rightworks



eBook

All things cybersecurity: The ultimate guide for the modern accountant



Table of contents

03. Intro
- Why cybersecurity is important for accounting firms
- Why your firm needs a cybersecurity strategy
- Stats about growing cyberthreats
- Purpose of this guide

04. Basics of cybersecurity
- Key definition
- Types of cyberthreats
- Defining terminology

08. Current threats/common challenges facing firms
- Data breaches
- Compliance issues
- Client data protection
- Remote work vulnerabilities
- Outdated software
- Lack of encryption
- Lack of processes and security policies
- Misconceptions about new tech

14. Importance of data security
- Understanding data security
- Why data security matters
- Consequences of poor data security

17. Essential cybersecurity measures
- Risk assessment
- Data encryption
- Access controls
- Network security
- Employee training
- WISP

30. Best practices for cybersecurity in accounting firms
- Regular software updates and patch management
- Secure client communication channels
- Data backup strategies
- Third-party partnerships

34. Legal and regulatory compliance
- Understanding relevant regulations
- Compliance best practices
- Penalties for non-compliance

39. Tools and solutions for cybersecurity
- Essential tools for accountants
- Advanced tools for enhanced protection
- A secure cloud solution for The Modern Firm®

44. Real-world case studies
- When impersonation attacks strike
- From local storage to secure cloud
- When client security affects your business

Intro: The ultimate guide to cybersecurity and accounting

When you hear the word *cybersecurity*, some of the following terms likely come to mind: data security, encryption, antivirus, malware, multifactor authentication, the cloud, networks, device protection, compliance…and the list goes on.

It's a lot. And it's overwhelming. Enough so that you might find yourself in a state of information paralysis. You know you need to take the necessary steps to ensure your firm is safeguarded against cyberthreats. You know you have compliance requirements you have to meet. But maybe you're unsure of where to start, who to ask for help, what you need to know and how to ensure you've done enough.

Cybersecurity isn't just a nice-to-have technical consideration; it is a fundamental and essential requirement for the success—and survival—of your firm.

As trusted advisors and custodians of your clients' sensitive financial and personally identifiable information (PII), your firm is a prime target for cybercriminals. The question isn't *whether* your firm will face a cyberattack, but *when*.

And the bigger question: How prepared are you?

The importance of cybersecurity for accounting firms

With cyberthreats rapidly evolving and accounting firms on the front lines, it's more important than ever that your clients know they can trust you to protect their PII and safeguard their financial data. Knowing that a single data breach can lead to severe financial loss, legal consequences and irreparable damage to your firm's reputation only solidifies the need for prioritizing cybersecurity. Your client relationships are built on trust, and cybersecurity is just another component of the valuable services you provide.

The necessity for a comprehensive cybersecurity strategy…and culture

Basic protective measures like antivirus and firewalls are no longer sufficient when it comes to your firm's cybersecurity strategy. It's no secret that cyberthreats and bad actors are growing increasingly sophisticated every day. To ensure the safety of your firm, you must be proactive and adopt a comprehensive cybersecurity strategy that includes robust security protocols, continuous monitoring, staff training, redundant backups and regular system updates—just to name a few. It's complex and it's a lot to handle. That's why your cybersecurity strategy must also include creating a culture of security awareness and preparedness across the firm.

The rising tide of cyberthreats: A few statistics

Here are some eye-opening statistics from the **Verizon 2024 Data Breach Investigations Report** that underscore the urgency for accounting firms to implement robust cybersecurity measures and trust experts to handle it for you:

- **Cyberattacks are on the rise.** When combined, ransomware and other extortion techniques show a strong rise and represent 32% of all breaches.
- **Misconfigured security is costly.** Professional error—employees misconfiguring security—was the cause in 28% of breaches.
- **"Human element" is the most common factor.** The human element—for instance, someone clicking on a malware link—was present in 82% of breaches.

And here are some additional numbers to consider. Among 240 accounting professionals who responded to a **June 2024 CPA Practice Advisor/Canopy survey**:

- **15%** have experienced a security breach.
- **49%** allow clients to email sensitive information, such as tax forms, to their firm.
- The two most common causes of security breaches were **"clicked a wrong link"** (compromised or malicious) and **"ransomware."**



Purpose of this guide

This comprehensive eBook is designed to equip your accounting firm with the knowledge and tools necessary to navigate the complex world of cybersecurity. We aim to demystify the challenges and provide actionable insights to help you understand and bolster your firm's security posture.

Whether you're a small practice or a large firm, this guide will walk you through the world of cybersecurity in an easily digestible way and offer strategies, best practices and resources to make cybersecurity manageable and effective.

Ready to find peace of mind and empower your firm to confidently face the cyberthreats of today and tomorrow? Let's dive in…

Section 1

Basics of cybersecurity

Cybersecurity 101: What every accounting firm needs to know to stay safe

Accounting firms are treasure troves of PII and sensitive financial data. Protecting your firm—and your clients' data—from cyberthreats should be at the top of your priority list. But where do you start? Don't worry; we've got you covered. Let's start at the beginning and break down the basics of cybersecurity.

What is cybersecurity?

The Cybersecurity & Infrastructure Security Agency (CISA) defines cybersecurity as "the art of protecting networks, devices and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity and availability of information." Basically, it's protecting your computers, devices, networks and data from bad actors (i.e., hackers and cybercriminals).

These digital "bad guys" are out to steal information, disrupt your services and even hold your data hostage. For accounting firms, this means you must defend your client data, financial records and other sensitive information from falling into the wrong hands. Think of cybersecurity as a multilayered digital shield that helps your firm stay protected in an increasingly connected world.

Types of cyberthreats

Let's talk about the numerous cyberthreats that exist. Unfortunately, there are several ways your firm could suffer from a cyberattack. Knowing what to look for is half the battle. So, we've put together a fun quiz to break down some common cyberthreats. Let's see what you know.



Cybersecurity: The act of protecting your computers, devices, networks and data from bad actors.

FILL IN THE BLANK QUIZ

How well do you know your cyberthreats?

1. _____ is a general term for any kind of malicious software that can damage or infiltrate your system. It's hidden in email attachments, web downloads or even fake updates. Once it's inside your system, it can steal your data, spy on you or lock you out.

a. Malware **b. Smishing** **c. Phishing**

Example: A hacker tricks an employee into downloading a program disguised as tax software, which gives them access to all your clients' PII.

2. _____ is when someone tricks you into giving up confidential information or performing an action (e.g., sending money or buying gift cards). Bad actors pretend to be trusted clients or partners and ask for sensitive details.

a. Vishing **b. Social engineering** **c. Zero-day exploit**

Example: A cybercriminal poses as a senior executive, urgently asking you for access to client files, which, in turn, hands over access to your firm's system.

3. _____ occurs when hackers send legitimate-looking emails or messages, intending to trick you into clicking a malicious link or providing personal information.

a. Phishing **b. Denial-of-Service (DoS) attack** **c. Password attacks**

Example: You receive an email that appears to be a password reset, but the link leads to a fake website designed to steal login credentials.

4. _____, also known as voice fishing, is similar to phishing, but it happens over the phone. A hacker may call, pretending to be someone from your bank, firm or another trusted institution, hoping you'll share sensitive details.

a. Smishing **b. Phishing** **c. Vishing**

Example: A scammer calls, claiming to be from your bank, demanding accounting information to "resolve an issue."

5. _____, or SMS phishing, uses text messages to trick victims into clicking malicious links or sharing personal data.

a. Smishing **b. Social engineering** **c. Malware**

Example: You receive an unprompted text message with a link, asking you to verify account information through the provided link that's designed to steal your information.

6. _____ is when hackers secretly intercept and sometimes alter communications between two parties. It's essentially like someone eavesdropping on a private conversation without either party knowing.

a. Denial-of-Service (DoS) attack **b. Password attacks** **c. Man-in-the-Middle (MitM) attack**

Example: A hacker intercepts communications between your firm and a client using an unsecured Wi-Fi connection, which gives them access to sensitive financial data.

7. _____ flood your firm's website or network with traffic, making it impossible for legitimate users to access.

a. Password attacks **b. Denial-of-Service (DoS) attacks** **c. Phishing attacks**

Example: Your firm's website goes down during tax season because a hacker bombarded your servers with traffic, preventing clients from accessing important documents and ensuring operations grind to a halt.

8. _____ occur when bad actors take advantage of a vulnerability in software that hasn't yet been fixed by the developer. They're especially dangerous because no solutions are immediately available.

a. Zero-day exploits **b. Vishing** **c. Social engineering**

Example: Hackers discover a flaw in your accounting software before a developer can release a patch, leaving your firm exposed.

9. _____ happen when hackers attempt to crack or guess your passwords to gain unauthorized access to your system.

a. Malware **b. Smishing** **c. Password attacks**

Example: A hacker uses automated tools to repeatedly guess your firm's password until they crack it, giving them access to sensitive financial data.

ANSWERS KEY: 1. a. Malware 2. b. Social engineering 3. a. Phishing 4. c. Vishing 5. a. Smishing 6. c. Man-in-the-Middle (MitM) attack 7. b. Denial-of-Service (DoS) attack 8. a. Zero-day exploits 9. c. Password attacks

Cybersecurity terminology you need to know

Now that you're familiar with cyberthreats, let's break down some essential cybersecurity tools and terms. The items below are the building blocks of a solid defense strategy.

- **Antivirus:** A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents.
- **Data breach:** The result of a hacker successfully breaking into a system and gaining control of its network. Data, like PII, credit card numbers and bank account numbers, are usually exposed.
- **Data encryption:** Encryption converts your data into a scrambled or 'secret' code that can only be read by someone with the decryption key. This ensures that your data will be unreadable even if hackers get their hands on it.
- **Endpoint detection and response (EDR):** A cybersecurity technology that monitors and protects your firm's devices from cyberthreats. EDRs can detect and block threats, contain them and even roll back the damage they cause.
- **Firewalls:** A firewall acts like a bouncer at a club, determining which traffic is allowed to enter and exit your network. It blocks unauthorized access while letting legitimate traffic through.
- **Multifactor authentication (MFA):** MFA adds an extra layer of security by requiring users to provide at least two verification factors to log in. This is typically something you know (a password), something you have (a phone) or something you are (a fingerprint).
- **Virtual private network (VPN):** A VPN creates a secure connection between your device and the internet and ensures that all data is encrypted and safe from prying eyes.



Section 2

Current threats/common challenges facing firms

8 Current and emerging cyberthreats you need to know about

Cybersecurity threats are constantly evolving, and accounting firms aren't immune. Firms are entrusted with some of the most sensitive information imaginable—client financial records, PII, tax details and more—making them a prime target for cybercriminals. That means firms have a great responsibility—wait, ***obligation***—to protect that data. From data breaches to misconceptions about technology security, firms need to be aware of current and emerging threats and be prepared to defend against them.

While cyberthreats are real, and attacks happen every day, there are steps you can take to protect your firm. The first step is knowing what's out there. So, let's dive in.

01. Data breaches: A looming threat

If your firm doesn't prioritize security, data breaches are much less of an "if" than a "when." And for accounting firms, the fallout can be disastrous. Think: lost clients, compliance penalties, operational disruption and reputational damage. According to **IBM's Cost of a Data Breach Report**, the average cost of a data breach jumped to $4.88 million from $4.45 million in 2023. That's a 10% spike within a year—a devastating price tag for any business, especially accounting firms.

But how does this happen? It's simple. Hackers use tactics like phishing, malware or exploiting weak passwords to gain access to confidential information. Once they have access, they're stealing data, installing ransomware and even selling it on the **dark web**.

What is the dark web?

It's known as the marketplace for PII and is accessible only through special browsers like Tor—a web browser that lets users access a network that anonymizes web traffic to provide private web browsing.

Types of data breaches

Data breaches come in several different forms, like:

- **Hacking or cyberattacks.** These breaches occur when hackers exploit vulnerabilities in your system, like malware attacks, phishing scams, ransomware or brute-force attacks on passwords.
- **Insider threats.** Sometimes, employees, vendors or partners who have access to sensitive information can intentionally or unintentionally expose data.
- **Physical breach.** This involves the theft or loss of devices containing sensitive information, such as laptops, USB drives or smartphones.
- **Social engineering.** Techniques like phishing, smishing and vishing trick individuals into revealing confidential information or providing system access.
- **Unintentional disclosure.** This can happen when sensitive data is exposed due to human error, such as uploading unprotected files to a public server or emailing a client's financial details to the wrong recipient.

You can **report a data breach** through the Federation of Tax Administrators website. Then, file reports with the Cybersecurity and Infrastructure Security Agency (CISA), and your state or local offices. More information can be found on the **CISA website**.



02. Compliance issues: Essential—not optional

You know that the accounting profession is heavily regulated, and failing to comply with cybersecurity standards has serious consequences. In fact, non-compliance can result in hefty fines, legal action and loss of client trust. But more importantly, if you fail to comply, it means your firm may be operating with inadequate security controls, and when you house as much PII as you do, that's a big no-no. Here are the compliance measures your firm needs to know about—and put into place.

IRS Security Six

The **IRS Security Six** serve as essential rules for how firms should lay out their strategies for protecting data. At face value, each element seems obvious and straightforward:

1. **Antivirus software**
2. **Firewalls**
3. **Multifactor authentication**
4. **Backup software services**
5. **Drive encryption**
6. **Virtual private network (VPN)**

FTC Safeguards Rule

The **FTC Safeguards Rule** requires financial institutions under FTC jurisdiction to have measures in place to keep client information secure, including providing security awareness training to all staff members. This means that financial institutions (including accounting firms) must develop, implement and maintain an information security program designed to protect customer information, also known as PII.

To avoid potential fines and loss of client data, it's crucial to ensure you have the following:

- **Someone to manage your information security program.**
- **A comprehensive risk assessment that identifies security gaps.**
- **Regular monitoring of how risks are managed and addressed.**

You must also designate a **Qualified Individual** to oversee your firm's information security program and put safeguards in place to resolve identified risks.



Written Information Security Plan (WISP)

We'll go into further detail about WISPs in a later section of this guide, but it's important to know that as an accounting firm, you **should have a WISP in place** to renew your Preparer Tax Identification Number (PTIN). If you don't have a WISP, you can't renew your PTIN. Your WISP should have:

- **A stated objective and purpose.**
- **A risk assessment and results.**
- **A list of all your security software and services.**
- **A plan for responding to a data breach.**
- **Security policies for staff and contractors.**
- **Policies for monitoring and reviewing the WISP.**

03. Client data protection: One of your most valuable assets

Clients trust you with their most personal information—it's up to you to protect it. PII, such as financial data, Social Security numbers and tax information, is highly valuable to cybercriminals, making it a goldmine for hackers.

> ***Human error accounts for 22% of data breaches.***
>
> *Source: Cost of a Data Breach Report 2024, IBM*

Beyond the initial data breach, **identity theft and fraud** often follow. In fact, the **most common type of data stolen** or compromised in 2023 was customer PII—at a whopping 46%. It isn't costly just to your firm but to your clients as well. The global average for all stolen record types rose to a high of $169 per record in 2023.



04. Remote work: An added layer of vulnerability

Remote work has become a standard for many industries, and the accounting profession has also made a signficant shift to a remote or hybrid environment. However, without the proper cybersecurity measures in place, a firm can become more vulnerable to a cyberattack. How? Unsecured Wi-Fi connections, the use of personal devices, lack of oversight of devices... and more.

92% of remote workers report using their personal tablets or smartphones for work tasks, with 46% having saved a work file onto those devices.

Source: The State of Remote Work Security, Lookout



Hackers can exploit remote employees by targeting unsecured home networks, especially when your team uses their personal devices to access sensitive client data. Without the protection of an office environment, these devices become more susceptible to phishing, malware and other types of attacks.

Firms must practice remote workspace security that includes:

- **Working in a secure cloud environment.**
- **Implementing a remote work policy that includes stipulations around private Wi-Fi connections, MFA, using a VPN and installing antivirus protection on all devices.**
- **Requiring continued security and phishing training.**
- **Partnering with security experts and third parties.**

05. Outdated software: An easy invitation for hackers

Outdated software is one of the easiest ways for hackers to exploit vulnerabilities. Software developers **release patches to update their applications and fix security flaws.** But if your firm isn't keeping up with these updates, you're essentially leaving a key under the welcome mat for cybercriminals.

Why is outdated software a risk?

1. **Previously undiscovered vulnerabilities.** When a software patch is released, it's often accompanied by documents of the flaw being fixed. Hackers can use that information to target your outdated systems.

2. **Compatibility issues.** Outdated software can become incompatible with newer security tools, weakening your overall defenses and creating security gaps that hackers can exploit.

3. **Lack of vendor support.** Software vendors eventually discontinue support for older software versions, which means they stop providing security patches or updates, leaving your firm vulnerable.

4. **Data breach exposure.** If hackers act on an unpatched vulnerability in outdated software, it can lead to significant data breaches that expose confidential client financial data.

06. Lack of encryption: Leaving the door wide open

Encryption is one of the simplest yet most effective ways to protect sensitive data. However, many firms still fail to encrypt client information, both at rest (when data is stored) and in transit (when data is sent). Without encryption, even a small data breach can have large consequences.

Firms should be encrypting data through:

- **Full-disk encryption**
- **Client portals**
- **Backups**
- **Applications with built-in encryption features**
- **A trusted partner that can manage your security**

07. Lack of processes and security policies: Up the creek without a paddle

Many accounting firms lack comprehensive cybersecurity policies, leaving employees uncertain about what to do in case a cyberattack happens. Without a plan, response times are delayed, meaning there's more time for even more damage to be done.

There are several consequences when it comes to lacking processes and policies:

- **Inconsistent data handling.** Without clear policies, employees may store sensitive client information on personal devices, share financial details via unencrypted email or upload confidential documents to unsecured client platforms.
- **Slow response to threats.** Firms without a formal cybersecurity incident response plan or WISP often struggle to respond effectively to breaches or cyberattacks.
- **Lack of regular audits.** A firm without a well-documented security policy is unlikely to conduct regular audits or vulnerability assessments, meaning there are potential security gaps that go unnoticed until they're exploited by hackers.



08. Misconceptions about new technology: Is it really less secure?

As accounting firms continue to **embrace digital transformation**, many remain hesitant to adopt new technologies, especially AI. And this reluctance stems from misunderstandings or fears about the security of these technologies.

Do any of the following statements sound familiar?

"AI will replace accountants and compromise data security."

"New technology is complex and isn't worth the effort."

"Cloud-based solutions are less secure."

"Automation means losing control over data."



While these phrases may seem true, they're unfounded. Running your business in the cloud is more secure than on-premises systems. Cloud-based solutions offer robust security measures like encryption, MFA, intrusion detection systems, 24/7 monitoring and automatic security updates.

AI won't replace accountants...but those who fail to learn and implement AI may lose their jobs to those who do take on AI. And in terms of cybersecurity, many AI tools are equipped with machine learning algorithms that actively monitor and identify suspicious activities—actually strengthening security.

The bottom line is that moving to the cloud and implementing new technology will only make your firm more efficient, move you ahead of the competition and—most importantly—keep you secure.

Section 3

Importance of data security

The importance of data security

Data security is the backbone of any successful accounting firm. With the increasing reliance on technology to manage client information and financial transactions, understanding the ins and outs of data security is crucial. So, let's break it down.

Understanding data security: A high-level view

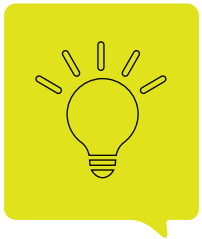
Data security refers to the measures and protocols put in place to protect sensitive data from unauthorized access, breaches and other cyberthreats. This includes everything from encryption and firewalls to policies that govern how data is accessed and shared. The scope of data security encompasses all types of data—client records, financial statements and internal communications—ensuring that every piece of information is safeguarded against potential harm.

Why data security matters

Data security isn't just about having the right technology in place; it's about ensuring the integrity and confidentiality of the information you handle every day. In a time where cyberthreats are rampant, understanding the stakes is essential for every firm. Here are some key reasons why prioritizing data security in your firm is crucial.

▹ Protecting sensitive client information

Accounting firms are entrusted with highly sensitive client information, including personal identification details, financial records and tax information—collectively referred to as PII. A breach of this data not only puts your clients at risk but can also lead to identity theft or fraud. Protecting PII isn't just a best practice; it's your fundamental responsibility.



***46%** of breaches involved customer PII.*

Source: Cost of a Data Breach Report 2024, IBM

▹ Maintaining firm reputation and trust

Trust is the foundation of the accountant-client relationship. When clients know their information is secure, they feel more confident engaging with your firm. Conversely, any hint of a data breach can severely damage your firm's reputation. A strong commitment to data security reassures clients that you take their privacy seriously, fostering lasting relationships built on trust.

Consequences of poor data security

The consequences of poor data security can be severe and multifaceted, impacting not only your firm's bottom line but also your reputation. From financial losses to legal challenges, the risks are substantial. Let's take a closer look at what can happen when data security is compromised.

▹ Financial losses

Data breaches can be incredibly costly. The direct impact of a breach can result in significant financial losses, including the costs associated with remediation, legal fees and potential fines. Additionally, the longer it takes to recover from a breach, the more damage a firm will see in both operational downtime and lost business opportunities.

Data insight:

The global average cost of a data breach has risen to $4.88 million. This amount is the highest ever reported and represents a 10% increase from the previous year. For professional services organizations (including legal, accounting and consulting firms), the cost of a data breach is even higher, with an average cost of $5.08 million.

Source: Cost of a Data Breach Report 2024, IBM

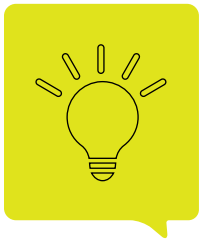


▹ Legal repercussions

The legal implications of poor data security are profound. Compliance with laws such as the GLBA, GDPR or CCPA (to name a few) isn't just a suggestion; it's a requirement. Failing to protect client data can lead to hefty penalties and lawsuits, further adding to the financial strain on your firm.

▹ Reputational damage

Perhaps the most insidious consequence of data breaches is the lasting damage to your firm's reputation. Once trust is broken, it's incredibly challenging to rebuild. Clients may choose to take their business elsewhere, and word of mouth can quickly tarnish your firm's image. In a profession where reputation and trust are everything, this kind of damage can be irreparable.



17% of respondents who had suffered a security breach indicated that while they did not have a direct financial loss, it caused significant reputational damage.

Source: June 2024 CPA Practice Advisor/Canopy survey

Moving forward

As we delve deeper into this guide, we'll explore specific strategies and tools to bolster data security within your firm. Remember, investing time and resources into data security isn't just about compliance; it's about safeguarding and preserving your clients, your firm and your future. Read on for practical tips and best practices that will help you create a robust data security framework.

Did you know?

In 2023, the number of publicly reported data compromises rose to 3,205, impacting an estimated 353,027,892 individuals. That's a 78% increase over the 1,801 data compromises in 2022.

What is a data compromise? The overall term used to refer to events where personal information is accessible by unauthorized individuals and/or for unintended purposes. This includes data breaches, data exposures and data leaks.

Source: ITRC Annual Data Breach Report



Section 4

Essential cybersecurity measures



6 essential cybersecurity measures your firm should know about

It's no secret that accounting firms handle a treasure trove of sensitive data, from client financials and personal information to tax details...and much more. With this sheer amount of data comes the ever-increasing risk of cyberattacks. And that means implementing cybersecurity measures is no longer optional; it's absolutely critical to safeguarding your business and clients.

In 2023, 40% of production data was successfully encrypted by bad actors after a cyberattack, meaning the data was unrecoverable.

Source: Ransomware Trends 2024, Veeam

In this section, we'll cover the six key areas that all accounting firms should focus on to stay secure: risk assessment, data encryption, access controls, network security, employee training and WISPs. With this information in hand, you'll be ready to take proactive steps to protect your firm and clients.

1. Risk assessment: Your foundation for security

***67%** of organizations do not have a recovery plan.*

Source: Ransomware Trends 2024, Veeam

What is a cybersecurity risk assessment?

A cybersecurity risk assessment is the process of identifying, analyzing and evaluating risks to your firm's digital infrastructure. Think of it as a health check-up for your firm's security. It's about knowing where your vulnerabilities are, understanding how they could be exploited and deciding on the best course of action to minimize those risks.

The goal? To reduce the impact of threats before they happen.

Why do you need a cybersecurity risk assessment?

These types of risk assessments are crucial for accounting firms because they provide a clear picture of potential cyberthreats. Without a structured approach, your firm is at risk of data breaches that could damage your reputation, result in hefty fines and even lead to lost clients. A robust assessment can prevent these outcomes and ensure compliance with industry regulations like the **Gramm-Leach-Bliley Act (GLBA)**, which mandates the protection of customer information.

Think about it this way: You can't protect what you don't understand.

How to do a cybersecurity risk assessment: A step-by-step guide

Before you start: Most accounting firms don't have dedicated IT departments and that's OK. This guide is designed for firms just like yours! If your firm doesn't have a dedicated IT department, you can work with your existing staff or an IT service provider or professional to complete your risk assessment.



Phase 1: Get organized

Timeframe: 1 week

1. **Form your risk assessment team.**
    - **Assign a team leader.** This is usually the managing partner or operations manager.
    - **Include core team members.** This group should include a partner responsible for client data, an office manager, a senior accountant and your external IT support provider (or internal, if you have one).



If you're a smaller firm, this core team may just be you and one other person.

(And that's fine!)

2. **List out what you need to protect.**
    - **Technology inventory.** Make a list of:
        - Computers and laptops
        - Tax and accounting software
        - Cloud-based applications
        - Client portals
        - Document sharing tools
        - Backup systems
        - Mobile devices
    - **Client data inventory.** Document where you store:
        - Tax returns
        - Financial statements
        - Client correspondence
        - Payroll information
        - Bank account details
        - Other PII

Phase 2: Identify threats

Timeframe: 1 week

1. **List tax season threats.**
    - Phishing emails pretending to be the IRS or other trusted authority
    - Fake client emails with "urgent" requests or tax documents
    - Ransomware targeting tax data
2. **Identify daily operations risks.**
    - Weak passwords
    - Unsecured file sharing
    - Personal devices accessing firm data
    - Email compromise
3. **Outline client portal risks.**
    - Unauthorized access attempts
    - Insecure password practices
    - File upload vulnerabilities

Phase 3: Evaluate your risks

Timeframe: 1 week

1. **Rate your risks.**
    - **Rate the impact.** Using a simple rating system, identify what impact potential risks may have on your firm.
        - Low = minor inconvenience
        - Medium = temporary disruption
        - High = major impact or loss
    - **Rate the likelihood.** Determine how likely a potential risk is to occur.
        - Low = may happen yearly
        - Medium = could happen quarterly
        - High = could happen frequently

Use the ratings on impact and likelihood to determine which risks should be prioritized when implementing a protection plan.

2. **Run through an assessment checklist.**

Review your technology and client data inventory from phase 1. For each system, determine the following:

- How do we protect it now?
- Who has access to it?
- What would happen if it was breached?
- How quickly could we recover?

Phase 4: Make an action plan

Timeframe: 1 week

1. **Prioritize password security.**
    - Set up a password manager.
    - Enable MFA wherever possible.
    - Create a password policy.
2. **Protect data.**
    - Encrypt client files.
    - Set up secure file sharing.
    - Configure automatic backups.
3. **Secure email.**
    - Enable spam filtering.
    - Train staff on phishing.
    - Encrypt emails, especially sensitive ones.
4. **Depending on your risk assessment from phase 3, prioritize the following:**
    - Client portal security
    - Security awareness training for staff
    - Written security policies
    - Incident response plan (this should be part of your WISP)

Phase 5: Create documentation

Timeframe: 2-3 days

1. **Identify essential documents.**
   - List of all systems and software
   - Where client data is stored
   - Security measures in place
   - Action items and timeline

2. **Build emergency contact list.**
   - IT support provider
   - Cybersecurity partner (if applicable)
   - Third-party vendors
   - Insurance provider
   - Key firm members

3. **List contacts to report breach.**
   - The IRS offers a full list of who to contact here.

Phase 6: Take action

Timeframe: Ongoing

1. **Follow an implementation schedule.**
   - **Get quick wins**
     - Update all passwords
     - Enable MFA
     - Install security software
   - **Update staff**
     - Share new security policies
     - Provide security awareness training
     - Set up password managers
   - **Secure client data**
     - Review client access
     - Ensure secure file sharing
     - Update backup systems
   - **Review**
     - Test all new security measures
     - Update documentation
     - Plan ongoing training

2. **Conduct regular reviews.**
   - **Quarterly review checklist:**
     - Were there any security incidents?
     - Did we add new software or systems?
     - Have we changed how we handle data?
     - Is staff following procedures?
     - Are there any new types of client data?



Common cybersecurity mistakes to avoid

1. Thinking, "We're too small to be a target."
2. Forgetting about mobile devices or remote users.
3. Not training or doing background checks on temporary seasonal staff and/or contractors.
4. Overlooking non-technical security measures.
5. Assuming cloud providers handle all security.

PRO TIP

Pro tips for cybersecurity success

1. Start with protecting the most sensitive data first.
2. Make security a part of your daily routine.
3. Keep instructions clear and simple.
4. Document everything, but keep it practical.
5. Review policies and efforts during both busy and quiet seasons.
6. Partner with managed security providers who have the expertise and enterprise-level tools to keep your firm safe.

When to get help

Consider working with a cybersecurity partner when:

- Starting your first risk assessment.
- Handling sensitive client data.
- Adding new services or technologies.
- Having experienced security incidents.
- Preparing for busy season.



2. Data encryption: Protecting sensitive information

What is data encryption?

Encryption is the process of converting your data into a scrambled or 'secret' code that can only be read by someone with the decryption key. It ensures that your data will be unreadable even if hackers get their hands on it.

For accounting firms that handle sensitive client data, like Social Security numbers (SSNs), tax information and financial details, encryption is a critical line of defense against cyberthreats. Without robust encryption measures in place, your clients' PII is at risk of being stolen, manipulated or sold.

Types of encryption

- **Symmetric encryption**: Uses a single key for both encryption and decryption and is best for encrypting large volumes of data. Common symmetric encryption methods include AES (advanced encryption standard), which is known for its high level of security and efficiency.

- **Asymmetric encryption**: Uses a pair of keys—a public key to encrypt data and a private key to decrypt it. It's used most often in situations where secure data exchange is needed between two parties, such as sending encrypted emails.

1 in 5 respondents know their organization has lost sensitive data. And there are 26% who suspect they've lost sensitive data but don't know for sure because they don't have the tooling or expertise to find out.

Source: Operationalizing Encryption and Key Management, Enterprise Strategy Group™ by TechTarget

What you need to encrypt

Use the list below to determine what data needs to be encrypted and how their encryption

Priority level 1: Highly sensitive data **Must encrypt:**	Priority level 2: Business operations data **Must also encrypt:**
Tax returns and supporting documents	Internal financial records
SSNs	Employee information
Bank account information	Client correspondence
Investment account details	Engagement letters
Payroll data	Workpapers
Client financial statements	Audit documentation
Estate planning documents	



Tools and best practices

Implementing encryption can be straightforward with the right tools and strategies. Here are some essential tools and best practices. And ultimately, working with a trusted cybersecurity partner who can handle all of this for you is probably your best move.

Encryption tools:

- **BitLocker (for Windows) and FileVault (for macOS):** Both tools provide disk encryption to protect data on desktops and laptops.
- **SSL/TLS (secure sockets layer/transport layer security):** Secures data exchanges over the internet and is essential for protecting client data transmitted through email or web portals.
- **PGP (pretty good privacy):** Encrypts emails and ensures sensitive information stays private.
- **VPN (virtual private network):** Encrypts data transmitted over the internet, preventing unauthorized access to sensitive data.

Encryption best practices:

- **Use strong encryption algorithms:** Secure client data with AES-256. It's a trusted standard and meets compliance requirements.
- **Regularly update encryption protocols:** Keep encryption software updated to patch any potential vulnerabilities. Failing to do so leaves data exposed to new threats.
- **Encrypt data backups:** Ensure backup data is encrypted in case devices are lost or stolen.
- **Secure encryption keys:** Store encryption keys securely and away from the data they encrypt. Mishandled keys can lead to unauthorized access.

How to build a robust data encryption strategy

To create a successful data encryption strategy, you need to first understand what client information needs to be protected and then implement a systematic approach to keep it secure. Here's what your firm can do:

1. Identify and classify sensitive client data:

- Determine the data types that are the most sensitive (i.e., PII).
- Classify data to apply different levels of encryption.
  (Hint: PII should have the strictest encryption controls.)

2. Implement encryption:

- Encrypt databases, local storage and backups to ensure sensitive information remains safe.
- Use SSL/TLS to secure data transfers between your firm's network, client devices and external systems, protecting data shared via email, cloud services or web portals.

3. Develop a key management plan:

- Use automated key management solutions to securely generate, store and rotate keys.
- Ensure only authorized personnel have access to encryption keys, and audit key usage regularly.

4. Integrate DLP (data loss prevention):

- Use DLP tools to monitor how data is accessed and used within your firm to prevent the unauthorized sharing of sensitive information.

How to keep your data secure

Ensure your firm's data encryption is effective by using this checklist:

☑ Encrypt all data at rest (e.g., files on computers, servers, backup systems).

☑ Use SSL/TLS to encrypt data during transmission (e.g., client portals, emails).

☑ Implement strong encryption algorithms (e.g., AES-256) to meet regulatory compliance standards.

☑ Regularly update encryption software to protect against emerging threats.

☑ Securely manage encryption keys with a robust key management system.

☑ Encrypt backup files to safeguard client information.

☑ Monitor data access and movement with DLP solutions.

☑ Educate staff on encryption practices.

3. Access controls: Who can access your data?

Access controls are essential when it comes to authorizing which staff members should have access to sensitive client information. When you set strict controls on who can view, edit and share data, firms can significantly reduce the risk of data breaches, internal threats and accidental data leaks.



Role-based access controls (RBAC)

RBAC limits data access based on a user's role in your firm. By segmenting access, firms can minimize the chances of unauthorized users viewing or manipulating PII. It also makes it easier to track who accesses what information, which helps during audits and compliance verification efforts.

Implementing MFA

MFA adds a second layer of security to the login process, requiring users to verify their identity with more than just a password. When implemented, users enter a password, and then they receive a verification code via email or text, or they use a fingerprint scan.

Other AppSec tools

While using RBAC and MFA is a great starting point, firms should also consider additional application security (AppSec) tools to enhance their security framework, such as:

Single sign-on (SSO): SSO allows users to access multiple applications with a single set of credentials, which simplifies the login process and ensures all accounts are secured. It's also easier to allow or revoke access for staff members.

Password management tools: These help enforce strong, unique passwords across platforms and reduce the risk of breaches from reused or weak passwords.

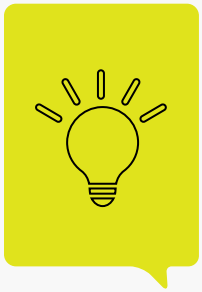
Security information and event management (SIEM): Monitors user activity across networks in real time, identifying suspicious behavior and flagging potential threats immediately.

Your checklist for implementing access controls

- ☑ Set up RBAC to limit data access based on employee roles.
- ☑ Implement MFA for all login processes.
- ☑ Use SSO or one-click login to streamline user authentication across multiple platforms/applications.
- ☑ Enforce strong password policies with the help of password management tools.
- ☑ Monitor user activity through SIEM systems to detect and quickly respond to unusual behavior.

4. Network security: Your digital fortress

Think of your firm's network as a large office building that is home to numerous businesses and tenants. Just as that building and businesses have multiple layers of physical security—locks on doors, key cards, security cameras and perhaps even a security guard—your firm's digital workspaces need similar protection layers.



Insight: The IRS Security Six protections are an important starting point for firms to safeguard their offices, devices and data:

- ▶ Antivirus software
- ▶ Firewalls
- ▶ Multifactor authentication
- ▶ Backup software or services
- ▶ Drive encryption
- ▶ Virtual private network

Firewalls and intrusion detection systems: Don't leave your digital doors unlocked

Just as you wouldn't leave your office doors wide open after hours, you shouldn't leave your network unprotected. Firewalls act like the doors and walls of your physical office—a barrier—keeping cyberthreats at bay. They monitor and control incoming and outgoing network traffic based on predetermined security rules.

Intrusion detection systems (IDS), on the other hand, are more like security cameras, watching for potential intrusions and sending alerts to security teams. Most often, IDS are available through cloud providers who can monitor networks 24/7. Together, they're your first line of defense against unauthorized access and cyberthreats.

VPNs for remote access: Your secure tunnel through the cyberworld

With the increase of remote and hybrid work in accounting firms, secure VPNs are essential (not to mention, a requirement for accessing firm resources remotely). Think of a VPN as a secure tunnel through the internet—like having a private, encrypted pathway for your data to travel through. When your staff accesses client financial data from their devices, from home or while traveling, VPNs ensure that sensitive information remains protected.

Layered security approach: Defense in depth...because one lock isn't enough

Remember the old saying about not putting all your eggs in one basket? The same applies to cybersecurity. A **layered security approach** means implementing multiple security measures that work together to protect your firm's data. It's like having multiple security checkpoints from the front entrance of your office building all the way to your front door, and even the individual offices inside. Each checkpoint adds an extra layer of security. A layered security approach includes:

- Network security and regular monitoring
- Endpoint/device protection
- Email security filters
- Data encryption
- Access controls and authentication
- Employee security awareness training
- Regular security updates and testing
- Backup and disaster recovery



Cloud providers can help implement a comprehensive enterprise-grade layered security solution more affordably than trying to build it in-house.

5. Employee training: Creating your human firewall

Now that you understand how a firewall acts as a barrier, it's time to think about how your employees can act as a human firewall, adding another layer of support. They are your greatest asset and sometimes your most significant vulnerability. In fact, according to CISA, **over 90% of successful cyberattacks start with a phishing email**. Investing in proper cybersecurity training for your team can make your employees one of your main lines of defense.

More than just checking boxes: The importance of cybersecurity awareness

Just as you train your staff on accounting principles, processes, best practices and software/apps, cybersecurity training should be a fundamental part of your firm's professional development program. Your employees need to be informed about potential threats and how to handle them, and training equips them with the knowledge they need to recognize cyberthreats.

When cybersecurity becomes second nature: Creating a culture of security

Building a security-conscious culture in your firm isn't just about implementing strict rules and policies; it's about making security awareness second nature and a shared responsibility. Each person on your team needs to understand their critical role in protecting client data. Think of it like basic accounting principles: Just as your staff automatically double-checks their numbers, they should automatically think twice before clicking on suspicious links or sharing sensitive information. Creating a culture of cybersecurity means you integrate it into the fabric of your firm, making it part of onboarding and ongoing professional development. It means encouraging open discussions and celebrating employees who report suspicious activities.



Make cybersecurity discussions a regular part of team meetings, just as you would discuss client updates, process revisions or tax law changes. Security policies and efforts should be reviewed and updated regularly with input from your team.

From rookies to cyber-savvy pros: The benefits of security awareness training

Making security awareness training programs an ongoing part of your cybersecurity efforts reinforces your commitment to a healthy cybersecurity culture. These programs should be engaging and interactive, using real-world scenarios and examples that are relevant to accounting firms to better arm your staff.

Your security awareness training programs should be ongoing and cover the following:

- Current phishing and social engineering tactics
- How to identify suspicious emails and links
- Safe password practices
- Data handling procedures
- Safe remote work protocols
- Social engineering awareness
- Incident reporting procedures



Insight: What to watch for and what to do

Common human errors:

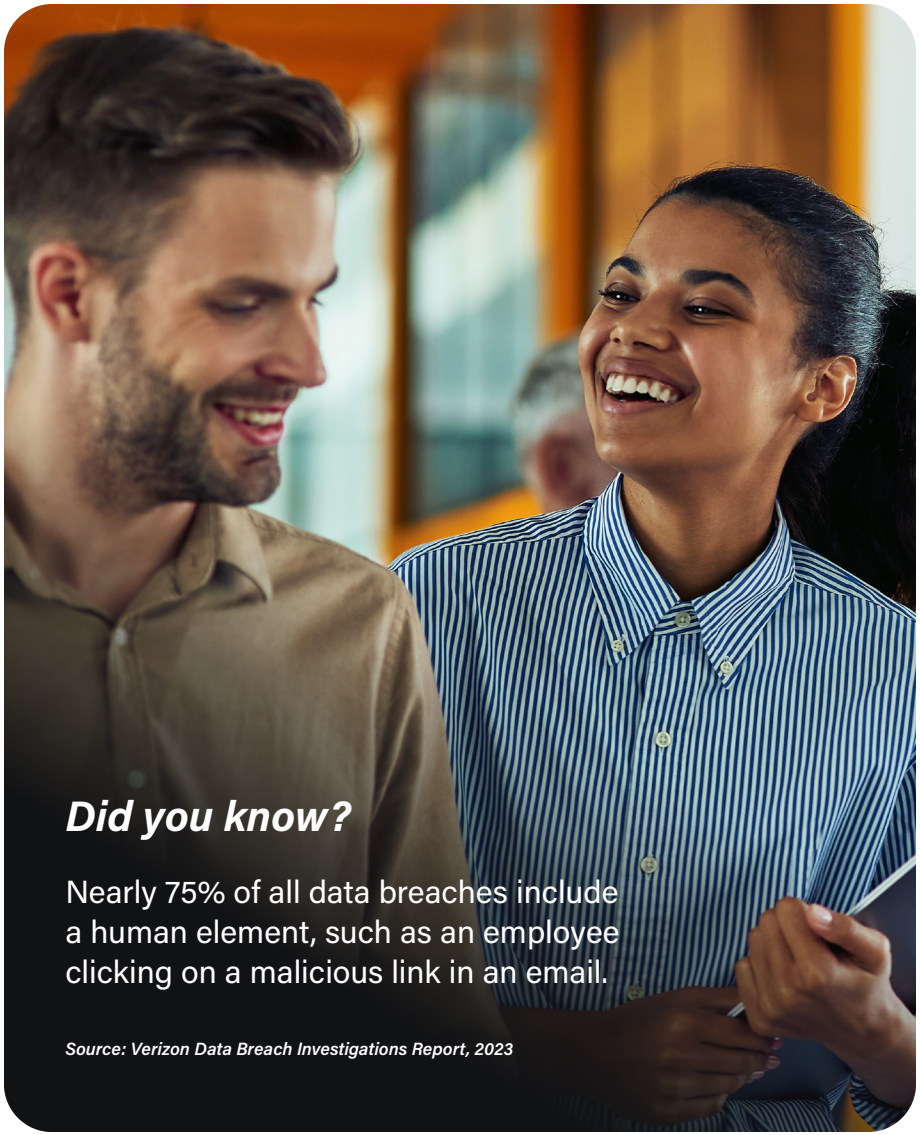
- Clicking suspicious links or attachments.
- Using weak passwords.
- Sharing credentials.
- Not verifying requests for sensitive information.
- Connecting to unsecured networks.

Ways to mitigate risk:

- Regular training and awareness updates.
- Clear security policies and procedures.
- Technical controls to catch human mistakes.
- Making secure behavior the easy choice.
- Building security into workflows.

The human error factor: Because we're all human, after all

Human error remains one of the leading causes of data breaches. Just one click on a malicious link can compromise an entire network. Regular training and refresher courses help minimize these risks, much like continuing education helps maintain professional expertise. When your team understands the importance of cybersecurity, they'll feel more empowered, vigilant and proactive in identifying and reporting potential security issues.





6. Written Information Security Plan (WISP): Your cybersecurity playbook

A WISP is exactly what it sounds like—a documented strategy for protecting sensitive information. Think of it as your firm's cybersecurity playbook, outlining the administrative, technical and physical safeguards your firm has in place to protect client data, how to respond to incidents and how to maintain security standards.

Beyond the regulatory checkbox

Beyond being a legal requirement—tax preparers must have one for PTIN renewal—a WISP demonstrates your firm's due diligence and compliance with regulations. It helps identify security gaps and vulnerabilities, and provides:

- Clear guidelines for staff
- Documentation for clients and regulators
- Incident response procedures
- Risk assessment frameworks

Building your security blueprint

Your WISP isn't a static document. Rather, it should be a living and breathing blueprint for security protocols—a plan that's reviewed and updated regularly as threats and technologies evolve.

Your WISP should include:

- ☑ **Designated security coordinator**. A qualified person(s) to oversee your firm's security plan.
- ☑ **Risk assessment procedures**. Must document all systems containing client data, identify potential threats and vulnerabilities, evaluate existing security measures, and regularly review and update.
- ☑ **Security policies and procedures**. Includes access controls, employee and third-party background checks, authentication requirements, data encryption standards, password policies, incident response procedures, employee training requirements and vendor management protocols.
- ☑ **Technical safeguards**. Outlines network security measures, encryption requirements, backup procedures, software update protocols and device security standards.
- ☑ **Physical safeguards**. Defines office security measures, equipment protection, paper record security and clean desk policies.
- ☑ **Training and oversight**. Details employee security awareness training programs, ongoing education requirements, compliance monitoring, and regular testing and update schedules.
- ☑ **Incident response plan**. Outlines steps for handling security breaches, communication procedures, recovery protocols and documentation requirements.
- ☑ **Third-party management**. Specifies vendor security requirements, service provider oversight, contract requirements and regular assessments.

An effective WISP requires expertise in both technical and legal requirements. Most firms benefit from working with a qualified cybersecurity partner that can help:

- Develop a comprehensive plan.
- Ensure regulatory compliance.
- Keep your plan updated.
- Implement required security measures.
- Provide ongoing training and support.

WISP requirements:
Why expert help is better than DIY

First things first: What's a WISP and why do you need it?

- Written information security plan (WISP) required for **all tax preparers**.
- Plan must detail measures to protect sensitive data.
- Ensures compliance with cybersecurity regulations (e.g., FTC Safeguards Rule).
- Penalties for non-compliance **up to $43,280/day**.
- Acknowledgment of plan required for PTIN renewal.

DIY WISP creation

Before you decide to write your own WISP, consider these factors:

1 Understand the time commitment
- Could take up to 40 hours of potentially billable time.
- Requires ongoing maintenance and updates.

2 Recognize the complexity
- Requires in-depth knowledge of technology and regulatory requirements.
- Risk of misunderstanding or misapplying suggested security protocols.

3 Ensure legal compliance
- Requires ability to navigate, interpret and apply data disclosure laws.
- Potential for non-compliance and associated penalties.

4 Take inventory of information and technology
- Requires deep dive into every type of information your firm handles and stores.

5 Provide employee training and verify data suppliers
- Establish initial and ongoing training sessions for employees.
- Verify all data suppliers use reasonable security measures.

6 Manage security strategy and incident response
- Must stay vigilant with rapidly evolving cyberthreats and security developments.
- Requires crisis management skill and timely response to data breaches.

VS

WISP creation with Rightworks

If the DIY path looks daunting, there's an easier way. Check out these 3 steps:

1 Initial consultation
Meet with our team to determine the best solution for your firm's needs.

2 Tech stack assessment
We'll do a tech stack assessment and provide suggestions for how you can use the right tools to keep client data safe.

3 Security planning
Following the assessment, we'll offer recommendations for a comprehensive cybersecurity strategy to bridge any identified risks, adding peace of mind beyond IRS compliance.

The right partner can help you get it right

Creating a WISP can seem overwhelming. Without one, you leave your firm vulnerable to cyberattacks and risk costly penalties and reputational harm. Our cybersecurity experts can help you develop a comprehensive WISP to safeguard your firm and ensure compliance. Let us simplify the process and strengthen your security strategy.

Secure your firm's future today! →

rightworks

Section 5

Best practices for cybersecurity in accounting firms



Best practices for cybersecurity in accounting firms: Practical steps for securing client trust

We've said it several times already, but handling sensitive client data is a fundamental part of running an accounting firm. And since your clients trust you with their PII, it means cybersecurity is a must-have.

If you're thinking, "I'm no tech expert; I'm not sure how to handle this," don't. You don't need to be a cybersecurity expert to put some key protective practices in place. In this section, we'll share four actionable steps you can take to safeguard your firm's data, secure client trust and keep cyberthreats at bay.

1. Perform regular software updates and patch management

One of the easiest—but most overlooked—steps in cybersecurity is ensuring all software is up to date...all the time. Cybercriminals jump on vulnerabilities faster than you can say "vulnerabilities." They exploit outdated systems easily, so regular updates are essential.

Action steps:

- **Set automatic updates:** Whenever possible, enable automatic updates on all devices and applications.
- **Develop a patch management policy:** Create a policy that includes regularly checking for updates on less common software or legacy systems that may not update automatically.
- **Remind employees:** Regularly remind employees to avoid delaying updates, especially for critical software and applications like antivirus, operating systems and client management tools.

2. Secure client communication channels

While traditional email may be the most convenient, it's generally not secure enough for sharing sensitive information. To protect client communication, use encrypted email and secure client portals.

Action steps:

- **Send encrypted emails:** Implement encrypted email systems to secure client communications.
- **Use client portals:** Set up client portals where clients can securely upload and download sensitive documents. Consider portals like SmartVault, Canopy or TaxDome to secure your workflows, from practice management to document management.
- **Provide client training:** Educate your clients on the importance of using secure portals and not sending sensitive data via email or text messages.

3. Implement data backup strategies to protect what matters

Backing up your data is one of the most important cybersecurity practices you can implement. It's not just a lifesaver if there's a data breach, but it "comes in clutch" if files are corrupted or accidentally deleted (humans do make mistakes). Imagine the fallout of losing years of financial records. Data backups prevent that nightmare scenario from becoming a reality.

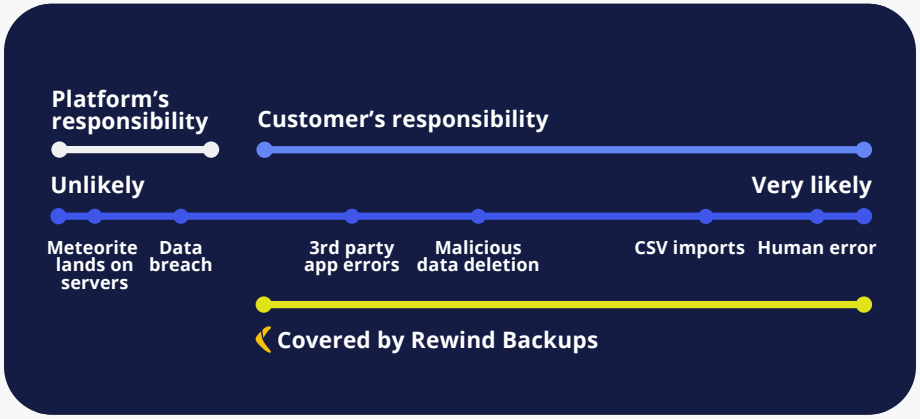
Action steps:

- **Establish a regular backup schedule**: Consistency is key, whether it's daily (strongly recommended), weekly or monthly. Remember to back up both client and internal files.
- **Consider Rewind for QuickBooks® Online**: If your firm uses QuickBooks, which does maintain disaster recovery backups of its entire platform, you still need to back up your own data, such as customers, transactions, deposits and invoices.
- **Move to the cloud**: Start running your operations in a **secure cloud environment** and look for a provider that offers rolling data backups.

Data backup: Understanding the Shared Responsibility Model

It's crucial to understand that data backup and cloud security is a shared responsibility between the provider and you—the customer. Even though providers secure the underlying infrastructure, you're responsible for:

- **Responsibly configuring cloud services.**
- **Managing user access and permissions.**
- **Securing devices that connect to the cloud.**
- **Training employees on security best practices.**



An example of the Shared Responsibility Model with QuickBooks Online as the platform and you as the customer. This example shows how tools like Rewind Backups for QuickBooks Online can help.



You'll notice in the chart to the left that QuickBooks Online is responsible (Platform's responsibility) in the unlikely event that a meteorite lands on its servers or a data breach occurs based on a company-wide attack. However, you are responsible for:

- **Third-party app errors.** This includes any applications that integrate with QuickBooks Online to sync financial data. If there's a snafu with a third-party app, it's on you to recover that data.
- **Malicious data deletion.** Whether cybercriminals or employees with ill intentions maliciously delete your data via ransomware, phishing attacks or malware, if your data is wiped, QuickBooks Online can't recover it. It's on you to recover the data. (Are you seeing the theme here?)
- **CSV imports.** While a bulk upload can typically get data back quickly and easily, if the upload fails or the file isn't clear of duplicates or bad data, you risk wiping out existing data. And, again, it's your job to recover it.
- **Human error.** Humans aren't perfect, and they never will be. It's inevitable that someone will inadvertently delete important data—never to return. It's up to you to recover or recreate that deleted data.

Secure third-party partnerships

Many firms rely on third-party software and integrations, from tax software to CRM systems. But every vendor you work with adds a layer of risk, making vendor management a critical cybersecurity step. Food for thought: Your security is only as strong as your weakest vendor link.

Action steps:

- **Evaluate vendor security policies**: Before you partner with a new vendor, run through this evaluation checklist:
  - **Review security certifications and compliance**
  - **Assess data handling practices**
  - **Check backup and recovery procedures**
  - **Verify encryption standards**
  - **Evaluate access controls**
  - **Review incident response plans**

- **Secure third-party integrations:** Use integration platforms that offer encrypted connections to ensure any data transferred between software remains secure. Look for platforms with a track record of effective security and encryption.

- **Move to the cloud:** We've said it several times, but it's still worth repeating. Move your business into the cloud. Partner with a cybersecurity vendor that gives you one-click login access to all the tax and accounting apps you need in one place, safely and securely.

Take control, one step at a time

It can seem overwhelming to juggle so many cybersecurity practices, but each step makes your firm a more secure and trusted partner for your clients. And remember this: You're not alone. **Partnering with a cybersecurity provider** can bring expertise that fills in the gaps, letting you focus on what you do best: serving your clients.

PRO TIP

Get cyber insurance

Why do you need cyber insurance? Cyberattacks can be devastating—and your firm may not have the funds to adequately recover from one. Look for a plan with the following coverage:

- **Data breach liability**
- **Business interruption**
- **Ransomware protection**
- **Reputation management**
- **Cyber extortion**
- **Privacy liability**
- **Crisis management and public relations**
- **Multimedia liability**
- **Regulatory fines and penalties**

Bottom line: Attacks are complex and may lead to financial fallout. Comprehensive cyber insurance can keep your firm afloat.



Section 6

Legal and regulatory compliance

Regulations and compliance: Why they can make (or break) your accounting firm

While regulations and compliance may not be the most exciting part of running your accounting firm, they are critical to your success. The reality is that if you don't follow regulations and remain in compliance, you're not going to have a firm to run.

Whether you're a sole practitioner or managing a large firm, understanding and implementing regulatory requirements is essential to running a modern accounting practice. And whether you're handling individual tax returns, providing advisory services for small businesses or managing complex financial data for corporations, regulations like the FTC Safeguards Rule and the IRS Security Six are essential guardrails that protect both your clients and your firm. When you can confidently tell clients about your security measures and compliance protocols, you're showing them that protecting their data is a cornerstone of how you do business. And because they likely consider you their most trusted advisor, they're counting on you to protect it.

So, what regulations do you need to know about, and what do they mean for your firm? If you're ready to turn compliance from a challenge into a competitive advantage, let's dive in and explore what you need to know to keep your clients' data secure and your firm's reputation strong.



Understanding relevant regulations and standards

The first step to keeping your clients' data safe is understanding exactly what's required. And while navigating these regulations and standards might feel overwhelming, understanding them is crucial—not just to avoid expensive penalties, but to maintain the trust your clients place in you. Think of these regulations and standards as your playbook for protecting sensitive data. Let's learn which ones matter most for your firm and why they're relevant.

FTC Safeguards Rule

The FTC Safeguards Rule requires financial institutions, including accounting firms, to develop, implement and maintain a comprehensive information security program. It emphasizes the protection of client data and includes the following measures:

- **Conducting risk assessments**
- **Implementing safeguards like access controls to sensitive data**
- **Encrypting client information**
- **Regularly reviewing and testing security practices**
- **Training staff**
- **Monitoring service providers**
- **Creating a written incident response plan**
- **Designating a qualified individual to oversee the firm's information security program**

IRS Security Six

The IRS Security Six outlines basic security measures for tax professionals to protect against identity thieves and hackers. Think of the components as the six pillars holding up the security framework of your accounting firm. Here are the six steps outlined by the IRS and its Security Summit partners to safeguard taxpayer information:

1. Antivirus software: Protects against malware and other digital threats.

2. Firewalls: Shields networks from unauthorized access.

3. Multifactor authentication: Adds a layer of security beyond simple passwords.

4. Backup software: Ensures data can be restored in the event of data loss.

5. Drive encryption: Protects data stored on devices.

6. VPNs: Secures remote connections.

GDPR (General Data Protection Regulation)

The GDPR primarily impacts firms handling data from European citizens. Its scope is broad, requiring firms to have stringent data processing and storage protocols. US firms without any business or clients in the European Union may find GDPR less directly applicable, but many adopt its principles for broader data protection strategies.

GLBA (Gramm-Leach-Bliley Act)

This act requires financial institutions, including accounting firms, to explain how they share and protect nonpublic, sensitive personal and financial information. It forms the basis for many security requirements in the profession and includes requirements for privacy notices and information security programs.

PCI DSS (Payment Card Industry Data Security Standard)

If your firm processes, stores or transmits credit card information, compliance with PCI DSS is essential. It outlines security measures for protecting cardholder data.

CCPA (California Consumer Privacy Act)

Similar to GDPR, CCPA is the first major state privacy law in the US. It focuses on the data privacy rights of California residents, granting them greater control over their personal information. That makes it relevant for firms serving California clients or handling California resident data.

State-specific data protection laws

In addition to CCPA, many US states have their own data protection laws. For example, New York's SHIELD Act requires businesses to implement data security measures. Here are some things to consider:

- Firms must comply with laws in states where clients reside.
- Each state has unique data breach notification requirements, such as:
    - Notification timelines
    - Required security measures
    - Penalties for non-compliance





Compliance best practices

Understanding regulations is one thing, but making them work in your daily operations is another. That's where many firms hit a wall. Effective compliance isn't about creating a thick binder of policies that sits untouched on a shelf (we've all been there). What you really need is to build day-to-day habits and systems that protect client data while allowing your team to work efficiently. Sure, things like documentation, regular security assessments and audit trails might sound overwhelming at first. But here's the good news: You can break these practices down into manageable steps that become as natural as checking your email. As a result, you'll build a healthy security culture that protects your firm while keeping your workflow smooth and efficient.

Document, document, document

Maintain comprehensive records of your data processing activities and protection policies. This is your evidence of compliance and is crucial during audits. Throughout this eBook, you've seen multiple references to WISPs, and this is where your documentation comes into play. Your WISP should detail the following:

- **Security policies and procedures**
- **Risk assessment procedures**
- **Employee training programs**
- **Incident response plans**
- **Data backup procedures**
- **Access control policies**

Conduct regular audits and assessments

Schedule periodic audits to evaluate your firm's compliance posture. Use these audits to identify weaknesses and areas for improvement. Consider using automated assessment tools to streamline compliance processes and reduce the risk of human error. Here's what your audits and assessments should include:

- **Regular review of security measures**
- **Testing of incident response procedures**
- **Evaluation of third-party vendors**
- **Assessment of employee training effectiveness**
- **Monitoring of access controls**
- **Regular security updates and patches**
- **Consistent verification, testing and review of backups**

Penalties and damages for non-compliance

The consequences of failing to protect client data go far beyond immediate financial penalties, though those can be severe. Perhaps even more devastating is the long-term damage to your firm's reputation and client relationships that can follow a data breach or compliance failure. **Think about it: When clients trust you with their most sensitive financial information, they expect it to be handled with the utmost care.** And if that trust gets broken, it can be nearly impossible to rebuild—if you even get the chance to try. Understanding the implications in the following three areas is imperative.

The real cost of non-compliance

Let's talk numbers...or money. When it comes to non-compliance, the financial hit can be brutal. The FTC imposes fines for breaking the Safeguards Rule, and there are IRS penalties for ignoring Security Six protocols. According to eSudo, if a business fails to comply with its obligations under these rules, it could face civil penalties imposed by the FTC, including fines up to $43,280 per violation. That's enough to break any bottom line.

When trust walks out the door

Think of trust as your firm's foundation. Just as you wouldn't build a house on unstable ground, you can't build lasting client relationships without rock-solid trust. And here's the thing: When you drop the ball on compliance and experience a data breach, you don't just lose data and money—you lose the very thing that keeps clients coming back. And just like trying to rebuild a house after the foundation crumbles, trying to rebuild trust after a breach is an uphill battle you might not win.

PRO TIP

Want to keep client trust strong?

Make it a habit to regularly share your compliance measures with clients. It's like showing them the blueprints of how you're protecting their data.

Your reputation is on the line

Think about this: Reputational damage can have the most significant impact on accounting firms, resulting from loss of client trust. News of a breach spreads fast, and once your reputation takes a hit, it's not just your current clients you need to worry about—it's every potential client who Googles your firm's name in the future. In a profession where reputation is paramount, the damage can be devastating.



Quick look:
Common themes across regulations and standards

1. Data protection requirements

- Encryption of sensitive data
- Access controls
- Security monitoring
- Incident response planning

2. Client rights

- Transparency about data handling
- Notice of breaches
- Protection of personal information
- Access to stored information

3. Documentation requirements

- Written security policies
- Risk assessments
- Incident response plans
- Employee training records

4. Compliance obligations

- Regular assessments
- Updates to security measures
- Staff training
- Third-party vendor management

Section 7

Tools and solutions for cybersecurity

Tools and solutions for cybersecurity

Just as accountants rely on specialized software to prepare tax returns and financial statements, protecting client data requires specific tools designed for security. Modern accounting firms need a complete toolkit of cybersecurity solutions—not just a single lock on the door, but a comprehensive, layered approach to security that protects data at every point.

Essential cybersecurity tools for accountants

Modern accounting firms must adopt a multifaceted, layered approach to cybersecurity, leveraging a suite of tools and solutions that provide protection from every angle. This section explores essential cybersecurity measures both within and beyond the cloud, ensuring robust defenses for your firm's sensitive data.

Antivirus and anti-malware software

Think of antivirus software as your firm's immune system: It continuously monitors for threats, quarantines dangerous files and removes malicious code before it can spread. Today's solutions must go beyond basic virus protection to guard against sophisticated viruses, ransomware, malware and other malicious software that can encrypt your files or steal client data.

Look for solutions that:

- **Update automatically to defend against new threats.**
- **Scan files in real time as they enter your system.**
- **Monitor program behavior to catch previously unknown threats.**
- **Provide detailed reporting on blocked threats.**



PRO TIP

Regular updates matter!
Schedule regular scans and updates to keep your antivirus software effective against the latest cyberthreats.

Think about this:

Over 450,000 new malicious programs (malware) and potentially unwanted applications (PUA) are registered daily, emphasizing the need for robust antivirus solutions.

Source: AV-Test Institute

Firewalls

A firewall acts like a security guard for your network, checking the ID of every piece of data trying to enter or leave. Modern firewalls do more than just block suspicious traffic; they actively monitor network activity for signs of intrusion. You'll want to consider both hardware and software firewalls.

Hardware firewalls:

- **Protect your entire office network.**
- **Provide enterprise-level filtering.**
- **Monitor all incoming and outgoing traffic.**

Software firewalls:

- **Protect individual devices.**
- **Allow customized rules per device.**
- **Add extra protection for remote workers.**

Encryption tools

Encryption tools transform sensitive client data into an unreadable format that can only be accessed with the right key. It's like putting files in an unbreakable safe where only authorized users have the combination.

Your firm needs encryption:

- **For files stored on computers and servers.**
- **When transmitting data to clients.**
- **For email communications containing sensitive information.**
- **On mobile devices that may contain client data.**

Password management solutions

Strong passwords are essential, but managing dozens of complex passwords is nearly impossible without help. Password managers serve as a secure vault for all your login credentials. They help you create, store and manage strong, unique passwords, reducing the risk of unauthorized access.

Here's how they can help:

- **Generate random, complex passwords.**
- **Store passwords in an encrypted format.**
- **Autofill credentials securely.**
- **Allow secure password sharing when needed.**
- **Enforce password policies across your firm.**



Nearly 80% of data breaches involve phishing and the misuse of credentials (compromised), highlighting the importance of strong password practices.

Source: 2024 Verizon Data Breach Investigations Report

MFA solutions

While strong, unique passwords are essential, they are no longer enough. MFA adds extra layers of security by requiring additional proof of identity, like the following:

- **One-time codes sent via text, email or phone/voice call.**
- **Authentication apps on smartphones.**
- **Biometric verification (fingerprints or facial recognition).**
- **Physical security keys.**

Advanced cybersecurity solutions for enhanced protection

Given the amount of PII accounting firms handle, basic defenses don't provide enough protection. Firms must ensure they are taking additional measures for enhanced protection by proactively detecting and mitigating threats before they can compromise sensitive financial and client data. The following advanced tools and strategies are designed to fortify your firm's security against even the most persistent threats. The good news? A **managed security provider** can help with all of these.

Intrusion detection and prevention systems (IDPS)

These systems act like a sophisticated burglar alarm for your network, constantly monitoring for suspicious activity by:

- Watching for unusual patterns of behavior.
- Blocking known attack methods automatically.
- Alerting IT staff to potential breaches.
- Keeping detailed logs of security events.

Security information and event management (SIEM) systems

SIEM systems are like having a security command center that monitors all your defenses at once by:

- Collecting data from all security tools.
- Identifying patterns that might indicate an attack.
- Providing real-time alerts of security incidents.
- Generating compliance reports automatically.

Data loss prevention (DLP) tools

DLP tools ensure sensitive data doesn't leave your network without authorization by:

- Monitoring all data movement.
- Blocking unauthorized file transfers.
- Preventing accidental data leaks.
- Tracking sensitive information usage.

Virtual private networks (VPNs)

VPNs create a secure tunnel for data traveling over the internet, an essential component for remote workers accessing firm resources. VPNs work by:

- Encrypting all network traffic.
- Hiding network addresses from attackers.
- Preventing eavesdropping on public Wi-Fi.
- Enabling secure remote access to firm resources.

Secure cloud solutions for The Modern Firm®

Today's accounting firms face sophisticated cyberthreats that target sensitive client data, making robust security defenses essential. Just like you wouldn't trust your spam folder alone to catch malicious emails, relying on basic or outdated security measures puts your firm at risk. That's why more firms are **moving their operations to the cloud**, where expert partners handle security updates, data backups and system monitoring—letting you focus on what really matters: serving your clients with confidence.

As accounting firms increasingly move to the cloud, choosing a secure cloud platform is vital for maintaining data integrity and accessibility. Secure cloud providers offer robust security measures, including encryption, regular security audits and compliance with industry and regulatory standards.

Cloud security platforms

Cloud security brings enterprise-level protection within reach of firms of all sizes, with benefits that include:

- Automatic updates and patch management.
- 24/7 monitoring and threat detection.
- Scalable resources as your firm grows.
- Built-in backup and disaster recovery.



Backup and disaster recovery solutions

Having backups isn't just about preventing data loss; it's about ensuring business continuity. Here's what you should look for in a provider:

- Automated daily backups.
- Multiple backup locations (redundant) in Tier III or Tier IV facilities.
- Regular testing of restoration procedures.
- Quick recovery options for critical systems.



Verify security certifications!

Evaluate cloud providers based on their security certifications, such as ISO 27001, and their ability to meet your firm's specific compliance requirements.

Remember: Cybersecurity isn't a one-time purchase. It's an ongoing investment in protecting your firm's future. The right combination of tools, training, procedures and partners creates multiple layers of protection that work together to keep your clients' data safe.

Choosing the right cybersecurity solutions for your firm: A checklist

(because who doesn't love a checklist?)

Evaluation criteria

When selecting security tools, consider:

- ☑ Integration with existing systems.
- ☑ Ease of use for staff.
- ☑ Vendor reputation and support.
- ☑ Compliance with industry regulations.

Budget considerations

Balance security needs with resources by:

- ☑ Prioritizing critical protections.
- ☑ Considering total cost of ownership.
- ☑ Evaluating managed service options.
- ☑ Factoring in potential breach costs.

Tailoring solutions to your firm's needs

Your security strategy should reflect your firm's:

- ☑ Size and complexity.
- ☑ Client requirements.
- ☑ Risk tolerance.
- ☑ Regulatory obligations.

Section 8

Real-world case studies



Real-world cybersecurity cases in accounting: Learning from experience

Accounting firms just like yours have faced—and overcome—serious security challenges. Their stories show that you can protect your firm and clients while growing your business with the right approach. Let's dive into what these firms experienced in the real world.



Case study highlights: What you can learn from fellow firms

The Pagura Company: When impersonation attacks strike

What happened: A cybercriminal impersonated the company's owner, Steve Pagura, and tricked a business partner into sending tens of thousands of dollars to a fake architect. The attacker then tried to get $500,000 more by pretending to have a great lumber deal. In a third attempt, they posed as the company's financial manager, trying to redirect customer payments to fraudulent accounts.

Key takeaway: After losing tens of thousands of dollars to sophisticated impersonation attacks, The Pagura Company implemented comprehensive security measures with a trusted security partner and hasn't suffered a successful attack since.

What they learned:

- Unsecured Wi-Fi connections are a major vulnerability.
- Regular security awareness training is a must, even for senior staff.
- Having a security partner who responds quickly to threats is a must-have.

Read the full story here.

Bateman Accounting: From local storage to secure cloud

The problem: The three-person firm kept all its data on a single local computer with virtually no security protection. This firm's portal provider was unreliable and expensive and failed to maintain adequate protection for its growing client base—so much so that the firm wasn't even notified about critical security updates.

Key takeaway: Moving from a single local computer to a **secure cloud environment** transformed both security and efficiency for this three-person firm.

What changed:

- Eliminated vulnerable local storage.
- Implemented comprehensive cloud security.
- Improved client communication with security portals.
- Enhanced staff productivity.

Read the full story here.

Harsch Business Services: When client security affects your business

What happened: One of Harsch Business Services' clients suffered a devastating breach after a programmer took down the company's firewalls and never restored them. Russian cybercriminals stole PII, such as Social Security numbers, birth dates and other sensitive information. The company had spent over $100,000 trying to recover, and their survival was in question due to lost customer trust.

Key takeaway: After witnessing multiple client security breaches—including one that almost destroyed a client's business—Harsch Business Services took proactive steps to protect both their firm and educate their clients.

The impact:

- Prevented security breaches through proactive measures.
- Improved client trust through security leadership.
- Created new business opportunities through security consulting.

Read the full story here.



Setting up secure remote work environments: A checklist

Based on the success stories we've researched and studied, here are some key elements that keep your firm—and data—safe in a remote environment.

1. Cloud-based setup

- ☑ Move critical applications to a secure cloud environment.
- ☑ Use multifactor authentication.
- ☑ Get 24/7 support.

2. Employee training and rules

- ☑ Conduct regular security awareness training.
- ☑ Create clear steps for handling sensitive data.
- ☑ Implement simple ways to report suspicious activity.

3. Client communication

- ☑ Use secure portals for sharing documents.
- ☑ Outline clear security policies.
- ☑ Update clients regularly about protection measures.

What to do when things go wrong: A checklist for handling security incidents

While you will already have procedures in place (as outlined in your WISP), here's a quick and easy checklist to help you respond to a data breach.

1. First things first

- ☑ Disconnect the device from the internet (don't turn the device off, though, because that can hide the malware).
- ☑ Stop using any affected systems.
- ☑ Call your security partner.
- ☑ Write down what happened.
- ☑ Tell affected clients as required by law.

2. Long-term steps

- ☑ Figure out what went wrong.
- ☑ Add new security measures.
- ☑ Update your training.
- ☑ Be open with clients to rebuild trust.

3. Prevent future problems

- ☑ Conduct regular checkups.
- ☑ Watch for trouble.
- ☑ Plan for problems.

Remember: Every successful firm started with one step. Pick one improvement and build from there. Better yet, work with a cybersecurity partner who can handle all of these things for you.



Rightworks provides peace of mind with the total package of a secure digital environment for accounting firms

With Rightworks, your firm can enjoy complete managed cloud services, including:

- **Rightworks OneSpace: Maintain peace of mind and a competitive edge in a reliable, flexible and secure cloud environment that's customized for accounting firms, along with advanced data analytics.**
- **Rightworks Total Security: Experience enterprise-grade protection to keep your data, applications and devices safe, as well as security training for employees.**
- **Rightworks WISP: Get expert help to create your WISP—a simplified solution to your regulatory requirements from a partner that can identify and help fill your security gaps.**
- **Productivity applications: Improve workflows and give your team the tools they need, including secure email and managed Microsoft 365 applications.**
- **1:1 guidance and support: Access an expert team of tech advisors providing 24/7, award-winning support to keep your firm secure and optimized for growth.**

Rightworks is the catalyst that can set your firm on a course to greater efficiency and growth while boosting cybersecurity.



Secure your firm today!

Contact one of our technology experts at 888.210.0237, and put your firm on a secure path to stability and success. **rightworks.com/get-started**

rightworks