**, following on the heels of healthcare and information technology.

Of course, this does not mean you should avoid online accounting software and other digital tools — they are an integral part of modern bookkeeping and accounting.

Plus, cloud accounting tools are typically more secure than their desktop-based counterparts.

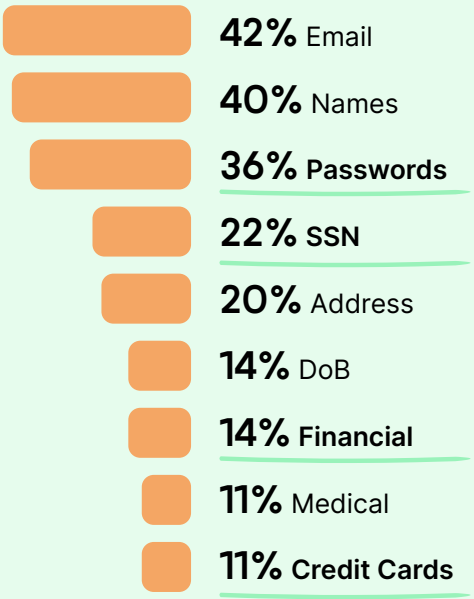
But as the use of various cloud platforms increases, it is essential to assess your security strategy and safeguard your client data. While the tools themselves may be more secure, the way you choose to manage data across different apps may open you to other risks.

Just as you use a stack of online applications to do your accounting and bookkeeping work — accessing sensitive client data in the process — you need to think about a complementary "security stack," a set of tools and behaviors to protect your handling of that sensitive information.

We'll introduce you to some great options for your security stack later in this guide, but first, let's talk about the security risks facing firms and your obligations to clients.

Likelihood of exposure based on data type

A "breach" can contain different types of data — email addresses and names are the most common. More alarmingly, about one in ten breaches reveal credit card information. Here's the likelihood of being breached based on different types of data:



Source: Data Breach QuickView Report, based on reports during the first half of 2020

Key cyber security threats

Due to the highly sensitive nature of client financial data, a "head-in-the-sand" approach is simply not an option for most accounting and bookkeeping firms. As noted above, cybercriminals target businesses working in the financial services sector almost as frequently as those in healthcare and information technology. And this should come as no surprise if we take a closer look at the type of data that advisors handle.

As part of their job, accountants and bookkeepers access the most sensitive information belonging to their clients. This can include the personal data of the business owners, the company's financial statements, lists of clients and vendors, banking credentials, IDs, Social Security Numbers, credit cards, personal details about employees, and an abundance of other data.

Accounting firms and their employees can have unrestricted access to:

Business Owner Data

- Social Security Numbers
- Bank logins
- Logins to payment service providers
- Tax filings
- Data about business financials, clients, and vendors
- Photos of government-issued IDs
- Personal addresses of beneficial owners
- Phone numbers
- Email addresses
- Credit card information
- Articles of incorporation
- Articles of organization

Data About Employees

- Social Security Numbers
- Names, addresses, and phone numbers
- Email addresses
- Bank account numbers
- Employment information, i.e., salaries and contracts
- Emergency contacts

If you're providing tax services, monthly bookkeeping, or payroll services, your firm likely has access to most of the information listed above. This is all the more reason to make sure you're not at risk of a breach.

One misconception held by many advisors is that unless you work for the Big Four, you're not really at risk. Smaller firms might feel like they're less of a target. But this couldn't be further from the truth. While large firms have the resources and savvy to fend off cyberattacks, small- to medium-sized practices are often ill-equipped to respond to a breach. Cybercriminals know this and actively target the underprepared "low-hanging fruit." This is why **in 2019, 43% of breaches involved small business victims**, according to Verizon's Data Breach Investigations Report.

Breaches by cybercriminals represent an external threat — but there are potential internal risks as well, like disgruntled employees, negligence, or human error. If your firm has employees, the risk of internal leaks (accidental or otherwise) goes up simply because the number of people accessing confidential data increases. A 2021 data risk report from Varonis revealed that 19% of sensitive files at small companies in the financial sector are accessible to **everyone who works at the firm**. This creates a lot of potential risk.

MISCONCEPTION

Cybercriminals only target the Big Four and big financial institutions.

REALITY

In 2019, 43% of breaches involved small business victims

Case Study

In 2016, the IRS suffered an automated cyberattack. Fortunately, no personal taxpayer data was compromised or disclosed by the breach — but the IRS noted that the cybercriminals succeeded in using 101,000 SSNs to access e-file PINs, which taxpayers use to e-file tax returns. What's important to note is that all of those SSNs were stolen "elsewhere outside of the IRS." Attackers often try to get hold of taxpayer information because it can be exploited in many different ways. This makes accounting and bookkeeping firms great targets for cybercriminals.

Source: Journal of Accountancy

What do attackers do when they breach your data?

Money is the main motivator behind most data breaches. As a result, cybercriminals look for targets that are easy to breach and have access to funds. This makes many small businesses great targets. Once breached, there are a number of different ways for an attacker to extract funds:

1. Steal funds from the business.
2. Encrypt data with ransomware and demand payment to restore access.
3. Threaten to delete data — or delete it outright.
4. Use sensitive information to extort your clients or other contacts.
5. Use personally-identifiable information to commit identity fraud.

According to Verizon's report, 71% of breaches are financially motivated. But even if your firm gets away without financial damages, your client's data and your firm's reputation still end up compromised.

Client security concerns & your legal obligations

Clients want assurances that their data is protected. As remote work becomes more widespread and professional service firms rely all the more on cloud software, anxieties about security threats are growing.

When it comes to financial data, such anxieties are already pretty high. For example, a recent Unisys survey on customer security concerns found that

64% of respondents were either very concerned or extremely concerned about "other people obtaining or using" their credit or debit card information.

But it doesn't end with simply understanding client concerns. If you provide tax preparation services, you are legally duty-bound to protect sensitive financial data by the Safeguards Rule, as outlined by the Federal Trade Commission (FTC). While FTC's Safeguards Rule is primarily aimed at financial institutions that store sensitive customer information, it also extends to those who are "significantly engaged" in providing financial products or services. This includes tax preparation.

Work in tax? The FTC's Safeguards Rule may apply to your firm

Summary of what the FTC Safeguards Rule requires professional tax preparers to do:

- Designate staff who coordinate your information security program.
- Identify reasonably foreseeable internal and external risks to security, confidentiality, and integrity of customer information.
- Design and implement information safeguards to control the risks you identify.
- Take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards.

Source: FTC Safeguards Rule

The legal duty to safeguard client data doesn't end with sector-specific legislation. After numerous high-profile data breaches across the United States, some states are passing legislation that mandates specific data management strategies for businesses across the board. This includes accounting and bookkeeping firms. At least 45 states have introduced or are considering **over 250 bills dedicated to cybersecurity**.

One recent example is the legislation set out in New York. In 2019, the state passed the New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act. The SHIELD Act mandates that businesses — including accounting and bookkeeping firms — implement data security measures to protect their customer information. These measures include:

- Administrative safeguards, such as conducting risk assessments and providing training to employees.
- Technical safeguards, which include assessing how information is processed, transmitted, and stored throughout different software.
- Physical safeguards, requiring businesses to assess risks of information storage and disposal, respond to intrusions and protect against unauthorized access.

In the event of a breach and failure to meet the recommendations and policies set out in the SHIELD Act, the state of New York can issue fines of up to $200,000.

"Federal law gives the Federal Trade Commission authority to set data safeguard regulations for various entities, including professional tax return preparers. According to the FTC Safeguards Rule, tax return preparers must create and enact written information security plans to protect client data. Failure to do so may result in an FTC investigation."

Source: IRS: Safeguarding Taxpayer Data

The "Shared Responsibility Model"

At this point, you may be wondering how much responsibility for safeguarding your clients' data falls on cloud software providers. Isn't it the vendor's duty to ward off cyberattacks and prevent data breaches? After all, they're the ones storing the data. The answer is a little more complicated than that.

Most cloud software providers follow a common framework when assigning responsibility: the Shared Responsibility Model. This framework outlines who has the "duty of care" to protect client information — that is, whether the responsibility to secure data falls on the cloud software vendor or on the user. As the name implies, this duty is shared by both parties. And while vendors take on varying layers of responsibility, more often than not it is **users like you who are responsible for appraising risk and then protecting access, identity and data when using the software.**

A survey conducted by Rewind showed that 40% of SaaS users had experienced data loss – and that an even higher percentage of respondents (49%) were unclear about their role in the Shared Responsibility Model.

This is why a security plan — which includes efficient external resources (your "security stack"!) and strategic internal processes — is integral to the long-term safety and success of your business. Next up, we're going to share an overview of what to include in yours.

Sources:

RiskBased Security — 2020 Mid Year Report: Data Breach QuickView

Verizon — 2019 Data Breach Investigations Report

Verizon — 2021 Data Breach Investigations Report

Rewind — The Shared Responsibility Model and SaaS, Explained

Practice Protect — Accounting Cyber-Security Guide

Varonis — 2021 Financial Data Risk Report

Unisys — In Financial Services, Customer Security Concerns Change and Intensify

IRS — Tax Professionals: Protect Your Clients, Protect Yourself from Identity Theft

National Conference of State Legislatures

Accounting Today — Why Cybersecurity Should Mean Everything to Every Tax Pro

Four critical components of a robust security plan

PART TWO

Security is a balancing act of trust and resilience. To stay competitive as a firm, you need to trust in and use digital technologies. At the same time, it's important to build resiliency against cyberattacks by safeguarding yourself and your clients.

In a recent report, Rethink the Security & Risk Strategy, Gartner gives two recommendations for achieving this balance. First, take the time to better understand how information flows through your firm (meaning: the technology you and your clients use). And second, design your security plan in a people-centric way. As we learned in Part 1, many breaches occur due to human behavior and mistakes. So it's critical that both your firm's employees and external collaborators follow best security practices when accessing sensitive data.

With these strategies in mind, we're going to walk you through a step-by-step framework that includes four key components:

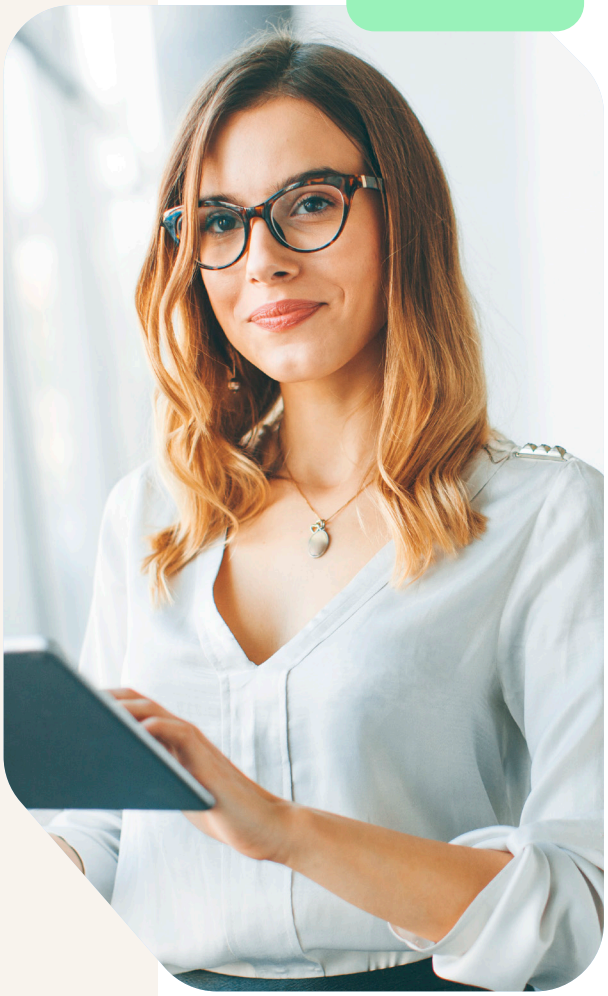
STEP 1: Identify security threats

STEP 2: Implement security technology

STEP 3: Adopt and reinforce secure behavior at your firm

STEP 4: Advise and influence your clients to follow security best practices

Steps 3 and 4 each build on the groundwork of the previous levels. Once you outline a security plan for your business that systematically incorporates all four components, you'll be much better equipped to defend against potential threats.



STEP 1:

Identify security threats

Before building your security stack, it's helpful to identify the potential threats. Below, we've highlighted the threats you're more likely to encounter as a firm. Once you're familiar with them, it will be easier to put together an appropriate data security plan.

Here's an overview of some of the most common methods of cyberattack:

- You've likely heard of **phishing**, which is an underhanded process of collecting sensitive information by setting up fake websites. It can also take the form of convincing people to download attachments that infect your system or network with malware.
- There are multiple ways that **passwords** can be compromised. This includes guessing or stealing the correct passcode, using a program to hack the password, or installing a "keylogger" on your system, which records the strokes on your keyboard.
- A **ransomware** attack uses malware to infiltrate and then control your network. Cybercriminals then demand a "ransom" if you want to access your own data or stop the hackers from releasing private information on a public forum.
- **Distributed Denial of Service** (DDoS) happens when a hacker overloads your server with requests until your website or entire network has to shut down.
- **Malicious software or malware** can include viruses, worms, ransomware, and spyware. Malware applications will try to gain unauthorized access to data or corrupt important information.
- An **inside attack**, often perpetrated by disgruntled or former employees, happens when someone gets internal access and leaks confidential data.
- **Advanced Persistent Threats** (APTs) happen when an attacker breaches your network over time to avoid setting off any alarm bells and alerting you to their hack. This is particularly insidious because they may breach your data through multiple routes.
- A **Man in the Middle** (MitM) attack happens when someone hacks your transaction with another party or service, often installing malware so that they can steal data.
- An **SQL injection attack** is the use of a coding language (SQL) to attack a website, then access private databases or download sensitive files.
- **Zero-day attacks** happen when hackers target flaws in the security of your network that you didn't even realize existed.

As you add more tools to your app stack, more people to your firm, and more clients to your portfolio, you also increase the potential avenues of attack. Fortunately, we are about to discuss the key types of security technology that can protect your firm from hackers and data breaches.

STEP 2: Implement security technology

This wouldn't be a guide to cybersecurity without a discussion about security technology — it's an integral part of any security plan. We've put together a list of solutions in this section. Implementing them will go a long way in protecting both your firm and your clients from data breaches.

There is no such thing as impenetrable cybersecurity. Everyone runs a risk of being breached — from the smallest firm to the most mature enterprise. But while you might not get to **perfect**, you can get to **really good** by deploying a combination of technologies at your firm.

Ultimately, to figure out which security technologies are best for your firm and where you should deploy them, you need to run a risk assessment. The FTC recommends that you "make a list of all equipment, software, and data you use, including laptops, smartphones, tablets, and point-of-sale devices." With a list of assets in place, you can start to build a security plan that directly addresses areas of risk.

Six ways to secure your firm — and your clients' data

1. **DATA BACKUP SOLUTIONS**
No matter how good your data security is, new exploits appear every day and there are always risks. One of the most important parts of your security stack should be a data backup solution that helps you quickly recover if ever breached.

2. **PASSWORD MANAGERS AND TWO-STEP AUTHENTICATION**
You're likely accessing dozens of applications, each of which requires a strong, unique password to ensure security. If you are following best practices when it comes to passwords, your best bet will be to keep them in a password manager. You should also use two-step authentication to secure your logins further.

3. **ANTIVIRUS SOFTWARE**
A good antivirus will go a long way in protecting you from most types of malware. While it won't prevent every data breach, it will secure you from the majority of viruses and malicious programs.

4. **FIREWALLS**
A firewall lets you monitor incoming and outgoing traffic throughout your network and block unauthorized access. If multiple staff members are accessing sensitive data at your organization, it may be worth investing in a firewall to establish stronger controls.

5. **ENCRYPTION SOFTWARE**
Encryption software helps you prevent unauthorized access to digital information. Using cryptography, it obscures the content of a file (for example, a financial statement) and keeps it obscured until the file is "unencrypted" (usually by entering a password). If you are storing or transferring sensitive client information, it's imperative to encrypt it — that way, even if the files themselves are compromised, the data stays safe.

6. **RELIABLE TECHNOLOGY PARTNERS**
While this isn't a technical solution, it's important to keep in mind that every application you use has a team of people behind it. What firms need is assurance that these teams are themselves responsive and client-centric when it comes to dealing with potential breaches. Recalling the Shared Responsibility Model from earlier — how confident are you that your app partners will devote resources to helping you recover and secure data in the event of a breach? Most applications have a privacy policy that's worth checking and can provide more insight if you speak to their support teams.

STEP 3: Adopt and reinforce secure behavior at your firm

You and your staff are integral to the success of your security policy. Even with fantastic security technology, your plan is incomplete without internal awareness and behavioral training.

Training isn't something that just happens once, either. It's an ongoing, evolving process that requires regular communication with employees about their roles in alleviating security risks. Some high-level responsibilities include:

- **Strong username and password management:** From encouraging the creation of more complex passwords to ensuring they're securely stored (and not shared), secure password policies are often the first line of defense that employees must embrace. To enable your staff further, roll out a firmwide password management solution.
- **Using multi-factor authentication:** Multi-factor authentication (MFA), sometimes known as two-factor authentication (2FA), is a security measure that requires users to provide two authentication factors before gaining access to an account. The first step is usually a password, while the second step may take the form of a text message, biometrics, or a code. Whenever employees need to access sensitive data within your network, this additional layer of security helps ensure that users are who they say they are.
- **Document and data management:** Make sure that you have backups of mission-critical data so you can restore it in the event of a breach. In addition, implement protocols for shredding sensitive documents or erasing private data on devices that are going to be recycled, donated or discarded.
- **Encryption of media:** If you've engaged encryption software, it's still up to staff to make sure that information stored on devices like laptops or USB drives is encrypted before it leaves the office.
- **Protection against inside attacks:** Efficient onboarding and offboarding protocols (that include immediately removing credentials and network access) should be carefully followed when employees leave the firm.
- **Heightened security awareness when traveling out of office:** Educate employees on the risks of accessing unsecured public networks as well as completing transactions that require accessing sensitive information in non-secure locations. If you store sensitive files on a server in your office or headquarters, setting up a Virtual Private Network (VPN) is a great option for accessing those files securely. A VPN provides a "cable-like" connection between your remote computer and your office server.

Implementing these policies and practices requires both education and consistent upkeep. But you don't have to go at it alone. You can seek training for staff at local chambers of commerce, accounting and bookkeeping community groups, accreditation bodies, and through app partners that offer it. Providing security training for your team is integral to a secure and resilient practice.

STEP 4: Advise your clients on security best practices

Many of the employee best practices and approaches that we discussed in Step 3 apply to your clients as well. But of course, adoption of these policies is much more complicated when you are trying to incentivize people outside your firm to play a role in your security plan.

A good strategy might be to invite clients to join you in building a culture of resiliency, while reminding them of the risks (outlined above) that threaten their data. You can then explain how behavior helps mitigate those risks.

For instance, ask them not to share any sensitive information with you via email or text. Or let them know you won't send them emails that require clicking on unsafe, external hyperlinks — so they can be on the lookout for phishing schemes masquerading as your firm.

Transparency and trust-building play a tremendous role in this process. You have to be upfront with clients about the plan and practices you have in place, so they know you are invested in the security of their private information. You should regularly update them as the plan evolves over time and immediately inform them if their data is ever compromised.

Of course, all these approaches require you to practice what you preach and become deeply committed to your firm's continuous development of cybersecurity measures. In doing so, you reduce your own liability and fulfill the obligations that require you to protect client access, identity, and data.

Sources:

Gartner — Rethink the Security & Risk Strategy

EDUCBA — Security Technologies

Federal Trade Commission — Cybersecurity For Small Business

Business News Daily — Cyberattacks and Your Small Business: A Primer for Cybersecurity

U.S. Chamber of Commerce — Internet Security Essentials for Business 2.0

Practice Protect — Accounting Cyber-Security Guide

McKinsey — Transforming Cybersecurity

Forbes — 5 Steps To Secure Your Customer Data

Data security as a firm differentiator

PART THREE

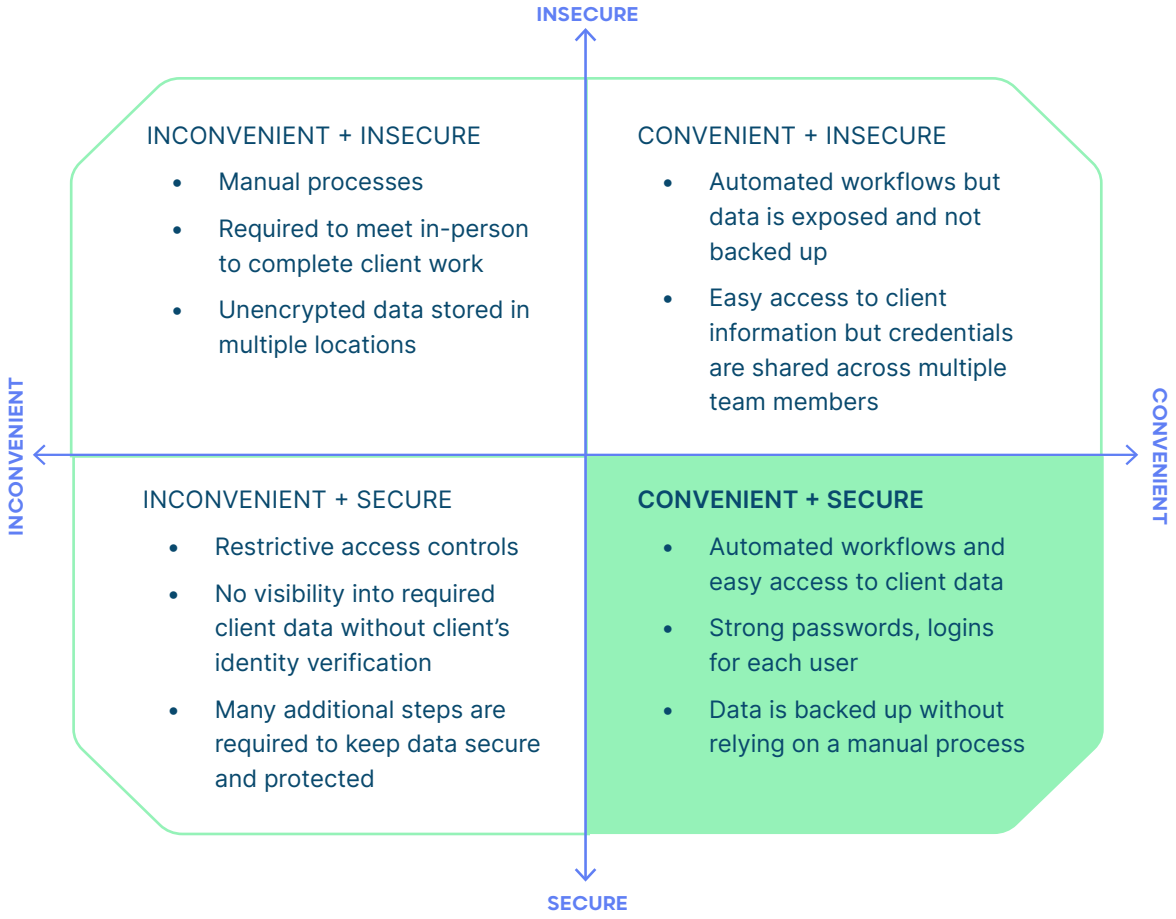
So far, we've covered the security landscape, the threats you face, your responsibilities as a firm, and security technology. But you may still struggle to put things into action. This is normal — cybersecurity can be overwhelming. As a result, many small businesses adopt a "head-in-the-sand" attitude to security. In a 2021 small business survey conducted by CNBC and Momentive, **42% of small businesses reported that they have no plan in place to respond to ransomware or a cyber attack.** More than 2 out of 3 respondents also reported having no cybersecurity insurance for their business.

If you are struggling to get started, we'd like to help you get through this hump. And one of the best ways to do it is to broaden your perspective about why you're getting more serious about cybersecurity. Yes, as accountants and bookkeepers, you are custodians of your clients' financial data, and the duty to be proactive falls on you. But in addition to meeting obligations, being proactive about security also brings benefits to your firm.

When done right, security coincides with convenience

You should aim for the right balance between security and convenience. This means following a process that gives you confidence about how you manage clients' data — and does so without slowing your firm down. Here's the good news: a lot of the tools that help secure your firm also make your firm *more* efficient, not less. (More on this in **Part 4**.)

For now, think about your firm: your daily activities, the type of client information you access, how you manage it, what you do with it, how many different applications and databases it touches, and how many people on your team and your clients' teams have access to it. Then look through the matrix below, and ask yourself, "Where does my firm land?"



Unfortunately, too many cloud accounting and bookkeeping firms ignore security and fall into the "Convenient + Insecure" category. They stay in that category because of the perception that increasing security also means introducing inconvenience at the firm. Having read this far, you should already know that this is far from the truth, and there are plenty of ways to run a practice that is both convenient and secure.

But if that's not enough, there's one more benefit to implementing strong security practices at your firm — it gives you more credibility.

Reinforcing your firm's credibility

Besides protecting your firm and your clients from potential breaches and liability risks, implementing strong data security procedures helps you differentiate your practice.

While not all small business clients may be aware of every specific cybersecurity threat, they are certainly sensitive to how their data is handled by advisors and other stakeholders. Since differentiation is often a challenge for accounting and bookkeeping firms, implementing data security best practices gives your firm another tool to position your expertise.

If you're not sure whether this is a viable differentiator for your firm and your target clients, you can run an assessment. The accountant-centric agency, Hinge Marketing, suggests that for a differentiator to matter, it should meet three criteria: it must be true, it must be important to your clients, and it must be provable.

Can you use data security to differentiate your firm?

- → Is it true? Do you have strong data security practices in place (or are planning to)?
- → Does it matter to your clients? Are they concerned about how their data is handled?
- → Can you prove it? Are there tools, apps, policies or behaviors that show your adherence to data security?

While this will not be important to every client, some will be very concerned about your data security policies. And even those who are on the fence stand to be swayed towards your firm due to the data security assurances that you can offer.

Sources: *CNBC | Momentive — Small Business Index Q3 2021*

Hinge Marketing — 21 Ways to Gain a Competitive Advantage for Your Firm

Solutions for an end-to-end data security stack

PART FOUR

So, how do you put everything into practice and ensure that you're keeping your clients' data secure? And how do you maintain the conveniences and advantages of cloud accounting at the same time?

In the past, firms relied on expensive IT consultants and other outsourced services to identify and mitigate potential data security risks. Today, the rapid adoption of cloud accounting has been accompanied by a rise in cybersecurity solutions and tools with built-in protection.

We cover three cybersecurity-centric tools in this section. Each one helps firms cover essential security pillars:

1. credential management
2. data backups
3. secure banking collaboration

Three tools for your cybersecurity stack

Practice Protect
MORE TRUST. LESS RISK.

Practice Protect, a data security platform built for accounting firms. Gain complete control over the access of client data and passwords within your business with enterprise-level automation, application security, and human powered support.

rewind

Rewind, which helps you ensure that your QuickBooks Online files are always protected and automatically backed up — allowing you to restore your entire file or individual items, including attachments, reports, expenses, and more.

relay

Relay, a business banking platform that lets you and your clients securely collaborate on banking. Issue logins for every user, set up permission levels, manage approvals, enable two-factor authentication, and rapidly respond to potential breaches.

More Trust, Less Risk with Practice Protect

Practice Protect
MORE TRUST. LESS RISK.

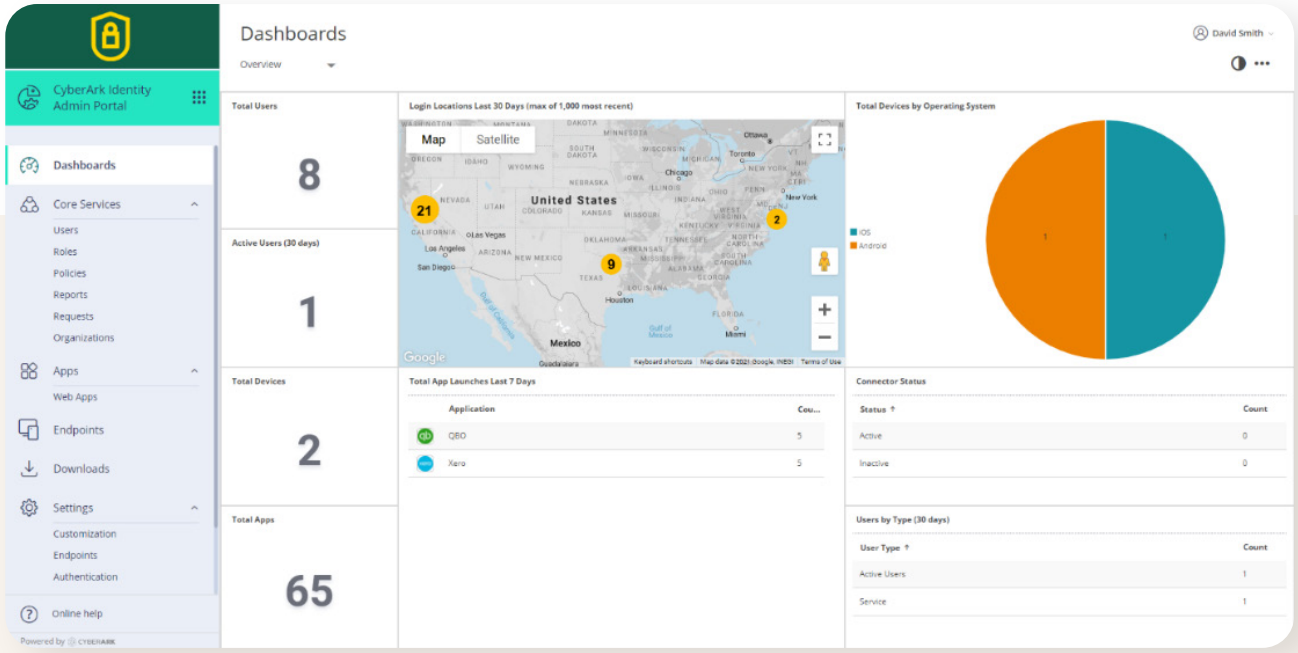
Your clients' data is the most important asset in your business. And keeping it secure is critical to maintaining relationships built on trust. Practice Protect gives accounting firms a comprehensive way to manage passwords, control access and protect data online. You can simplify your firm's security with a single portal for controlling all of your credentials — both internal ones and those used to access client data — suspicious activity alerts, advanced geo-locking and a complete audit trail.

Over 13,000 accountants use Practice Protect so they can:

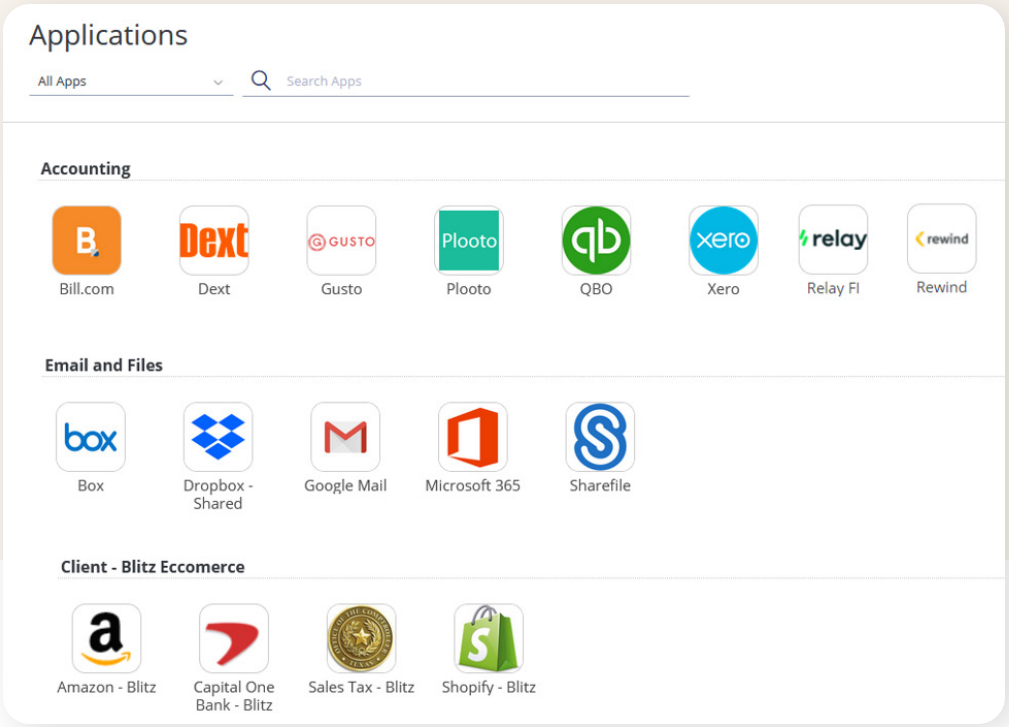
1. **HIRE WITH CONFIDENCE**
Get greater control and peace of mind as you add to your team. Built-in monitoring, IP-detection, and one-click lockout give you confidence to keep moving forward with growth.

2. **BUILD ELEVATED CLIENT TRUST**
Demonstrate due diligence as a responsible data custodian for clients and prospects. With Practice Protect, you can assure them that their banking information and sensitive data is safe in your hands with password safety policies and enterprise-grade encryption.

Usage Reports & IP Locks



Heightened Efficiency with Password Grouping



3. **GAIN BETTER CONTROL OVER CYBER SECURITY AND COMPLIANCE**
Secure your applications and email systems (G-Suite and Office 365 ready), boost cyber security standards and remain completely industry compliant.

4. **MANAGE REMOTE TEAMS MORE SECURELY**
Get peace of mind with work from home employees—built with decentralized teams in mind, Practice Protect offers password cloaking, advanced user permissions, and remote team policies.

5. **ENSURED CLOUD ACCOUNTING SAFETY**
Featuring over 6,000 cloud apps, Practice Protect is more than ready to support your firm's app stack.

Book a Demo of Practice Protect

Ensure data integrity with Rewind

90% of data breaches are caused by human error

Source: CybSafe — UK's Information Commissioner's Office (ICO) Analysis

45% of organizations that use SaaS apps have lost data

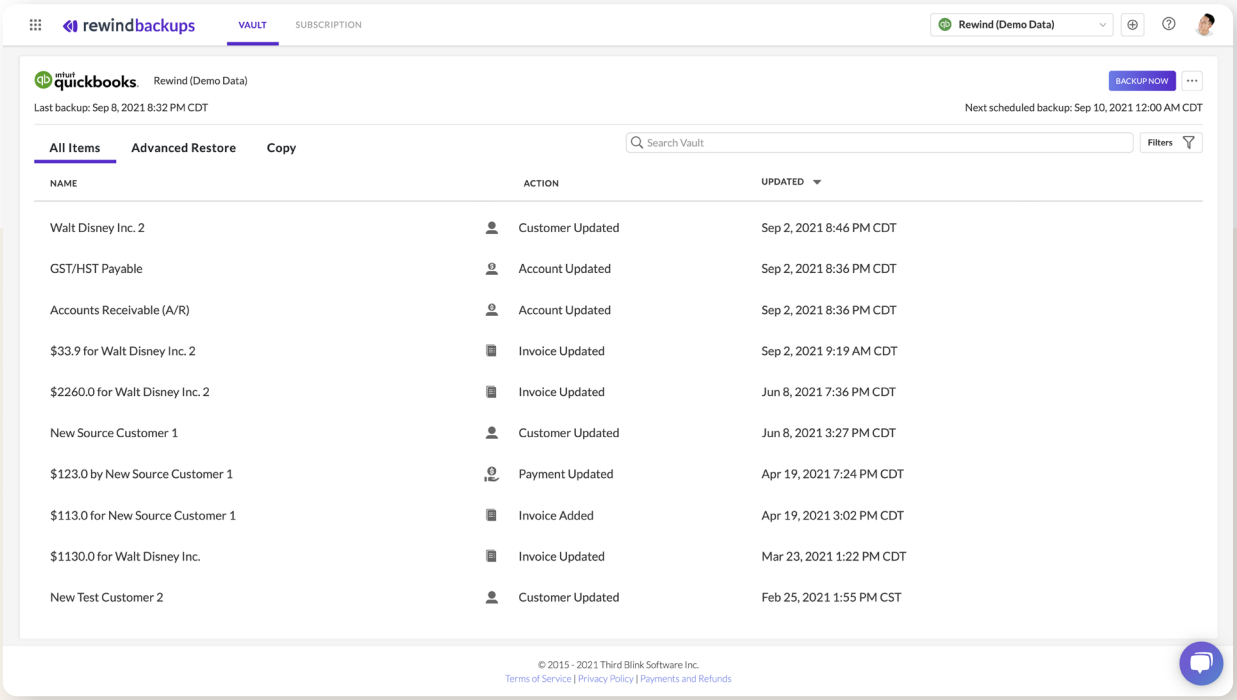
Source: Rewind — The Odds of Losing SaaS Data Come Down to A Coin Flip

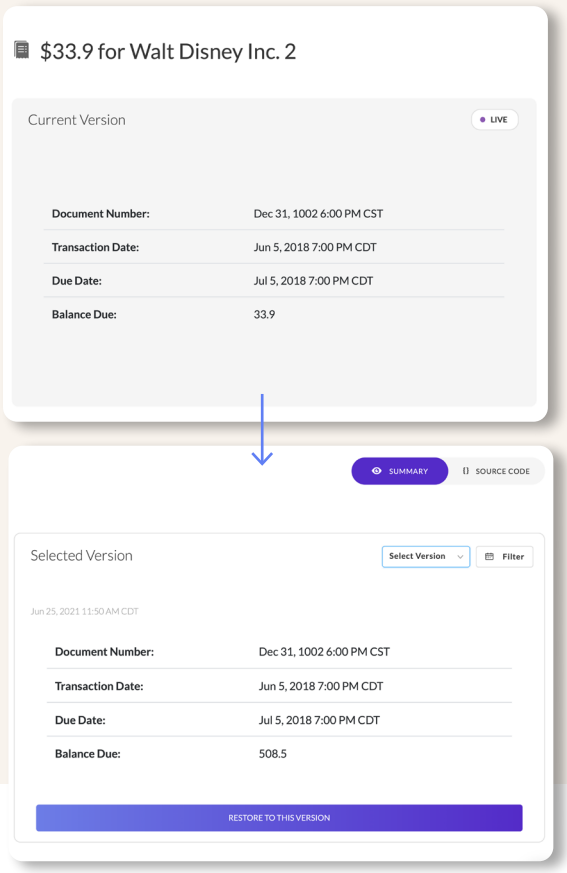
Rewind is an app that works natively within QuickBooks Online to back up your complete files automatically, every day. If a data disaster were to strike, Rewind can restore your files to exactly how they were at a previous point in time, minimizing lost time and potential revenue loss. It's like an insurance policy, but for your data: Rewind ensures that your sensitive data is always securely backed up (and ready to be restored, if need be). If your clients asked you today if their data was safe and secure, could you guarantee them anything? Implementing a security protocol will help provide that level of trust and differentiate you in the market.

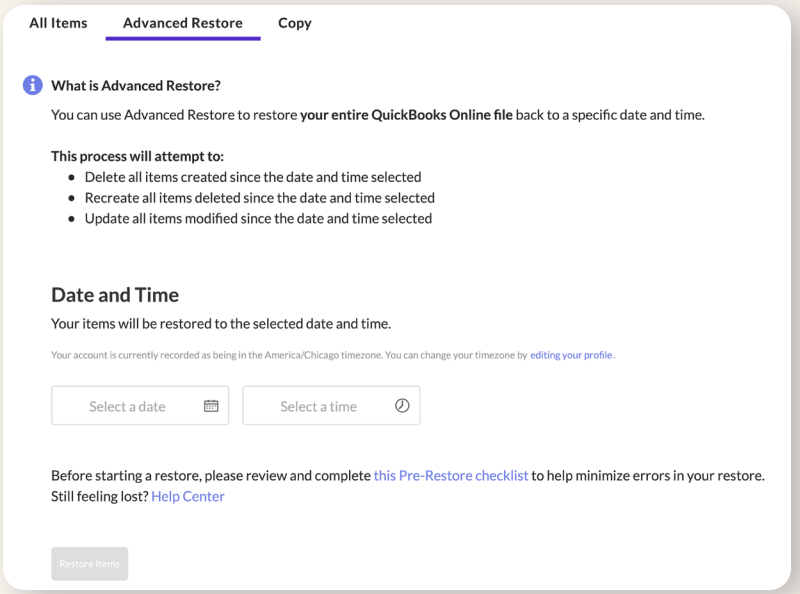
The Need for Cloud Backups

Many SaaS apps, including QuickBooks Online, don't provide account-level data backups or recovery. As a firm, you need assurances that the software and apps being used are keeping each client's sensitive information safe.

If a manual mistake is made, a buggy app is installed, or you become a victim of malware, your operation could come to a grinding halt as you deal with the fallout. With a robust data backup and recovery solution, your data remains safely at your fingertips.







Why Rewind?

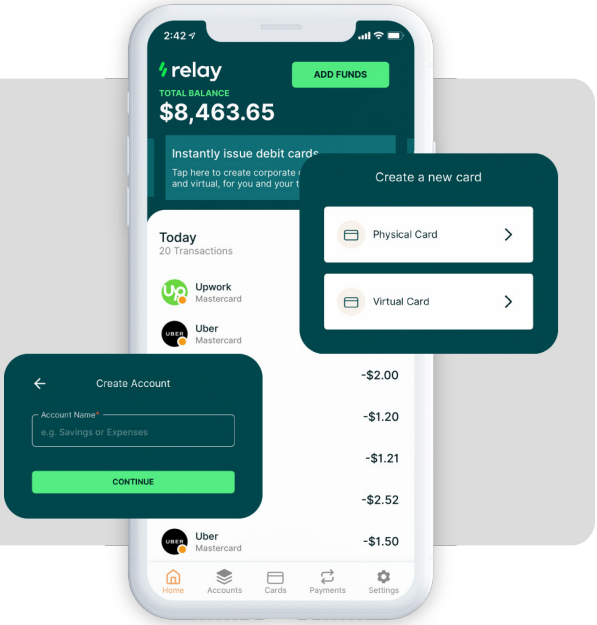
Rewind helps to usher in a new way of doing business - it brings automated daily backups and on-demand controlled data recovery. You don't want a minor setback to cost you by eating into the profitability of a company file or hurting the reputation of your practice. Rewind offers continuous backup coverage so no matter what the mistake was, you can recover your client file, down to a specific transaction to a point in time giving you on-demand data recovery. What was hours or weeks worth of manual work takes minutes with Rewind.

Rewind helps you say goodbye to making manual copies of client files, CSV exports or storing redundancies on hard drives. More importantly, gone are the days where accounting professionals do not have access to restoring client data in real-time. With Rewind, you get full access, control, and protection of the financial information that lives in a QuickBooks Online file.

Start your Free 7-Day Trial Today

Securely collaborate on banking through Relay

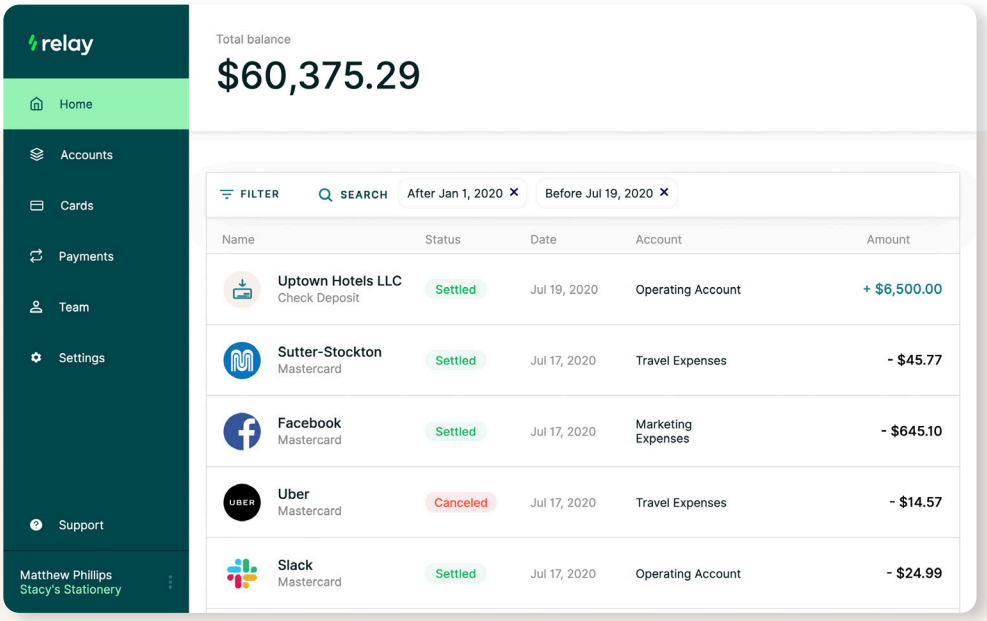
relay

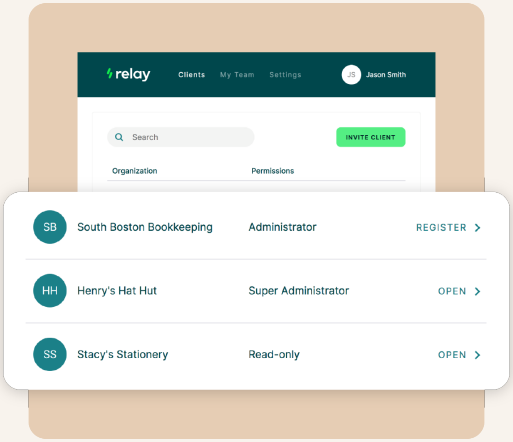


Relay is business banking that makes bookkeeping seamless. That means speeding up your workflows with direct, reliable bank feeds into QuickBooks Online and Xero, and securely collaborating on banking with your clients.

Every accountant and bookkeeper on Relay gets their own advisor portal, which lets them access multiple clients' banking from a single login. From there, advisors can pull statements and pay bills, as well as issue and use cards. Relay supports multiple users, enabling secure collaboration between business owners, their advisors, and their teams. Relay lets firms:

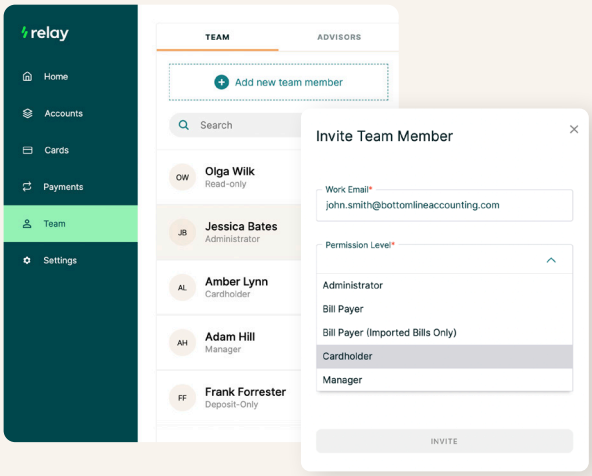
- Collaborate on banking with multiple clients through your own **Relay advisor portal**
- Control access to client banking with **role-based user permissions**
- Implement **financial controls** by setting spending limits on cards
- Automate spend management with **single- or multi-step approval rules**
- Issue login credentials and enable **2-factor authentication for every collaborator**





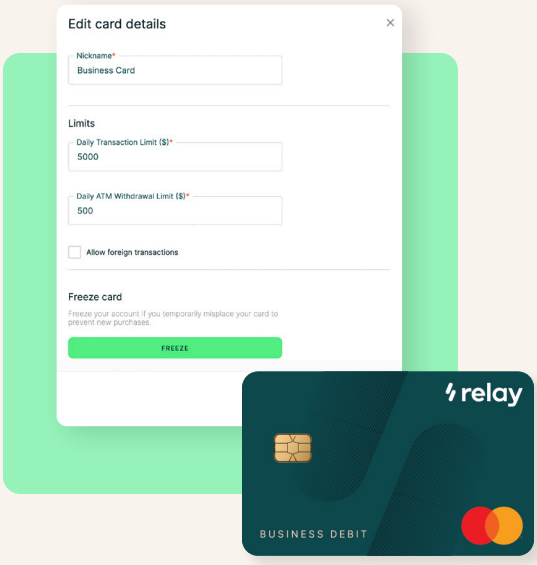
Switch between clients from your firm's portal

When your clients bank with Relay, you and your team can access their banking information securely from your advisor portal. Since every user gets their own login, you no longer have to hold on to the client's banking credentials. If your firm manages multiple clients, you also eliminate the need to switch between different bank accounts.



Eliminate risk with user permissions

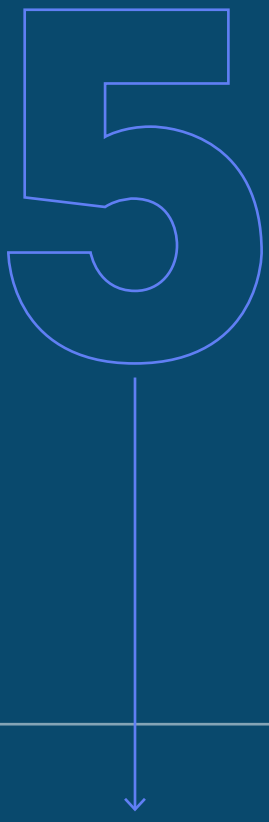
With Relay, you can further reduce risk by assigning each user a permission level based on their role in the business. Whether they are an administrator, need read-only access, just manage debit cards or bills — you can control the level of access each user gets.



Rapidly respond to threats and data breaches

Relay gives you and your clients the tools you need to both protect your business and respond to potential threats. You can secure each user's login with two-factor authentication, instantly freeze debit cards if credentials are ever stolen, and get a detailed paper trail if your data is ever breached.

Open a Free Relay Account



Checklist: am I handling my client's financial data securely?

PART FIVE

Implementing a data security stack can be a long process. Conducting a risk assessment of all your digital assets takes time, as does developing and executing your security plan. And of course, it's a process that you need to get right.

In the meantime, though, there are measures you can adopt almost immediately. **They will make your firm more secure in the short term, and set you up to implement your eventual security stack.** Take the assessment below, ticking the boxes for each thing your firm already does. By the end of the assessment, you'll have a better picture of your firm's security today, as well as any potential security gaps you may want to address.

ADVANCED PASSWORD USE

- [ ] Use strong, unique passwords for every account and update them regularly.
- [ ] Use a dedicated password manager — do not enable options to save or remember passwords on your devices.
- [ ] Never give out passwords or PIN numbers to co-workers or anyone else — including client bank login credentials.
- [ ] Enable multi-factor authentication to further protect access to secure networks or digital spaces that house sensitive data.

ENHANCED DEVICE SECURITY

- [ ] Require a password to unlock devices once they have entered sleep mode.
- [ ] Make sure all of your security software is up to date.
- [ ] Make sure all of your antivirus and antispyware tools are enabled.
- [ ] Limit login attempts, so that devices or accounts are locked if the wrong password is entered too many times.

INVEST IN PHYSICAL SECURITY

- [ ] Ensure that paper files are stored securely in locked rooms.
- [ ] Limit who has physical access to confidential documents.
- [ ] Track the storage of physical files over time, and shred paper copies that no longer need to be kept.

PROTECTION OF SENSITIVE DATA

- [ ] Understand how to identify suspicious attachments and links, so that malicious software isn't downloaded.
- [ ] Never give out sensitive information, over the phone, through email, or via other unsecured mediums.
- [ ] Know how to watch out for phishing indicators, like alarmist messages, requests for sensitive information, or misspelled words.
- [ ] Look out for indicators that websites are secure (via the web address or URL) before inputting sensitive data.

AWARENESS WHEN TRAVELING/AWAY FROM THE OFFICE

- [ ] Choose the most secure options when accessing public Wi-Fi.
- [ ] Never engage in transactions that access sensitive data over unsecured networks.
- [ ] Encrypt confidential data on all devices — especially information that is sent outside your firm to a client or contact.

EMPLOYEE TRAINING

- [ ] Introduce current and new employees to all security practices you're implementing (password use, device security, etc.) both in-person and via email or internal intranet.
- [ ] Inform employees of the response plan should a security breach occur.

Sources:

Federal Trade Commission — Cybersecurity For Small Business

U.S. Chamber of Commerce — Internet Security Essentials for Business 2.0

Practice Protect — Accounting Cyber-Security Guide

BONUS: USE BEST-IN-CLASS SECURITY SOFTWARE

- → Use Relay to securely collaborate with clients on banking.
- → Use Rewind to keep your QuickBooks Online data backed up.
- → Use Practice Protect to securely manage passwords and train staff.

relay Practice Protect MORE TRUST. LESS RISK. rewind

Conclusion:

Build your data security plan with confidence

You now have a foundation for understanding what it means to practice security at your firm, as well as the tools to ensure that you're protecting your clients. Understanding the risks and your obligations as an advisor is just the beginning — the next step is implementing them.

Start by assessing your firm's security preparedness with our 6-part checkup. As soon as you implement a few quick wins, your firm will already be ahead of many others.

And while there are no guarantees when it comes to security, advisors have a responsibility to make sure they stay aware of the evolving data security landscape. Now that you are equipped with the latest information and best practices, you're ready to build your cybersecurity plan and advise clients with more confidence.

In partnership with

relay

Relay is business banking that makes bookkeeping easy, designed to help you securely collaborate on banking with your clients. Relay automates AP, simplifies expense management, and auto-syncs enriched data directly to QuickBooks Online and Xero.

Open a free account to make banking collaboration more secure and up to 5x more efficient.

Learn More

Practice Protect
MORE TRUST. LESS RISK.

Practice Protect is a data security platform for accounting firms. The platform gives you complete control over client data and passwords, guarding against threats with more trust and less risk.

Learn how to protect your firm and your clients with a leading security platform.

Learn More

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.

Join the 80,000+ organizations who trust Rewind to protect their cloud data.

Learn More