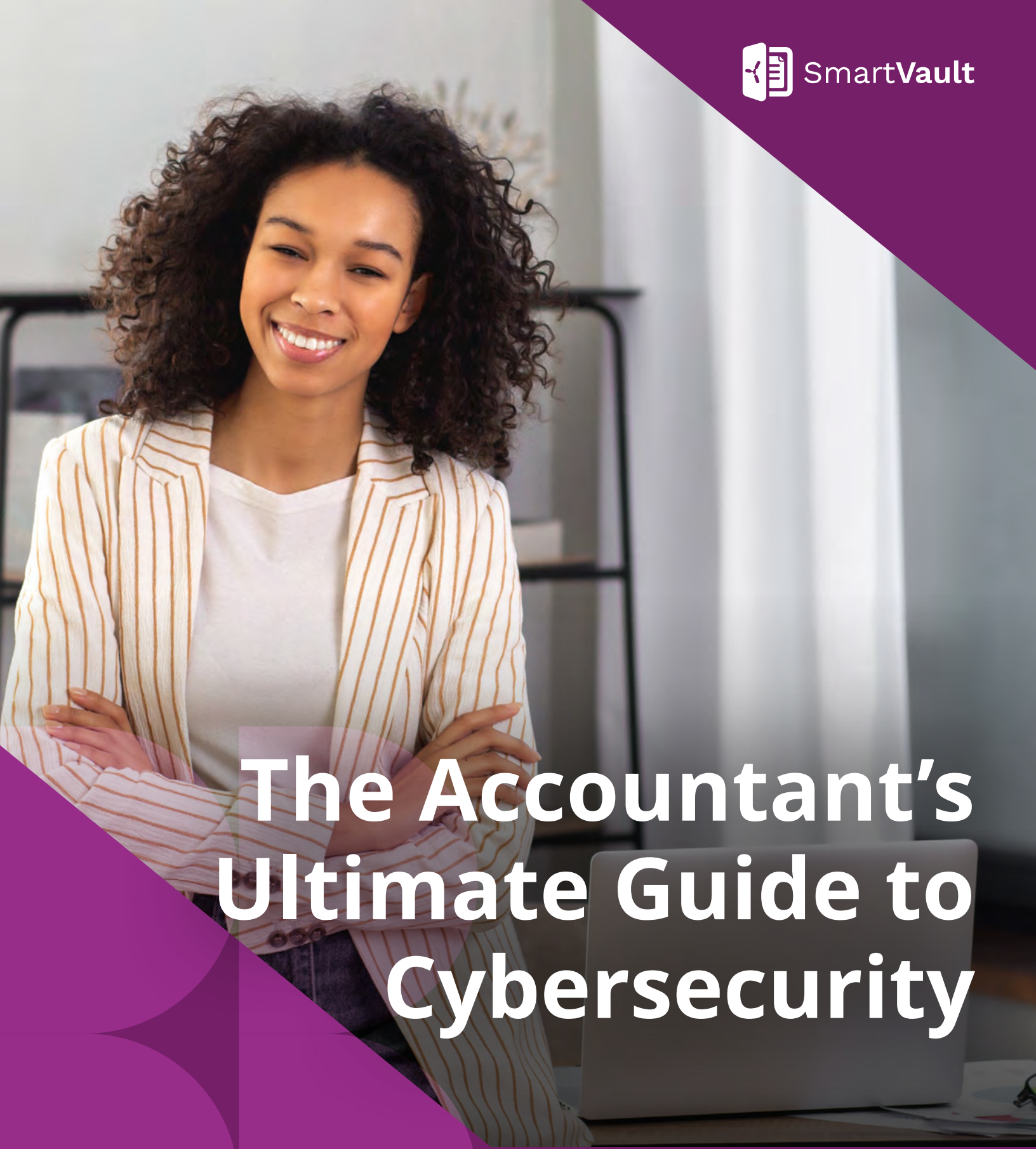
SmartVault



The Accountant's Ultimate Guide to Cybersecurity

Introduction

Clever cyber thieves have cost Americans millions of dollars, and while some traps might be easier to spot than others, it's best to stay on your guard – anyone, even the most vigilant person, can be fooled. Regardless of your firm size or who your clients are, this comprehensive guide will teach you about cybersecurity and actions you can implement to proactively protect your data. Here's a breakdown of what you'll learn in each chapter:

CHAPTER 3

CHAPTER 4

CHAPTER 5

CHAPTER 1

Cybersecurity Must be a Priority, and Here's Why

All businesses are susceptible to attacks, but some are at higher risk simply because of what they do and the clients they serve. Unfortunately, accounting and tax professionals fall into that high-risk category. And, if you're a smaller firm, you're at an even greater risk of being targeted by a cyber thief.

> **"It may seem counterintuitive, but the risk of cyberattacks is disproportionately higher for smaller and medium-sized organizations, which tend to be much more reactive than proactive,"**
>
> says Vijay Rathour, partner in the Digital Forensic Group.

Cybercriminals think that small and medium-sized firms are easier to hack since they often lack the sophisticated cybersecurity programs larger businesses have, like virus detection software and dedicated IT teams.

It can be easy to overlook cybersecurity and think you'll never be a victim to an attack. Don't make that mistake at your firm. "Identity thieves always seem to find a hook to lure victims, and we increasingly see tax professionals as a target given the sensitive client data they handle," warns IRS Commissioner Chuck Rettig.

Your Risks of a Breach Are Increasing

Cyberattacks, tax fraud, and scams are rampant, and each year, criminals only get bolder and cleverer. Unfortunately, the costs to accountants and taxpayers are enormous. Here's an example to put "enormous" into perspective: The government estimates billions of dollars were stolen by fraudsters from programs meant to help taxpayers during the pandemic. In fact, they're calling the massive amount of theft "the biggest fraud in a generation."

Worse still, reports have shown that scams are on the rise: there were eight million reports of tax scams and fraud, according to the 2022 Annual Report of the Identity Theft Tax Refund Fraud Information Sharing Mission and Analysis center. This number is **four times greater than the number of reports in 2021,** and it's not expected to drop anytime soon. "The number of attacks is large and increasing, both in volume and sophistication, and has expanded to...more complex tax scams," the report claims.

One of the most sophisticated schemes is recent: In March 2023, a federal grand jury indicted a group of seven individuals who allegedly filed over 370 false tax returns and attempted to claim over $110 million in tax refunds using stolen identities. The criminals used their victims' information to register with the IRS and change their victims' mailing addresses. They then accessed their tax information, like tax transcripts and wage records, and used the information to electronically file tax returns and claim fraudulent refunds.

Cybersecurity Stats

Just How Damaging Are Cyberattacks and Criminals?

There were **8 million reports** of tax scams and fraud in 2022 (ISAC)

In 2022, the IRS found more than **$31 billion was lost** to tax fraud and financial crimes (IRS)

On average, every **11 seconds**, a company is victim to a ransomware attack (Cyber Security Ventures)

95% of breaches are caused by human error (World Economic Forum)

The average cost of a data breach in the United States in 2022 was over **$9.4 million** and over $5 million in the UK (IBM)

22 billion records were exposed in 2021 breaches (RiskBased Security)

Over 70% of US tax-filing adults are concerned about data breaches when filing income taxes online (PC Mag Tax Survey 2021)

In 2020, malware **increased by 358%** and ransomware by **435%**, compared to 2019 (Help Net Security)

Your Clients Expect Data Security

Your clients trust you to keep their information safe. When you take proactive steps to protect data, it shows potential and current clients that you take data security seriously. This builds trust and credibility, which can lead to increased referrals, higher loyalty and retention, and more positive reviews. It also gives you a competitive advantage. Clients are more likely to choose a firm that prioritizes their privacy and security over one that does not.

In fact, taxpayers have high expectations for secure, online collaboration with their tax professionals, according to Intuit's 2022 Taxpayer Insights & Intelligence Brief. The report found that:

> **73%** want a secure place to upload documentation to their tax professional throughout the year
>
> **86%** expect their tax documents and information to be stored with industry-standard security
>
> **74%** expect to send their personal, sensitive data via a secure transfer

How can you meet these expectations? Your accounting tech stack should include a secure document management system and client portal. *We'll learn more about using technology to increase cybersecurity measures in Chapter 5.*

You Must Comply With the Law

Cybersecurity isn't just a matter of doing what's best for your clients and business. It's also about compliance: Tax and accounting professionals are legally obligated to secure their data from breaches.

The Federal Trade Commission requires paid tax and accounting professionals to have a robust data security plan called a Written Information Security Plan (WISP). Firms are also required to comply with portions of the Gramm-Leach-Bliley (GLB) Act, which requires you to outline how you will protect your clients' personal information. Firms that fail to comply may lose their business licenses and damage their reputation. *We'll talk more about these and exactly what you need for compliance in Chapter 3.*

And then there are the financial penalties: Section 7216 of the Internal Revenue Code (IRC) imposes criminal penalties on tax preparers who make unauthorized disclosures or uses of information furnished to them in connection with the preparation of an income tax return. IRC Section 6713 imposes monetary penalties on the unauthorized disclosures or uses of taxpayer information by any person engaged in the business of preparing or providing services in connection with the preparation of tax returns.

Don't risk your business and clients' livelihood by ignoring cybersecurity mandates. And as we just covered throughout this chapter, you can face a myriad of severe issues, such as permanent loss of trust in your firm, untold amounts of lost profits, and financial consequences, if you don't take cybersecurity seriously.

Ahead in Chapter 2

Learn four common ways cyber criminals access data, as well as the current tax scams accountants should be aware of and how you might (unknowingly) be putting your firm's data at risk.

CHAPTER 2

Understand What Makes Your Firm Vulnerable

You are the first line of defense when it comes to protecting your firm's and clients' data. The most effective way to safeguard it is to understand how criminals can access it and how vulnerable your firm is.

Common Attacks and Vulnerabilities

So, what's meant by "vulnerability?" Luke Kiely, a law enforcement veteran and SmartVault's Chief Information Security Officer, says it refers to what a criminal needs to exploit to get what they want. There are attacks that can happen to anyone and any industry, but there are also scams specific to tax and accounting professionals. Let's take a look at this further.

4 Common Ways Cybercriminals Access Data

Picturing some clever hacker in a dark room writing lines and lines of code, *Matrix-style*? That's actually not the case. All it takes to get into your system these days is a credit card and knowledge of where to buy the right software. Hackers can buy software online to do the job for them, and a breach can happen overnight. Mostly, though, it takes days, weeks, or even months for an attempt to be successful or discovered. To ensure you notice when someone is trying to hack into your system, be aware of the common methods. They include:

Malware

Cybercriminals design malware — short for malicious software — to steal your data and destroy and/or damage your computers and systems. Infections typically happen from clicking on a link or opening an infected email attachment. Malware includes things like viruses, spyware, and ransomware.

In the *Journal of Accountancy*, cybersecurity expert Vijay Rathour warned, "Malware can infect your system on Monday, map out every other computer it can reach through the network, and will encrypt every file it can access ...By the time you come into the office on Wednesday, your entire business has been immobilized. And that's when you get a message demanding ransom."

Ransomware

That brings us to ransomware. This is a type of malware that makes its victims pay — literally. Ransomware keeps you from accessing your data by encrypting your files, making them unreadable. The criminals give you an ultimatum: Pay up or lose the data indefinitely. Some attackers even demand a second ransom with the promise they won't sell your data online to other criminals. Ransomware is a final step in a larger attack, as the criminal already accessed your network and data through an initial method, like malware or phishing.

Phishing

This type of attack lures people into disclosing their personal information, like passwords and Social Security numbers, and it works well. An estimated 91% of all data breaches and attacks begin with a phishing email, according to the IRS. Criminals accomplish this by making the victim believe the message and request are trustworthy. These attempts are usually performed via email or text message and appear to come from known, trusted sources, like your partner, client, bank, loan provider, credit card company, or even places like big-box stores.

Man-in-the-Middle (MitM)

Also known as eavesdropping, a perpetrator puts themselves between you and an application (i.e., your mobile device and its Internet browser). The victim is completely unaware that all the information they're passing to the application is going straight to the perpetrator. The attacker may even install software to access all of your information. People put themselves at risk for this when they connect to the Internet using an unsecure public Wi-Fi.

Scams Specific to Tax and Accounting Professionals

In 2022, the IRS found more than $31 billion was lost to tax fraud and financial crimes. And while attacks can happen any time of the year, criminals tend to take advantage of the busy season. Hackers know you'll be distracted as you work around the clock to meet deadlines. Plus, they know the volume of documents exchanged between tax professionals and clients increases astronomically during tax season, making it the perfect time for criminals to attack.

Here are three common ways criminals scam tax firms and their clients:

1 Sending texts and emails claiming to be from the government and demanding immediate action.

One popular trick scammers use occurs via text, email, and even social media. They frequently contain links or attachments, and they often come with panic-inducing threats, such as demanding immediate payments to avoid being arrested. The IRS and state tax agencies will only ever contact you by mail. They do not call, email, direct message (DM), or text. Getting any one of these messages is a red flag.

2 Stealing taxpayers' identities and applying for fraudulent unemployment benefits.

If your client filed for unemployment but hasn't received the benefits, this may be because a scammer has stolen their identity and ensured the money is sent to their account. This is called "Claim Hijacking" or "Claim Account Takeover." Another red flag: You or your client receive notices saying they filed for unemployment, but they never did. They may even receive unemployment benefits they never asked for. When this happens, criminals make sure they also receive a 1099-G tax form to include the benefits on their tax returns.

3 Stealing tax refunds.

Michael Dexter Little, who was sentenced to nearly 20 years in prison in January 2022, filed false tax returns with the names and information of his victims. He obtained at least $12.3 million in fraudulent tax refunds. And, as we saw in chapter 1, he's not the only one. This scam is extremely popular and leaves millions of hardworking taxpayers high and dry each year. With this ages-old scheme, thieves will steal your identity, file a W-2 in your name, and then have your tax refund deposited into their account. To make things worse, they don't necessarily have to contact you to get the information they need.

4 Ways Firms Put Data at Risk

Cybersecurity is ultimately about the people. Everyone must recognize and embrace their roles and responsibilities in protecting themselves (and others) online.

Here are four common ways firms put their data at risk of attack:

1 Avoiding System Updates

Too many people increase their vulnerability by ignoring or postponing software updates on their devices. Even though updates can be time-consuming and frustrating, they're necessary because viruses and malware change and adapt all the time. And, if you work in a regulated industry, you're very likely to find yourself staring down the barrel of compliance issues if your system is breached.

2 Not Training Staff

Patrick Schreiner, a business cybersecurity risk advisor at one of America's Big Three Index Fund Managers, says untrained staff are a big source of mistakes that result in data breaches. He warns that cyberattacks frequently start when someone clicks a malicious link in an email or downloads an attachment. Luke Kiely, Chief Information Security Officer at SmartVault, agrees, and he recommends that you remind your team members to examine things like emails carefully.

Consider these tips: Phishing emails often have odd reply addresses, strangely worded content, and a sense of urgency – hackers frequently try to push people into responding hastily in order to get what they want. Ask yourself, 'Am I likely to get an email from a CEO asking to make a change to a bank account at 5pm on a Friday?' Kiely suggests. And, if one of your team members believes they might have made a mistake, it's crucial that they don't wait to tell you.

Remember the Bangladeshi bank that was infiltrated by hackers and robbed to the tune of $1 billion back in 2016? The attackers were able to get into the bank's system by sending in applications for open jobs and including viruses in downloadable files disguised as resumes. While this is an outsized example, it illustrates the point Schreiner wants to emphasize: People – not firewalls and other digital security measures – are always the weakest link. But there's good news: "The strongest link is ALSO the person. Reporting a suspicious email to your IT department may alert them to remove it from other colleagues' inboxes, help update their spam filters, and learn the tactics of attackers."

3 Not Following Simple Best Practices

Make good security hygiene a regular part of your routine. Use strong, long, complex passwords in addition to multi-factor authentication (or MFA). “MFA in general is a really easy win for a lot of people... [because it can] prevent bad actors from accessing your accounts even if they have your password,” says Schreiner. You should also protect yourself against malware by installing recognized, commercial antivirus software.

4 Using Email to Share Sensitive Data

Email is one of the most common and riskiest tools used in businesses today. This is because emails are mostly sent in clear text and move from server to server after you press send. Anyone with know-how can intercept and read your emails. Some hackers even gain access to the servers themselves, meaning they can read every email that has been stored in it – even if it was sent a few years ago.

Many of the documents that accountants require for tax returns include at least one data point that should never be sent via email. These include:

- Bank and financial account numbers
- Credit and debit card numbers
- Social Security numbers
- Income information
- Passport numbers
- Driver’s license numbers
- Personal health information
- Passwords or login information

Tip: Strong Data Security
Protecting your business and client data is a large obligation to meet. Use a cloud-based document management system and client portal to securely send files and confidently protect your data. We’ll talk more about this powerful technology in Chapter 5.

Form W-2, for example, has the person’s name, Social Security number, address, income, and more. This gives criminals exactly what they need to steal identities or make money selling the information to other criminals.

Know the Signs

Warnings You've Been Hacked

You could be hacked and not even know it. According to the IRS, here are some common signs that you're a victim of an attack.

You receive e-file acknowledgments for tax returns you have yet to file or you receive more acknowledgments than returns you've filed.

Your clients received a tax transcript that they didn't request or a message that someone created an online IRS account for them.

Clients contact you about or respond to emails or other requests that you didn't send.

Your clients tell you the IRS sent them authentication letters or a refund even though you haven't filed their tax return yet.

Your computer starts acting slow, unresponsive, or strange, including software taking longer to load, the cursor moving without you touching the mouse, and/or it locks you out of your computer or network.

Your clients receive a message that someone has accessed their online account or that the IRS disabled their online account.

The IRS rejects your client's e-filed return because they've already received another return with their Social Security Number.

Protect Your Data: Complete a Risk Assessment

So, how can you keep your firm safe from these threats? Start by completing a risk assessment. This is an appraisal of your practice's ability to keep itself from falling prey to a cybercrime and will help you identify, evaluate, and prioritize areas where your cybersecurity measures are leaving you vulnerable to an attack.

Know What Data You Have

The first step is knowing what you need to protect. Even though everyone is aware that they need to protect themselves against cyberthieves, Luke Kiely says firm leaders' biggest problem is that they're not always aware that their biggest asset is data. "You need to know what you're protecting," he cautions.

Make a list of the data you handle. The IRS recommends this categorization:

Personally Identifiable Information	Name & Contact Information	Personal Characteristics & Health/Insurance Information	Financial Data & Employment Information
• Social Security # • State-issued ID # • Driver's license # • Passport # • Mother's Maiden • Name Credit history • Criminal history	• Initials • Address Telephone number • E-mail address • Mobile number • Date of birth • EFINs / PTINs / CAF#	• Age • Gender • Marital status • Nationality • Insurance account # • Prescriptions • Medicare and Medicaid information	• Credit, ATM, debit card # • Bank Accounts • Security/Access • Codes • Passwords • Income/Salary • Service fees • Compensation info • Background check info

Map Where Your Data is and Where It Goes

Now that you know what information your firm has, you need to pay attention to how you're handling it. That means looking at the software and hardware you use, as well as evaluating your current operations. Think about your teams, both in-house and virtual, and the contractors or vendors who have access.

Review the flow of information you receive about and from your clients. Document as much as possible about how it is cared for, stored, and accessed. Is it online, offline, locally, or in the cloud?

Identify all potential points of failure in your workflow, systems, and personnel. For example, if your business stores all vital information in only one place, what would happen if the method you use to access it failed or was destroyed?

Let's say you have everything saved on an encrypted hard drive, but suddenly, that computer is infected with ransomware and everything is lost. Could you recover the data from another secure backup? What would happen if you couldn't?

This also applies to people. Perhaps your bookkeeper is the only one who knows vital or sensitive information about a client. If that person leaves your company, how would you recover those details — or would they just be lost?

Risk Assessment Worksheet

This worksheet is designed to help you assess what you need to address within your firm. Once you have identified any weaknesses, it will help you create an action plan to address them.

Answer Yes or No to the questions below to see how vulnerable your firm is today.

Policies	YES	NO
Are you operating without a designated employee responsible for cybersecurity programs?	☐	☐
Are you operating without a mobile device security policy?	☐	☐
Are you operating without a remote working policy?	☐	☐
Are you operating without a plan of action for what to do in the event of a cyber security breach?	☐	☐
Are you operating without adequate cybersecurity insurance?	☐	☐

Hardware/Software	YES	NO
Does your office use hardware that's more than 5 years old (computers, routers, modems, firewalls)?	☐	☐
Is there a newer version available of your firm's computer and mobile device operating systems and/or key software that has not yet been updated or is obsolete?	☐	☐

Password Management	YES	NO
Do staff members store login credentials on spreadsheets, written notes, or other unprotected methods?	☐	☐
Do your staff and/or clients share the same login credentials to access software or shared devices?	☐	☐
Do staff members use the same password for multiple logins?	☐	☐

Email	YES	NO
Does your firm request or share documents with clients and others using unencrypted email?	☐	☐
Do you think your staff would fail to recognize cybersecurity threats, including phishing emails?	☐	☐

File Sharing & Storage	YES	NO
Do staff or management ever use public Wi-Fi to access confidential information without additional security protection?	☐	☐
Does your firm store sensitive/confidential information on local hard drives, servers or removable storage (USB drives) without encryption?	☐	☐

Scoring

Count how many questions you answered 'Yes.'

1-3 Low Vulnerability	4-6 Moderate Vulnerability	7-14 High Vulnerability

Ahead in Chapter 3

Learn the best ways to develop a strong cybersecurity program, including a deep dive into creating a high-quality cybersecurity program that will lower your vulnerability and meet legal requirements.

SmartVault

CHAPTER 3

How to Develop a Strong Cybersecurity Program

Now that you have a better understanding of what risks your firm faces, it's time to create a robust cybersecurity program. Like we said in Chapter 1, the FTC requires paid tax and accounting professionals to have a Written Information Security Plan (WISP). Before we dive into WISP requirements, however, let's go over some best practices for keeping your data safe.

5 Best Cybersecurity Practices

There isn't a one-size-fits-all approach, but there are best practices that everyone should follow. Here are the top 5 that you should consider as your create your cybersecurity plan:

Use strong, unique passwords with at least 12 characters.

The strongest passwords have letters, symbols, and numbers. It's also important not to use the same password across multiple devices or accounts. You can use a password manager to help you remember unique passwords or you can use "passphrases." These short sentences or phrases can mean something special to you, like iLove_Snick3rs!

Keep all hardware and software updated.

If you fail to update your devices, browsers, software, and so on, you're vulnerable to malware and ransomware infections. Upgrade your modems, routers, hardware firewalls, and computer CPUs at least every 3-5 years. Make sure your team configures devices to automatically update.

Recognize and report phishing attempts.

The most common way hackers get your information is by sending you malicious links that look real but are hiding something malicious. These links can be embedded in emails, social media posts, private messages, texts, pop-ups, and more. They may ask for things like credit card numbers or bank account passwords. Some have links or attachments to download.

If something looks odd — it has misspellings or weird punctuation — or is even slightly suspicious, you and your team should promptly report it, delete it, and block the sender. Here are some signs a link may be a phishing attempt:

- The message is threatening or urgent
- There is weird spacing, bad grammar, or misspellings
- The email address has misspellings or doesn't match the display name
- It requests personal information or for you to complete a strange business request
- The offer is too good to be true

Be aware of social engineering.

This is a very common type of attack that tricks the victim into completing a request or providing personal information. The attacker pretends to be someone they're not, like your manager, team member, or even a friend or family member. They may contact you online (email, social media, etc.) or through phone calls.

Be wary of public Wi-Fi.

While it's great to empower your staff to work remotely, using public Wi-Fi can lead to serious consequences, like man-in-the-middle cyberattacks. If you must use public Wi-Fi, limit what you do online and don't log into your critical software or accounts. Using a personal hotspot or a virtual private network (VPN) is the most secure way to work in public areas like your library, café, or coffee shop.

Create a Compliant WISP

As we discussed in Chapter 1, the Gramm-Leach-Bliley Act (GLBA) requires financial institutions to protect client data. When the FTC implemented the GLBA, it also issued the Safeguards Rule, which is a list of requirements financial institutions, including tax and accounting firms, must follow. The FTC requires firms to:

- Choose at least one employee to coordinate their information security program
- Identify and assess risks to their clients' data
- Evaluate the effectiveness of their current safeguarding measures
- Create, implement, monitor, and routinely test a safeguarding program
- Ensure vendors and service providers maintain appropriate safeguards
- Update the program as needed (like when business operations or regulations change)

To help tax and accounting professionals accomplish the above tasks, the IRS joined forces with 42 state tax agencies and various members of the tax community to create the Security Summit.

So, What's in a WISP?

When writing your WISP, consider your practice's size, complexity, and scope. A large firm will have a longer, more robust plan than a smaller accounting firm, so there isn't a one-size-fits-all approach. However, there are three key areas each WISP should include:

- Employee management and training
- Information systems and technology
- Detecting and managing system failures

Here is the WISP outline the Security Summit recommends:

1. Define the objectives, purpose, and scope of your WISP
2. Designate who is responsible for creating, coordinating, and implementing your program, as well as list your authorized staff, their responsibilities, and what data they can access
3. Assess current risks and detail the types of information your firm handles, if you have any areas of potential data loss, and how you monitor and test these risks
4. List the hardware you use for work and where each piece is located (on the cloud, in your primary office, at a staff member's home, etc.)
5. Detail your Employee Code of Conduct and safety policies, including those for:
   - Data collection, retention, and disclosure
   - User access, both on site and remote
   - Network protection, Wi-Fi access, and connected devices
   - Electronic data exchange
   - Reportable incidents
6. Include a signed implementation clause that states when you executed the WISP

Checklist: Create a Compliant WISP

Download this free checklist to learn more about each section and confirm you're writing a compliant WISP.

DOWNLOAD THE CHECKLIST

Don’t Forget a Disaster Recovery Plan

While the word “disaster” might make you think of once-in-a-generation weather events and other freak scenarios only the most cautious worry about, it could be caused by something much more ubiquitous: a power outage, for example.

> **Tip: Automatic Data Backup**
> You won’t lose anything to natural disasters, power failures, or human errors if you use a document management system (DMS) with automatic data backup. We’ll cover this in more detail in Chapter 5.

Regardless of the cause, a disaster is a significant interruption and often means lost data and extensive money and time spent restoring everything. And you’re likely to experience at least one disaster during the life of your business. While exact estimates vary, most experts agree that the majority of companies – between 70% and 96% – were affected by an event that resulted in data loss in the last three years.

That’s why every firm needs a disaster recovery plan (DRP). A DRP is your blueprint for responding to unplanned events. Accounting practices without DRPs waste time trying to figure out the best path forward. They also must make quick decisions because they typically don’t have time to thoroughly think through each option when they’re facing an emergency.

Disaster Recovery Worksheet

You must consider everything from how you'll communicate with employees and clients to data backup and recovery. Use the prompts in this worksheet to get started. Make sure you designate an Owner who will help ensure each action item is completed.

Employee Safety

ACTION ITEM	OWNER	NOTES
Determine the best channel for communication to your staff. Could be text, phone, email or a team collaboration tool like Slack.		
Store employee contact information in a cloud-based system that you can access remotely.		
Establish an owner for team communication. It is helpful to assign primary and secondary roles for this task if possible.		

PHYSICAL LOCATION	OWNER	NOTES
Establish an owner who can access the physical location of the business to evaluate physical and/or network damage and determine safety and accessibility by employees.		
Store contact information for your building manager or landlord in a cloud-based solution so it's accessible in the event you need to report damage.		
Establish an owner for team communication. It is helpful to assign primary and secondary roles for this task if possible.		
Store all of your business insurance policy information in a cloud-based solution that you can access remotely in the event you need to file a claim.		
Establish systems and processes that support employees working remotely until it is safe to return to the physical location. Give employees laptops or tablets, use cloud-based systems so they can log-in remotely and work (if they are able), and establish a communication channel that can support remote employees (i.e. cloud-based email or team collaboration systems like Slack).		

DATA BACKUP & RECOVERY	OWNER	NOTES
Create a data map. This is a critical component of your business continuity planning. At minimum, you need a list of all of the systems you use today, what information is stored on each system (client and business data) and who can access these systems (both as admins and as users).		
Evaluate the risk of using a local storage solution versus a cloud based system. To start, think about how your business operations would be impacted if your entire office was destroyed. Would you be able to access a backup of your data? Can you carry out basic business operations?		
If you store data locally, make sure you are storing a backup of all your data in a second, offsite secure location. Restore from your backup to test the integrity of the stored data.		
In the event of data loss, a procedure needs to be established that supports industry compliance regulations with regards to notification to clients as well as third parties.		
If you have adopted cloud-based services*to store data, make sure you review security access and permissions for your staff and your clients on these systems at least twice a year. Adopting cloud-based services ensures your data is backed up and accessible by employees and clients from a browser or mobile device.		

CLIENT COMMUNICATION	OWNER	NOTES
Determine your channels of communication to clients. These can include email, your website or a recorded phone message on your business line.		
Draft a basic communication strategy that you can easily execute remotely. • Can you send an email to your client base? • Do you have the ability to record a phone message from a remote location? • Do you know how to update your website with an emergency message? The primary goal is to set expectations with clients you support letting them know if they can expect a delay or disruption in the service you provide, and whether it is safe to access your office as a result of the disaster.		
Establish the designated owner responsible for executing the communication strategy, and ensure the systems are in place to support the execution from a remote location. It is helpful to have primary and secondary roles if possible.		

The Ultimate Cybersecurity Program Checklist

Following this checklist will help you build a robust cybersecurity program with everything you've learned in this guide and more. The goal is to create a program that protects your firm and clients' data from hackers.

Step 1

Understand Cybersecurity Basics

Knowledge is key. Before you create new processes, you must understand the basics.

- Learn general cybersecurity facts and the common ways cybercriminals gain access to data (malware, phishing, man-in-the-middle, ransomware, etc.)
- Understand your obligations to comply with legal, regulatory, and industry mandates, including state data protection legislation
- Stay updated on cybersecurity threats/risks and regularly review, test, and update your program to meet the latest recommendations

Step 2

Evaluate Your Risks and Current Workflows

When you have a general understanding of cybersecurity, you can determine your practice's unique risks. Then:

- Designate at least one employee who is responsible for your cybersecurity program
- Identify vulnerabilities and risks that are specific to your firm, such as unauthorized access, loss of data, and use/disclosure of information
- Create an inventory of all the devices and hardware your practice uses to handle data (i.e., desktop computers, cell phones, routers, printers, etc.), including what you use each for and where they're located
- List the data your business handles, including both physical, hardcopy data and electronic data
- Review your Business Continuity Plan to define potential data loss scenarios (i.e., a computer is stolen or hacked, data is corrupted, hard-copy paper files are destroyed in a fire, etc.) and outline how you monitor, test, and respond to these risks and threats

Step 3

Create a Cybersecurity Program

Take what you learned from the previous steps to create a strong cybersecurity program. Your program should, at a minimum, document everything below:

Data Collection and Retention

- Identify how much data you store and for how long, where and how you store that data, and who has access to the data
- Review the flow of data, from when you receive it to when you're ready to store it
- Document as many details as possible about how your data is cared for and accessed
- Identify all potential points of failure in your workflow
- Ensure all data is encrypted in transit and at rest
- Don't use emails to send or request sensitive data
- Implement a secure document management system to request, send, and store data in the cloud

Data Backup

- Identify what data you need to back up (the information your business couldn't function without)
- Keep your backup data separate from your computer or network by using an external hard drive, USB, or, ideally, the cloud
- Consider a vendor for cloud storage that provides automated data backup, follows strict security measures, and helps ensure you don't lose your data to a disaster, cyberattack, or human error

Destroying or Deleting Data

- Destroy or remove data from computers, CDs, USBs, cells, and other electronic devices before you dispose of them
- Shred paper documents that contain sensitive information

Data Disclosure

- List the third-party companies that access your data and why
- Define requirements for third-party data access (i.e., 2FA, password requirements, etc.)
- Describe how you evaluate and confirm that third parties meet privacy standards
- Comply with IRC Regulations like Sections 7216 and 6713 for unauthorized disclosure

User and Remote Access

- Set access permissions based on employee roles and ensure your vendors provide strong access control options
- Require 2FA or, better still, MFA
- Create a process for unsuccessful login lockouts
- Develop a remote access policy

Network Protection

Define user protocols and requirements:

- Require passwords to have 12+ characters (a mix of letters, symbols, and numbers)
- Set passwords to expire regularly and ensure your vendors have appropriate password requirements and policies
- Remind employees not to use the same password for multiple devices or accounts
- Do not leave passwords or credentials on sticky notes, notebooks, etc.
- Consider using a password manager program to track passwords
- Require employees to lock computers before stepping away from their desks
- Remind employees to report suspicious emails, texts, or phone calls

Describe the process for adding new devices or software to your network:

- Confirm that all devices meet security requirements
- Designate an employee who approves each new software or device
- Develop a strategy for preventing staff from downloading risky apps
- Describe how you monitor computer systems for hackers or unauthorized access
- Use firewall protection, anti-virus, anti-malware, and other security software that updates automatically
- Ensure vendors automatically install patches that resolve software vulnerabilities
- Change the default admin passwords on your routers
- Require staff to install updates as needed on their hardware, computers, and devices
- Remind employees not to use public wi-fi for work
- Track activity across your documents, including who has accessed the data and when

Incident Response

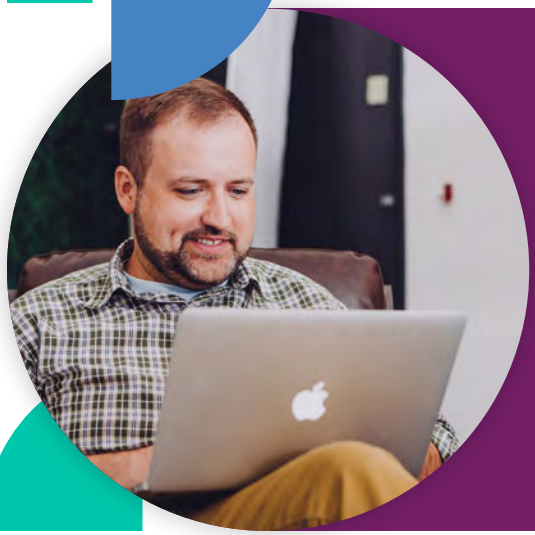
- Create an incident response team with clear assignments, objectives, and responsibilities
- Develop a framework that outlines action items and procedures
- Document information about external resources and how/when to notify the appropriate persons of the data breach, like your staff, clients, the IRS, the FTC, FBI, local law enforcement, etc.
- Describe steps to re-secure devices, passwords, network, and data
- Develop a continuity plan

Step 4

Ensure Employees Follow Processes

Employee Training

- Create a training program based on your cybersecurity program
- Require staff (full-time, contractors, and temp workers) to read the program and complete training during onboarding and at least twice each year
- Regularly remind employees of your policy and their legal obligation to protect customer data
- Ensure all employees pass a background check and submit references
- Develop and implement non-disclosure agreements and privacy guidelines
- Ensure terminated or separated employees do not continue having access to network and data



Ahead in Chapter 4

Learn how to share your cybersecurity plans with your clients to build their trust, as well as learn ways to stay updated on the cybersecurity threats of tomorrow without having to become an IT expert.

CHAPTER 4

What Happens After You Implement Your Cybersecurity Plan?

Once you've implemented your new cybersecurity program and trained your staff, it's time to bring your clients in. Additionally, you'll need to make sure you stay updated as new cybersecurity threats emerge.

Sharing Your Security Plan With Clients

Letting your clients know you have carefully considered processes in place will make them feel safer and help you build a relationship based on trust with them. And don't just verbally tell them about it – create a shortened, to-the-point data plan they can read for themselves and share with others. That way, they'll retain the information better and have the opportunity to look up your processes and reassure themselves you took every possible precaution. Hopefully, they will also refer you to other clients and strengthen that reference by sharing your plan with them.

> Feel free to use the flyer on the following page to get started. *Note it was written for firms who use* SmartVault's document management system and client portal.

Safeguarding Your Data is Our Priority

You trust us with a lot of personal information. These are some of the ways we keep your data safe.

We Follow Best Practices

We stay updated on the latest recommendations and risks, and we regularly educate our staff so they can confidently recognize cyberattack attempts, such as phishing emails or malware links. Our team is also trained on and required to follow best practices around document management, network protection, password creation and usage, and more.

We Actively Mitigate Risks

We've reviewed the flow of information throughout its journey—from the moment you begin sharing information with us to when we've finished the project. We identified the hardware and software we use, where it's located, who has access to it, and what vulnerabilities we face. We also determined ways to mitigate these risks, including requiring staff to regularly change their passwords and update their computers and software.

We Secure Everything in the Cloud

On the cloud, your data is encrypted—which means it's scrambled and unreadable—during transit and while at rest. We also control who accesses each piece of data. Approved users must verify their identity via two-factor authentication to access it. We can also see exactly what's happening, like who created, accessed, downloaded, and deleted documents. And automatic data back up means we won't lose anything to natural disasters, power failures, or human errors.

We Collaborate Safely Online

It's risky to share documents with sensitive information, such as financial or personal details, through emails. Our client portal allows us to safely share files with each other, and it gives you access to them whenever you need them and from wherever you're located. This helps us keep your data secure with the highest safeguards.

Plan for Today and Tomorrow

It's not enough to plan for risks you're aware of right now: Technology changes quickly, and if you don't stay current, cyberthieves will remain one step ahead of you. Keeping your data secure means planning for the threats of today and tomorrow.

But you're not an IT professional. Your tech knowledge is limited to certain things, and you don't have time to be sitting there trolling the Internet, looking for cybercrime news that won't necessarily translate to a non-tech person. So, how can you stay updated?

Stay Updated on Cybersecurity Threats

Here are three simple ways to ensure you don't miss information that's vital to updating your cybersecurity program:

1 Follow experts on Twitter and LinkedIn.

This is an easy way to make sure you're up-to-date on the latest cybersecurity news. Experts in the field post to LinkedIn and Twitter all the time and are the first to know when it comes to new threats. You'll likely also find educational videos that they post on their YouTube channels and be able to get information that previously would only have been available if you attended tech conferences. You can find experts through a simple Google search, but here are a few you should check out:

- Brian Krebs, investigative journalist and author of cybersecurity blog krebsonsecurity.com, which is updated daily
- Andy Greenberg, writer for WIRED, whose pieces frequently focus on cybersecurity and who is a recognized expert
- Graham Cluley, a researcher, host of the Smashing Security podcast, and writer whose daily blog, grahamcluley.com, offers cybersecurity tips for readers
- (Bonus) See hundreds of articles, webinars, and other resources about security and other imperative topics in SmartVault's Resource Center.

2 Talk to your fellow accountants.

When it comes to getting information that's particularly relevant to your profession, there's nobody better to talk to than another accountant. As you develop your cybersecurity program, reach out to your network to find out what others have been dealing with and how they decided to tackle the problem. Many accounting and finance experts are easy to reach, a phenomenon unique to this small profession. People who frequently talk about their tech stack, like Dawn Brolin and Randy Johnston, will also have information on fraud, scams, and cyber threats that are targeted at accountants and their clients.

3 Speak to your tech vendors.

In addition to communicating with other accountants, don't forget to speak with your tech vendors about cybersecurity. Remember: Since it's their products you're using to keep your data safe and since their reputations are incumbent on their solutions being as secure as possible, they'll be up to date on the latest risks and will be able to help you maximize their solution to ensure you're not vulnerable.

Ahead in Chapter 5

See how a document management system will enhance your cybersecurity, as well as how to find the right vendor and integrate the solution into your tech stack.

SmartVault

CHAPTER 5

Why a Document Management System and Client Portal Are Essential to Cybersecurity

Accounting practices will continue to face stronger security and compliance scrutiny by clients and regulators in the future. A document management system (DMS) that's built with security and compliance in mind will ensure your firm retains client trust, keeps data safe, and adheres to IRS regulations.

How a DMS Increases Data Security

We've covered a lot in this comprehensive guide. A sure-fire way to increase your cybersecurity and accomplish most of the best practices we've learned is to implement a DMS and client portal at your firm. A top-of-the-line document management system will solve many security issues by taking the following measures:

1 Encrypting data during transit and while at rest.

When sensitive data is at rest or being exchanged over the internet, it's crucial that your data is encrypted every step of the way so no one can hijack your information and use it for malicious purposes. By using advanced encryption methods such as SSL and AES-256, a cloud DMS could provide stronger protection for your data.

2 Providing controlled access to information.

How your information is stored and who has access to it is critical to your overall security and compliance framework. With a security and compliance-first cloud-based DMS, you can set granular access permissions to folders and documents, and allow access to files via authenticated logins. These security and compliance steps help enhance your data and document security measures, which could increase your level of compliance to regulations.

3 Offering secure data backup.

Your documents and metadata are always stored using highly redundant replicated storage. Multiple copies of metadata and documents are stored in multiple geographical locations and backed up regularly to ensure data availability.

4 Tracking all activity

An activity log is an automatically generated, time-stamped trail of all activities that happened in your document management system. It tracks all events from all users such as document creation, download, and deletion and generates an audit trail of what's happening in your account. No person, including the engineers of the platform, can make any changes to this trail, making it the authoritative record for auditing purposes. This feature is a requirement from several industry-specific compliance regulations. Depending on your industry, it could very well be the single most important determining factor during your cloud DMS vendor selection process.

Evaluate Tech and Vendors

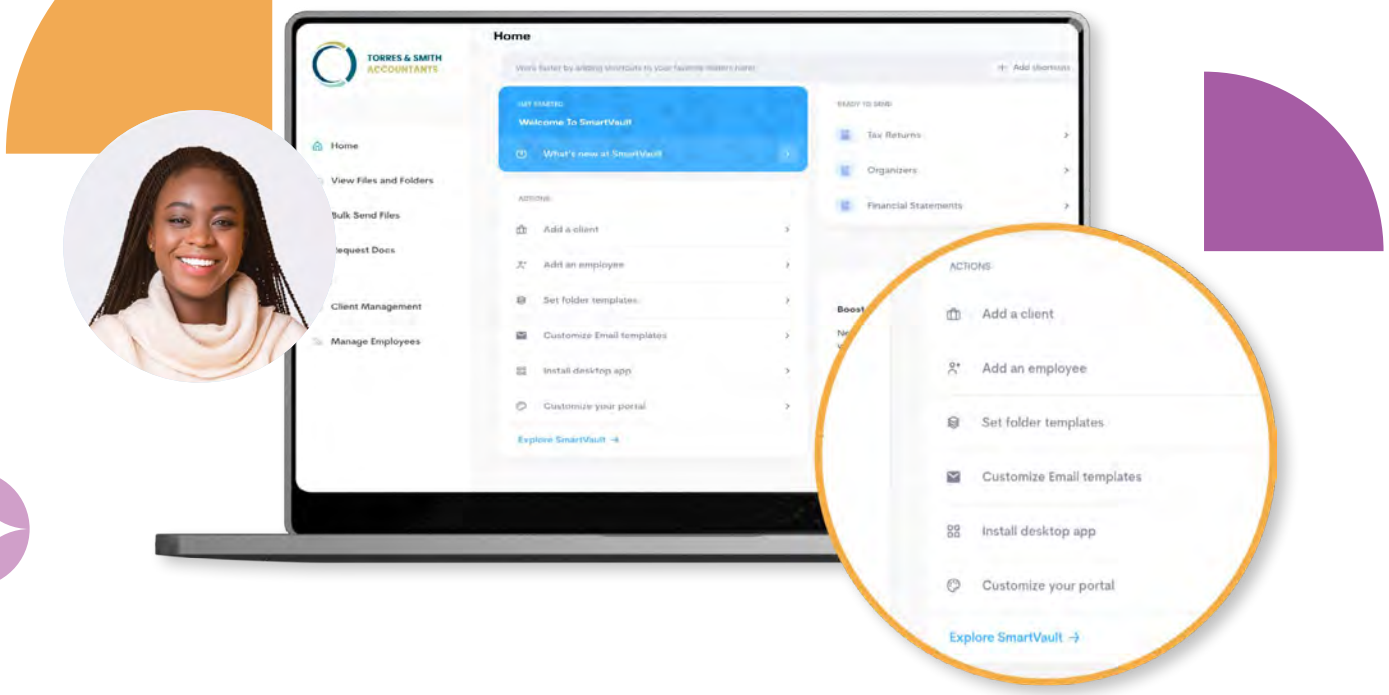
When researching document management systems, start by looking at comparison/review sites. You should also do an online search and ask your network of peers what they use or recommend. Consider who will use the technology and how. Don't forget to also consider security requirements and how the DMS will help you comply with certain regulations.

Make a list of the 'must-have' features and how they support your business goals. You'll also need to consider how the DMS will fit into or impact your current tech stack. This includes integration with the other apps you use today. And, of course, you'll want to consider price and what else the vendor offers. You'll want a partner who can help you configure the DMS to your needs and set you up for success. Confirm they offer services like:

- A dedicated Customer Success Manager
- Onboarding and system configurations, including migrating data as applicable
- A detailed knowledge base with training resources, webinars, and "How To" guides and articles, as well as an academy
- Personalized, live, one-on-one training sessions to get you up and running
- System usage reviews that include suggestions for improvement based on your unique needs.

Once you've chosen the top 2-3 finalists, consider doing a trial of the solutions to see them in action. You can select a few staff (or clients) to use it too and provide their feedback. When the trial periods are over, you should choose the DMS for your practice and move ahead to implementation and training.

SmartVault



Allow SmartVault to Manage Document Security for You

SmartVault is the easiest and most secure way to optimize how you, your staff, and your clients gather, store, share, and eSign documents in the cloud.

Implement document storage that scales with you
Enjoy unlimited storage and users in a central document cloud storage for your internal and client documents. Quickly find the file you need, when you need it, and share it securely with the right people.

Manage documents through a secure, branded portal
Give clients an easy and professional way to view, upload, and download documents from a portal that's accessible anytime, from anywhere, and on any browser.

Simplify how you request, gather, and track documents
Create and send request lists to clients, whether it's one or 1,000. Receive notifications, have full visibility, and manage all documents in one place. SmartVault automatically routes files to the right folder.

Boost efficiency with automated workflows
Scan, drag and drop, or upload files in seconds. Integrate with Lacerte, ProSeries, QuickBooks, Microsoft Office, DocuSign, and more to streamline tasks, save time, and focus on higher-level initiatives.

SmartVault

Facilitate fast and easy document esignature
Streamline multiparty collaboration and allow clients to sign forms and contracts from their desktops, laptops, or mobile devices. Send documents for eSignature and receive signed documents back in the same folder.

Gather, organize, and then share files securely
Built with bank-level security, all documents stored in and shared from SmartVault are encrypted – both in transit and at rest. Manage advanced user permissions so only authorized persons have access.

Don't stress about compliance and security
SmartVault supports compliance with major worldwide regulations, like HIPAA, GDPR, FINRA, SEC, GLBA, CCPA, and more.

> **"I estimate that we've boosted efficiency during tax season by at least 90% since implementing SmartVault... I used to survive during tax season. Now, I operate much more efficiently."**

Michael J. Yuda, CPA

More Features to Power Your Business

- Scanner Integration
- Connected Desktop
- Full Text Search
- Email Alerts
- Version Control
- Automatic File Lock
- PDF Printer
- Bank-Level Security
- Compliance Tools
- Activity Reports
- Tax and Accounting App Integration
- Customizable Folder Templates
- Mail Merge and Email Templates
- Autofiler
- Fillable Form Tool
- Quoting Tool