SmartVault

Cybersecurity is More Than Protecting Data:

3 Ways Security Can Move Your Firm Forward

Whitepaper

> The need for a proactive approach to cybersecurity is not just a matter of best practice.
>
> It's a critical imperative in safeguarding client data, ensuring legal compliance, and presenting and preserving digital trust."
>
> Luke Kiely, SmartVault, CISO

Introduction

While protecting your firm and clients' data is a crucial aspect of cybersecurity, your security program has impacts far beyond keeping your firm safe from criminals. Cybersecurity impacts your reputation, client and staff attraction and retention rates, finances, and regulatory compliance. In short, it affects the whole of your business and your ability to grow. We'll talk more about each of these throughout this whitepaper.

1. Builds Client and Staff Trust

Following cybersecurity best practices – especially when paired with technology that promotes security – increases your clients' trust in your firm. And it makes your practice more attractive to prospective clients and high-quality staff members alike.

First, let's talk about trust.

"Digital trust is dynamic and a very fragile concept," Luke Kiely, SmartVault, CISO and former cybercrime officer explains. "It can be easily eroded by a security breach, data leak, or a privacy violation." Unfortunately, these situations are becoming more common, and it's probably safe to assume you've been a victim of at least one – even if you don't know it.

Scary, right?

In 2017, Equifax lost nearly 150 million people's personal and financial information. And in 2019, Capital One had a data breach that affected 100 million people. Then in 2021, T-Mobile had a data breach that affected about 77 million people. Those are just three *big* examples, but don't let them trick you into thinking only big companies are targeted.

"Cybersecurity is – or at least should be – a paramount concern for any business of any size or industry globally," Luke says.

Let's go back to trust. He continues: "A business's reputation is influenced by digital trust, which can include online reviews, ratings, and word-of-mouth recommendations that people use to gauge trustworthiness."

> Digital trust is dynamic and a very fragile concept that a data breach or cyber incident can absolutely shatter."
>
> Luke Kiely, SmartVault, CISO

It's important to build and maintain this trust with your clients and staff. Simply put, clients won't work with you if they're convinced you can't keep their personal information secure. And you'll have difficulty finding high-quality staff if your reputation is questionable.

"In the modern workplace, a data breach or cyber incident can absolutely shatter that trust, causing customers and staff to abandon the affected business in favor of competitors with better cybersecurity and trustworthiness."

Your investment in cybersecurity, then, will not only keep your data safe, but it'll demonstrate your commitment. This helps attract new business and staff, generate referrals, and nurture lasting relationships.

Furthermore, modern clients actively seek out accounting firms that prioritize tech and data security—as is young, top-tier talent. Both of these groups have technology expertise and expect to work with an accounting practice that utilizes technology to increase security and streamline workflows, cut down on repetitive tasks, and improve communication.

Make Cybersecurity Practical and Effective

Be proactive and create a tailored program for your firm. Learn proven best practices in *The Accountant's Ultimate Guide & Checklist to Cybersecurity.*

Download Now

Your Staff Have a Vested Interest in Your Cybersecurity Processes, Too

Think your cybersecurity processes – or lack thereof – don't impact your staff? Think again. Here are five reasons why accounting firm staff care about cybersecurity:

1. Staff members want to confidently know the sensitive data they're handling is protected from breaches. Prioritizing cybersecurity helps reassure staff their work is secure.
2. Cybersecurity attacks like phishing or ransomware could significantly disrupt daily work. These disruptions would prevent your staff from completing time-sensitive tasks (resulting in more unnecessary stress). Strong cybersecurity lowers this risk.
3. Staff care about working for firms with strong reputations – the type of firm they're proud to be a part of. Robust cybersecurity preserves your firm's reputation.
4. If your firm is fined after a data breach or decides to pay ransom after a ransomware attack, it could impact your profitability and stability, perhaps putting their job security in jeopardy.
5. Job candidates in accounting are attracted to firms that demonstrate best practices in information security and use secure, modern tech to do so. Prioritizing cybersecurity strengthens your business's employer brand and helps attract top talent.

> The primary intention of compliance is to provide reasonable assurances a company has effective security controls and procedures in place."
>
> Luke Kiely, SmartVault, CISO

2. Complies with Regulatory Mandates

Accounting professionals who don't implement cybersecurity measures are vulnerable to attack and open themselves to hefty fines, penalties, and other legal consequences for not complying with mandates.

As Luke explains: "Compliance isn't intended to outright prevent a company from experiencing a security incident. The primary intention of compliance is to provide reasonable assurances a company has effective security controls and procedures in place."

A Written Information Security Plan (WISP) is one core regulatory requirement. "A WISP outlines an organization's strategy and policies for safeguarding sensitive information and ensuring data security," Luke explains. "They are a really valuable tool in helping a business enter the world of compliance and maintain a cybersecurity program."

Your WISP must specify how data is collected, stored, accessed, transmitted, and disposed of securely. Key elements include access controls, encryption, security training, and incident response plans. A comprehensive, up-to-date WISP demonstrates the firm's commitment to compliance with the best information security practices and data privacy regulations. It also helps mitigate risks like data breaches, theft, and misuse that could lead to legal liability, reputation damage, and loss of client trust if sensitive information is compromised.

The following pages provide a WISP outline to get you started.

Outline: Write a Compliant WISP

Here's what should be included in your WISP.

Section 1: Objective, Purpose, and Scope

- Define the scope and why you created the WISP
- Outline state and federal compliance obligations
- Clearly detail what is included in the plan
- Include a purpose statement that explains: what taxpayer information you collect, how you protect that information, and the processes or procedures you follow in your practice

Section 2: Identify Responsible Individuals

- List the individual(s) responsible for overseeing the program
- Designate two specific roles: the Data Security Coordinator (DSC) and Public Information Officer (PIO)
- Clearly define their responsibilities

Section 3: Risk Assessment

- Identify vulnerabilities and risks that are specific to your business, such as unauthorized access, loss of information, and use/disclosure of information
- List the information your business handles
- Define potential data loss scenarios (i.e., computer is stolen or hacked, hard copy paper files are destroyed in a fire, etc.)
- Outline how you monitor, test, and respond to risks and threats

Section 4: Inventory Hardware

- Describe all the hardware your practice uses to handle taxpayer data (i.e., desktop computer, cell phones, routers, printers, etc.)
- Explain what you use each item to accomplish
- List the location of each item and who accesses/uses them

Section 5: Document Safety Measures

- Define the policies and procedures you use to secure data
- Consider both physical, hard copy data, and electronic data
- Describe data collection and retention policies that include:
  - How much data you store and for how long and where
  - Who has access to the data
  - The plan for destroying or deleting data as needed
- Describe data disclosure policies, such as what third-party companies access the data and why, your requirements for third-party data access, and how you confirm each third-party meets privacy standards
- Describe network protection procedures, like:
  - What user protocols you have and how you monitor for unauthorized access
  - If you use firewall, anti-virus, anti-malware, and/or other security software
  - How you confirm all Operating Systems stay updated
- Describe user and remote access, such as:
  - If you use Two-Factor Authentication and/or Unsuccessful Login process
  - Your user password requirements
  - How you ensure remote access meets security requirements
- Describe process for adding new devices or software to your network, including how you confirm they meet security requirements and who approves each new software or device
- Include both an incident response plan and a breach notification plan that defines:
  - What steps you take to re-secure your devices, passwords, network, and data
  - How your DSC will notify appropriate persons of the data breach, like the IRS Stakeholder Liaison, the FTC, FBI, local law enforcement, etc.
  - The individual who is responsible for maintaining data theft liability insurance
- Define the Employee Code of Conduct and policies like:
  - Employee/contractor training
  - Employee background checks and screening
  - Non-disclosure agreements and/or privacy guidelines
  - Ensuring terminated or separated employees do not continue having access to network and data

Section 6: Draft Implementation Clause

- List the date of implementation and your firm information (name, address, etc.)
- Define how the WISP complies with the law and other applicable state regulatory requirements
- Is signed and dated by a principal operating officer or owner and your DSC

Ongoing: WISP Accessibility and Maintenance

- WISP format (i.e., PDF or Word) is easy to access and read
- Employees use WISP for training purposes
- WISP is stored safely in the cloud
- The practice reviews and revises the WISP as circumstances, new threats or risks emerge, or laws change

Note that this document is not an exhaustive list of what your WISP should include. You must consider your firm's size, complexity, and scope when writing your WISP. See the Security Summit website for additional information and requirements.

> WISPs are a really valuable tool in helping a business enter the world of compliance and maintain a cybersecurity program."
>
> Luke Kiely, SmartVault, CISO

3. Prevents Financial Loss and Business Interruptions

One of the most compelling reasons businesses prioritize cybersecurity is the protection it offers from financial loss. At the 2022 Tax Forum, the IRS made it clear that losing data is just one consequence of an attack: “Victims…may also experience financial loss due to paying the ransom, lost productivity, IT costs, legal fees, network modifications, and/or the purchase of credit monitoring services for compromised employees and customers.”

“Cyberattacks can result in significant financial damages,” Luke agrees. “Without robust cybersecurity measures in place, a single cyber incident can outright cripple a business financially, leading to, in extreme circumstances, bankruptcy.”

The Attack That Cost Over $400,000 a Day

For three months, the thieves spent time learning about the business—casing the joint, in movie parlance. They learned the names of key employees, their backgrounds, and where they lived. They knew who worked in which department and who might present an easy target. They built websites that looked just like the legitimate ones that belonged to this company—a big, nationwide organization that’s a household name but that shall remain nameless—and learned the names of their customers.

Finally, one day, they struck. An email came into a group mailbox, a place where the bystander effect is rampant and people tend to be less vigilant because they assume somebody else will be more careful. An unwitting employee opened the email and BOOM. The criminals were in.

The business struggled to survive for the next three weeks, hemorrhaging an eye-watering $400,000 a day just in operations losses. The criminals, triumphant, sent in their ransom demands, asking for hundreds of thousands more, to be paid in bitcoin, which would allow them to remain anonymous. Six months went by, and the company and law enforcement were still struggling to scope out all the places in the network the thieves could have hidden and evict them. After another six months, they were finally back in control of their data and assets, but at an enormous cost.

Why is this relevant? Because the accounting department was the criminals’ real target. Its cybersecurity was weak, and it possessed a lot of valuable financial and personal data.

An Accounting Firm Falls Victim to Ransomware

Here's another story that'll hit closer to home; it's one that Eric Green, host of the Tax Rep Network Podcast and one of the managing partners of Green & Sklarz LLC, shared on a recent episode.

"They demanded $10,000," Eric shared. "She did not have any cybersecurity [defenses], and she did not have [her data] backed up. And so, she paid them, and luckily for her, they actually released her data."

While she got her data back, experts still caution against paying ransoms. Luke noted, "The decision to pay a ransom or not has to be a business decision."

The FBI advises against payment to avoid incentivizing cybercriminals, but accountants with no backups may see no alternative. That's why it's imperative to have technology that takes care of data backup and security for you.

Proactively Protect Your Business

When you choose the right technology, you can increase cybersecurity, improve staff and client satisfaction, comply with regulations, remain competitive, and protect your firm from financial loss from fines or breaches.

Built with bank-level security and features like access control, two-factor authentication, data backup, encryption, version control, and audit trails, SmartVault helps firms of all sizes securely store, share, and collaborate on documents online – all while staying compliant with leading industry regulations. At the same time, SmartVault's intuitive cloud-based interface makes it easy for accountants to collaborate on projects with clients.