



Practical Cybersecurity: Cost-Effective, Straightforward Strategies for Financial Institutions



SmartVault

Whitepaper

Table of Contents

Education is Your Best Defense	1
Common Cyberattack Methods	1
Evaluate Your Risks	2
Create a Plan + Follow Best Practices	3
Create a Cybersecurity Plan	3
Build a Security Culture	7
Regularly Backup Your Data	9
Use Multi-Factor Authentication	11
Consider Personal Device Use	12
Follow Security Best Practices	13
Protect Your Data Like You Protect Their Money	14
Implement a Document Management System	14

Cybercrime is a reality for every modern business, regardless of their size. In fact, many cybercriminals consider smaller businesses — like community banks and credit unions — prime targets. Why? For one, they know ***your institution is a goldmine***: From Social Security numbers to birthdates and addresses, your files have exactly what criminals need to steal identities, make money by selling the stolen data on the black market, and more. Secondly, criminals assume smaller institutions don't have strong security processes.

Don't be an easy target. In this whitepaper, you'll learn measures you can quickly implement to protect your institution. We'll also discuss how cybercriminals target financial institutions and how you're legally obligated to keep data safe.

“Without robust cybersecurity measures in place,” Luke Kiely, SmartVault, CISO and former cybercrime officer warns, “a single cyber incident can outright cripple a business financially, leading to, in extreme circumstances, bankruptcy.”

Education is Your Best Defense

It's often said, "The best defense is a good offense." The same is true for cybersecurity. Protecting yourself from cybercriminals is about being proactive. You must learn how criminals infiltrate systems and how vulnerable your systems are. This will help you develop a cybersecurity plan specific to your needs.

Common Cyberattack Methods



Malware

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



Phishing

This attack lures people into disclosing their personal information, like passwords and Social Security numbers, by making the victim believe the message and request are trustworthy. These attempts are usually performed via email or text message and appear to come from known, trusted sources, like your team members, customers, vendors, or big-box stores.




Ransomware

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



Man-in-the-Middle (MitM)

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



Cybersecurity is – or at least should be – a paramount concern for any business of any size or industry globally.”

Luke Kiely, SmartVault, CISO

Evaluate Your Risks

There are four main types of weaknesses financial institutions need to keep an eye out for:



Process vulnerabilities. These occur when the procedures you’ve implemented to safeguard your system aren’t sufficient. Examples include weak passwords.



Network vulnerabilities. These are problems in your software or hardware that put you at risk of a cyberattack, such as using a Wi-Fi network with weak security.



Operating system vulnerabilities. These are issues with an operating system (OS) that allow hackers to access any device that uses that OS. Not updating your software leaves you at risk of an OS vulnerability.



Human vulnerabilities. Another way to put this is “human error.” This term refers to anything a user does that makes a system vulnerable to attack, and it’s the most common source of weakness. Examples abound; they include things like clicking on an email attachment that’s infected with malware, failing to update an operating system, or storing sensitive information on a server that’s not secure.

As you identify the areas of vulnerability, make them a top priority to fix. In the next section, we’ll go over some straightforward things you can do right now.

Create a Plan + Follow Best Practices

As you can see, cyberthieves have many clever ways to steal information. And unfortunately, cybercrime is not only here to stay, but it's on the rise: Some reports suggest attacks now happen every 39 seconds, and the cost of these crimes is expected to skyrocket to [\\$10.5 trillion per year](#) by 2025, up from \$6 trillion in 2022.

The takeaway: If you haven't taken the proper steps to protect yourself, it's not a question of if you'll be hacked, but when.

“The only thing worse than a data breach is multiple data breaches. Take steps so it doesn't happen again.”

Federal Trade Commission, [Data Breach Response: A Guide for Business](#)

Create a Cybersecurity Plan

Financial institutions that don't implement cybersecurity measures are vulnerable to an attack and potentially open themselves to hefty fines, penalties, and other consequences for failing to comply with regulations, of which there are several.

The [Gramm-Leach-Bliley Act \(GLBA\)](#) is the most robust. It requires financial institutions covered by the rule to “develop, implement, and maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.”

A subset of GLBA is the Safeguards Rule that requires a Written Information Security Plan (WISP), which “outlines an organization's strategy and policies for safeguarding sensitive information and ensuring data security,” according to Luke.

Whether your institution is covered by the FTC or another regulatory body, following the requirements in the WISP can help you create and maintain a strong cybersecurity program.

A comprehensive, up-to-date plan demonstrates your commitment to the strongest security practices. It also helps mitigate risks like data breaches, theft, and misuse that could lead to legal liability, reputation damage, and loss of customer trust if sensitive information is compromised.

We provide a checklist on the following pages to get you started in developing your written security plan.



Checklist: Writing a Security Plan

Use this checklist as a guideline for creating your security plan. There are multiple regulatory bodies that mandate how financial institutions should protect data. Check your state and federal laws for specific requirements for your institution.

Section 1: Objective, Purpose, and Scope

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

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 customer 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 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.)
- Ensure your plan complies with the law and other applicable state regulatory requirements

Ongoing: Accessibility and Maintenance

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

Note that this document is not an exhaustive list of what your security program should include. Check applicable regulations for additional information and requirements.

The fallout of a cyberattack



Lost data,
productivity,
& revenue



Damaged
relationships
& reputation



Significant
stress & anxiety



Penalties,
fines, & costly
recovery efforts

Cybersecurity Checklist: Stay Protected Against Data Breaches

How many must-have
security protocols do you
have implemented today?

[Download the Checklist](#)



Build a Security Culture

We know that robust cybersecurity programs are crucial. What's equally important – and often overlooked – though, is communicating your program to your staff. You can have the strongest cybersecurity program, but the simple fact of the matter is: if no one knows their roles or follows your policies, your business will be exposed to unnecessary risk.

It's no surprise, then, that employee education and training is one of the most vital components of an effective cybersecurity program. “The biggest portion of insider threats is what I call the careless or negligent insider,” Luke explains. “That's where you have employees or contractors who may accidentally compromise security by mishandling data, using weak passwords, or [falling victim to a phishing attack](#).”

It's not as simple as asking people to read your program, though. You need to create a security culture, which the [National Protective Security Authority](#) defines as “the set of values, shared by everyone in an organization, that determine how people are expected to think about and approach security.”

Building and maintaining this culture requires effective, ongoing communication that ensures everyone understands and takes accountability for keeping data safe. It also needs to be a priority from the top down. Executives and managers must understand the importance of cybersecurity and lead by example.

Following are tips and insights from cybersecurity experts on how to build a security culture.

Keep Training Simple

“Having simple policies and procedures for staff to digest and follow is the starting point to a successful program,” Luke explains. Avoid overwhelming staff with technical jargon and too much information. Instead, Luke recommends “keeping it simple and focusing on key policies relevant to each person’s role.” Also, don’t just rely on one form of communication, as people learn in different ways. Offer a mix of in-person training, videos, ‘how to’ guides, FAQ articles, and more.

Focus On the Why and the How

A common mistake businesses make is centering the training on why cybersecurity is important; while that’s crucial for your team to understand, your training needs to be much more robust to be effective.

“You have to teach them what their specific role is and how they should respond to a cyberattack,” Luke explains. “When you think about phishing emails, for example, it is critical that staff are trained to identify them and what to do if they receive one.” Luke also encourages businesses to take training further by rehearsing cybersecurity incidents and practicing their response plans. “These rehearsals include your staff, but also IT, legal, senior management, and potentially your HR and public relations teams...anyone who will be a critical decision-maker in the event of a cybersecurity incident.”

Educate and Train Multiple Times a Year

Cybersecurity threats constantly evolve, so it’s important to ensure staff understand and follow the latest best practices. Quarterly or biannual training helps keep policies top of mind. If you think your staff will balk at multiple trainings a year, consider how it’ll help them in their personal lives as well. Hackers, after all, don’t just attack businesses. Your staff can implement what they learn through the training to protect their personal accounts.

Avoid the Blame Game

When errors happen, you must balance accountability with learning. “Do not criticize, blame, and target people who don’t do the right things,” Luke says. “As soon as you start doing that, you create a bad culture,” where suddenly people may be discouraged from reporting incidents. Instead, focus on constructive feedback and improvement. Encourage staff to ask questions and report suspicious emails or activities without fear of reprimand – and always thank staff for voicing their concerns or reporting incidents. Use mistakes as an opportunity to improve your company’s security defenses and maintain a blame-free response to encourage continued transparency.

Regularly Backup Your Data

While “data loss” and “disaster” make many people think of once-in-a-generation weather events, they’re mainly caused by more ubiquitous things. How many times have you lost power, misplaced a flash drive, had a computer malfunction, or accidentally deleted or saved over a file? It happens quite a bit!

Depending on the type and amount of data missing – and how it went missing (human error versus cyberattack, for example) – data loss can be a significant interruption that causes you to lose money and time. Some events, like floods, fires, or thefts, can cause your office to close its doors and work virtually.

If you want your business to move forward and continue operating, you’ll need access to your files.



Data Backup Best Practices

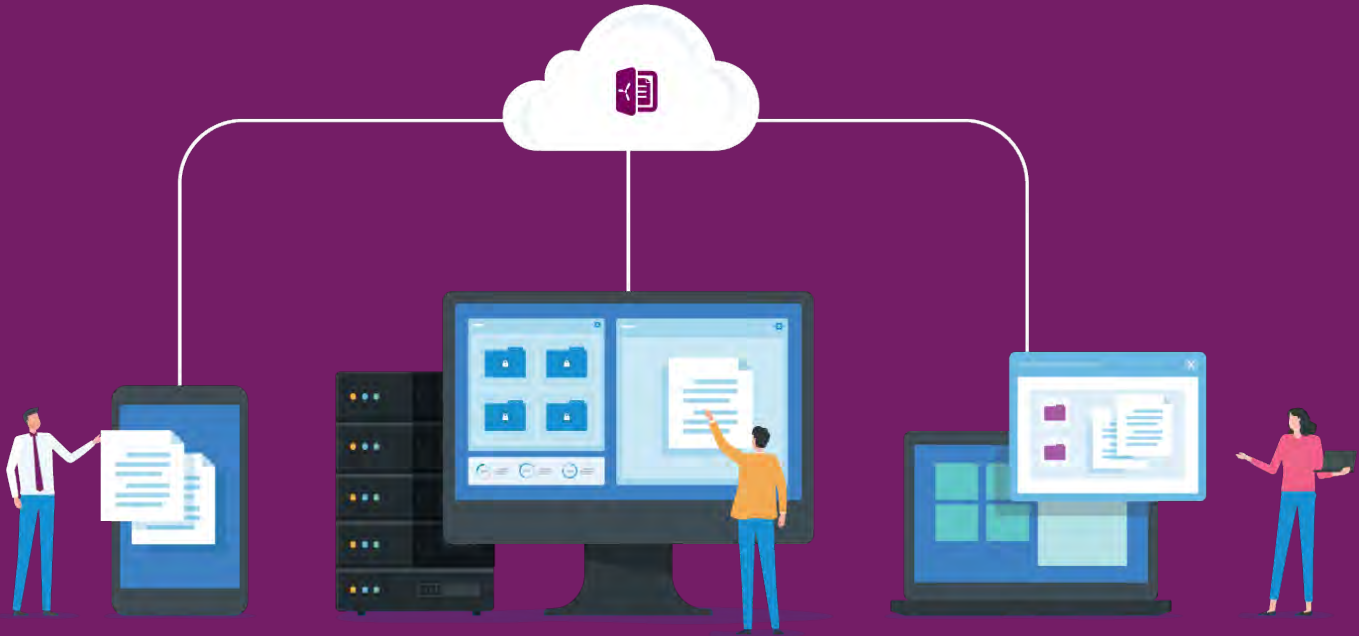
Many businesses still operate with one computer that contains all their customer data, and many frequently don’t have data backups. Even in this digital age, some still work with hardcopy paperwork stored in their desks or filing cabinets. This could all lead to some significant problems. Regardless of the reason, “If you can no longer access your data, you can no longer deliver service,” Luke warns. “The business stops, and you start losing money.”

The best way to prevent and recover from loss is to [have your documents in the cloud](#). Why?

Cloud vendors have greater resources and invest heavily in ensuring their customers’ data stays safe. You’ll benefit from advanced security measures like automatic data backup, file versioning, activity tracking, bank-level encryption, granular access controls, and multi-factor authentication (MFA). Whether you experience an office fire or a computer malfunction, the cloud makes it significantly easier for you to recover and get back up and running.

Cloud providers store your data on multiple remote servers, which they maintain and back up regularly so you don’t even have to think about it. Features like automatic file locking prevent people from working on a file simultaneously, and if someone accidentally deletes or overrides a file, you can quickly find the previous version through its version history.

There are other benefits beyond better security: Modern clients expect modern banks. They want to easily and quickly communicate and collaborate with you online. They want streamlined processes and to submit, review, and e-sign everything from the comfort of their homes or mobile devices.



Six reasons to proactively prepare for data loss

- 1 Disasters can happen to anyone.** A flood, ransomware attack, a simple human error, or a computer failure can strike anytime.
- 2 Lost data may be impossible to get back.** It can be incredibly difficult, if not impossible, to retrieve lost files and information if you don't have proper backups.
- 3 Downtime equals closed business.** Data loss leads to less (or zero) productivity, revenue, and opportunities.
- 4 Restoring is time-consuming.** Thoughtful disaster planning speeds up recovery so you can get back up and running fast.
- 5 Your reputation will be destroyed.** If you can't quickly recover or the hacker publishes the data or sells it to another criminal, customers will lose confidence in your business, leaving you for a competitor and not referring you to others.
- 6 Penalties can apply.** You can face fines for misplacing sensitive customer data.

Use Multi-Factor Authentication

Despite being widely available, uptake of multi-factor authentication (MFA) is still relatively low. Luke says, “We talk a lot about secure passwords, but the reality is that it doesn’t matter how good your password is if it’s not used with other layers of security, and a password is not likely to be good enough to secure access to valuable online services by itself.”

MFA, including two-factor authentication (2FA), is an extra layer of security for online services. It is becoming a routine, built-in feature for many services, such as email, cloud file storage, and payment methods. It will usually be a case of enabling this feature within the online service. If your service doesn’t provide this feature, consider whether you can continue to rely on that service. A password can be easy to steal or guess, and yes, a second factor can also be stolen. But stealing a matching pair is much more difficult.

“It doesn’t matter how good your password is if it’s not used with other layers of security.”

Luke Kiely, SmartVault, CISO

It’s About More Than Security: How Digital Trust Can Make or Break Your Bank

“Digital trust is dynamic and a very fragile concept that can be easily eroded by a security breach, data leak, or a privacy violation,” says Luke Kiely, SmartVault, CISO.

“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.”

It’s important to build and maintain this trust with your customers and staff.

“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 customers and staff, generate referrals, and nurture lasting relationships.

Consider Personal Device Use

Mobile technology is an essential part of a modern business. There is so much data being stored on tablets and smartphones every day. What's more, because they often leave the safety of the office (and home), they need more protection than "desktop" equipment. In an effort to embrace the ubiquity of technology and to cut down on costs, many businesses allow staff to "bring your own device" (BYOD) to work. However, this poses a security risk.

Each institution should consider the use of BYOD in the workplace and avoid such solutions becoming permanent without considering how much risk you're willing to accept. After all, BYOD means corporate data is being processed or residing on personal devices.

From a legal perspective, the responsibility for protecting information typically rests with the business, not the device owner. As such, you should understand the relevant data protection laws and regulations for your industry and location, and you need to consider how any commercial or partner agreements are affected by adopting BYOD.

Whatever BYOD approach you take, it is highly recommended that a set of mitigations are implemented to protect data. Luke has a few suggestions, including "setting the minimum services and data available to a personal device, employing strong authentication approaches, and monitoring the service and data being accessed."



Follow Security Best Practices

Cyberattacks are becoming more sophisticated, but basic protection remains the same. Here are some additional practices to consider:

Strong, Unique Passwords

The strongest passwords have letters, symbols, and numbers. It's also important not to use the same password across multiple devices or accounts. You can use a password manager to help you remember unique passwords. Set passwords to expire regularly and ensure your vendors have appropriate password requirements and policies.

Set Access Permissions

Configure user permissions to granularly separate access to data and folders and the actions each person can take (read-only, edit, delete, etc.) with your files and folders.

Leverage Antivirus and Anti-Malware Software

Antivirus software helps detect, block, and remove viruses before they can infect a system. Anti-malware programs identify and neutralize other forms of malicious software. Running comprehensive antivirus and anti-malware scans regularly allows you to proactively catch and mitigate threats before they have a chance to do harm.

Software Updates

Too many people increase their vulnerability by ignoring or postponing software updates. Even though updates can be time-consuming and frustrating, they're necessary because viruses and malware change and adapt constantly. Upgrade your modems, routers, hardware firewalls, and computer CPUs at least every 3-5 years. Make sure your team configures devices to automatically update.

Be Wary of Public Wi-Fi

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

Partner with Security-First Vendors

Since it's their products and their reputations are incumbent on their solutions being as secure as possible, your DMS vendor will be up to date on the latest risks and can help you maximize their solution to ensure you're not vulnerable.

Protect Your Data Like You Protect Their Money

Financial institutions handle a high volume of documents daily, from loan applications to identification forms, bank statements, and more. Without an organized system for securely storing, managing, and accessing these documents, important files can be lost, misplaced, or mishandled. This is where a document management system and client portal comes in.

Implement a Document Management System

One of your top priorities should be implementing a [document management system \(DMS\)](#) that's integrated with a client portal. A DMS provides financial institutions with the organization, security, and efficiency they need to stay compliant and better serve customers. Here are things you should look for in a DMS:

- Bank-level security that'll protect your data with the strongest security measures
- Automated cloud backups for availability if your local systems are damaged, lost, etc.
- Version control and activity tracking to preserve history and access previous versions
- Encryption at rest and transit and robust access controls to restrict who can view, edit, and delete documents
- Mobile access so you can access and collaborate on documents from anywhere
- Indexing and search to quickly find documents
- An integrated client portal to collaborate online



Streamlining Executive Team and Board Alignment While Strengthening Security

To deliver on their commitment to its 125,000 members' financial success, Frontwave's Board and Executive Team must stay aligned through clear communication facilitated by the Executive Administrator (EA).

To make sharing and collaborating on documents easy and secure, the EA uses SmartVault, a cloud-based document management system. "Since I joined Frontwave three years ago, SmartVault has become engrained into my work managing board materials," the EA explains. "I enjoy using the system because it's user-friendly, and it's easy to navigate and find the documents we need."

SmartVault provides a centralized, secure location that empowers the EA to easily share and maintain confidential documents. "Sharing files via email poses a significant risk," the EA says.

"I appreciate how SmartVault enables us to be more secure by giving us one place to upload documents."

SmartVault's granular permissions, encryption, and other bank-level security measures help protect sensitive information, giving Frontwave and its members peace of mind that their data is protected from breaches and data loss.

[Read the Story](#)

6 Reasons You Need a DMS

For community banks and credit unions, technology that improves efficiency and the customer experience is key to remaining competitive with larger financial institutions. Implementing a document management system and client portal can provide significant benefits for your financial organization, customers, and teams. Here are six:

1. Builds Your Community

Technology like document management and client portals allow smaller financial institutions to provide amazing service that feels super personalized – and it's this great service that keeps customers happy and encourages them to recommend you to their friends and neighbors. As you continue to scale and build relationships with the people in your area, they'll see your commitment to providing financial services that help their neighborhoods grow and prosper.

2. Simplifies Customer Collaboration

Working in the cloud can solve everyday headaches you experience when working with customers, such as playing phone tag to remind them to complete a form or resending important information to a customer who lost your first email in their inbox. These situations, while minor, are frustrating for both parties and make your business look disorganized and difficult to work with. Client portals give customers access to their own documents, so they can securely log in to access, share, review, complete, and eSign documents 24/7. This is more convenient than having to call or visit a branch during business hours, increasing customer satisfaction – which means increased referrals. Portals enable staff to share documents and information with customers instantly as well.

3. Makes Employees Happier (and More Efficient)

The cloud is a highly effective way to streamline your process, facilitate communication, and make your teams' experiences positive. Digitizing processes eliminates the need for physical files, helps staff save time on admin tasks, and makes it easy for employees across branches to collaborate. Having a central repository for files also makes it faster to retrieve information and provide excellent service. The ability to work remotely also gives staff flexibility.

4. Creates User-Friendly Processes

Traditional software requires everyone to spend time learning how to use it, which creates a major barrier to making even necessary changes. Cloud software, however, is designed to be user-friendly and intuitive, regardless of how tech-savvy a person is. Not only will you be able to come up to speed on the features quickly, but you can rest assured your customers and employees, regardless of their skill level when it comes to tech, will have an easier time as well. Upgrading to the cloud will also make your system more accessible.

5. Secures Your Data

Cloud vendors have greater resources and invest heavily in ensuring their customers' data stays safe. You'll benefit from advanced security measures like automatic data backup, file versioning, activity tracking, bank-level encryption, and multi-factor authentication (MFA). And granular access controls let you be in 100% control of who accesses what folders and documents. These security standards create peace of mind for your team and customers and can help you meet the most stringent industry regulations with ease.

6. Keeps You Up and Running

Whether you experience a building fire, a computer malfunction, or someone accidentally deleting a file, the cloud makes it significantly easier for you to recover and get back up and running. Cloud providers store your data on multiple remote servers, which they maintain and back up regularly. They'll help you restore your data quickly. Better still, using the cloud actually reduces your vulnerability to disasters. Storing your information on remote rather than on-premise servers means that even if a flood or other weather event impacts your home or office, you won't lose everything.

Over 3 million people securely gather, store, share, and eSign documents in the cloud with SmartVault.

With SmartVault, you'll have a cloud-based document management system and client portal that prioritizes security and compliance and makes it more secure for you, your staff, and your customers to work together online.

Learn more or schedule a demo: www.smartvault.com