SmartVault

Don’t Lose Your Data:

A Blueprint for Secure Backup, Recovery, and Business Continuity

Whitepaper

SmartVault

Data Loss & Disasters: More Common Than You Think

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!

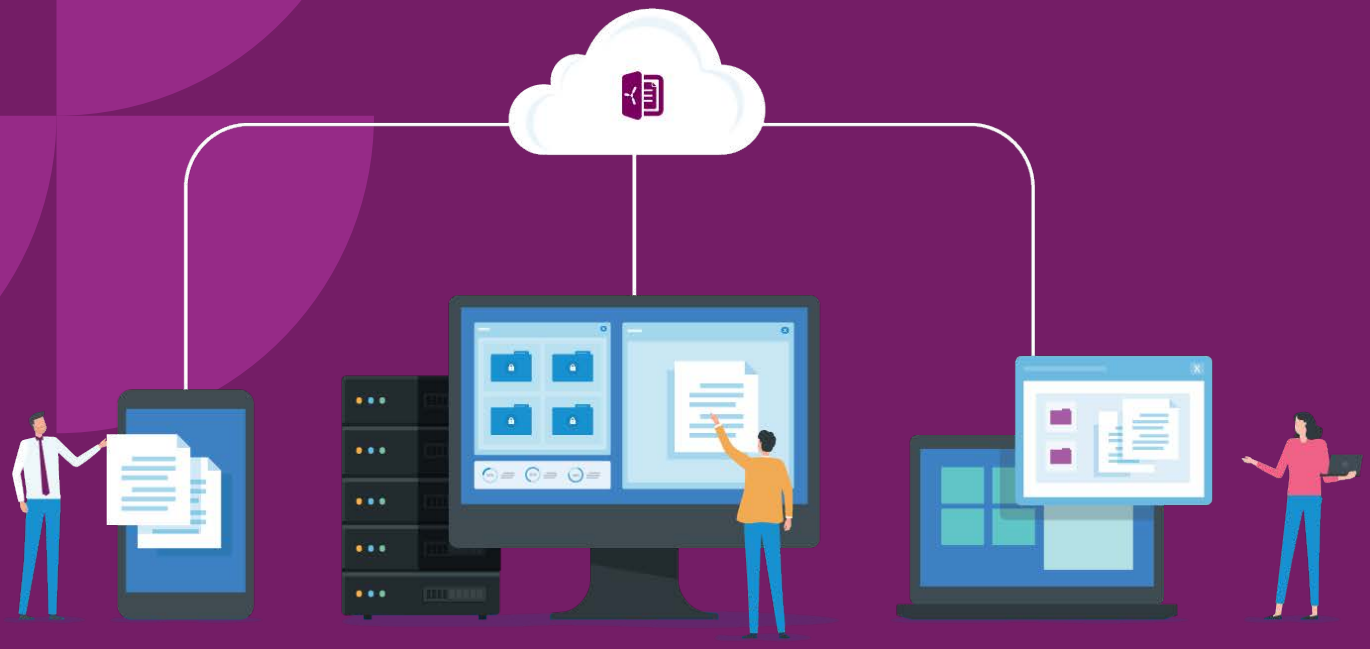
Depending on the type and amount of data missing – and how it went missing (human error versus cyberattack, for example) – data loss can be a significant interruption that causes you to lose money and time. Some events, like floods, fires, or thefts, can cause your office to close its doors and work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

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

That’s where your data backup procedures and disaster recovery plan come into play. Your backup procedures – a core part of your overall plan – should ensure you have access to your files, even when something happens to your computer or the original documents.

Your disaster recovery plan is your blueprint for responding to and recovering from data loss events or losing access to your office, computers, or any place you store your documents.

This eBook discusses creating data backup procedures, protecting yourself from data loss, and preparing your firm for a fast recovery if you experience an event.



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, clients 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.

Data Backup:
Your Key to Fast Recovery

Many businesses still operate with one computer that contains all their client 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, according to Luke Kiely, SmartVault CISO, and Eric Green, Founder of the Tax Rep Network and Partner at Green & Sklarz, LLC.

Regardless of the reason, "If you can no longer access your data, you can no longer deliver service," Luke warned on a recent Tax Rep Network Podcast. "The business stops, and you start losing money."

Backing up your data lets you quickly restore files when they're lost or corrupted. In the same podcast, Eric shared a story about a client who lost all their documents when an apartment in the building caught fire, kicking on the fire suppression system. "If you've never been in that," Eric started, "it's not like a little bit of water spray. It destroys everything." The water seeped into the storage room below and flooded the client's filing cabinets. It turned their documents into "paper mache." Of course, this happened right after they received an audit notice. A forensic expert had to reconstruct the destroyed files.

Another of Eric's clients fell victim to a ransomware attack, where an attacker encrypted their data and demanded payment for the decryption key. "They demanded $10,000," he recalled. "She did not have her data backed up, so she paid them. Luckily for her, they released everything." However, she could've quickly recovered, continued operating her business, and avoided paying the ransom if her data had been securely backed up and readily accessible.

Yes, those scenarios are rare, but don't use that as an excuse not to be prepared. You also need data backups for smaller, more common events, like when someone accidentally deletes a file or has their computer stolen.

Having reliable backups makes recovery quicker, far more possible, and much more affordable.

Data Backup Best Practices

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 accountants. 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.

When everything you do is online, you also open your client base to anyone around the globe. And, you can hire staff from anywhere instead of being limited to those who will come into a physical office. This means higher growth and scalability.

You Need a Cloud-Based DMS

A cloud-based DMS enables an efficient workflow and a positive, high-quality client experience – both are crucial to your firm's productivity and profitability, says Executive Vice President of K2 Enterprises and Accounting Today Top 100 Most Influential alum Randy Johnston.

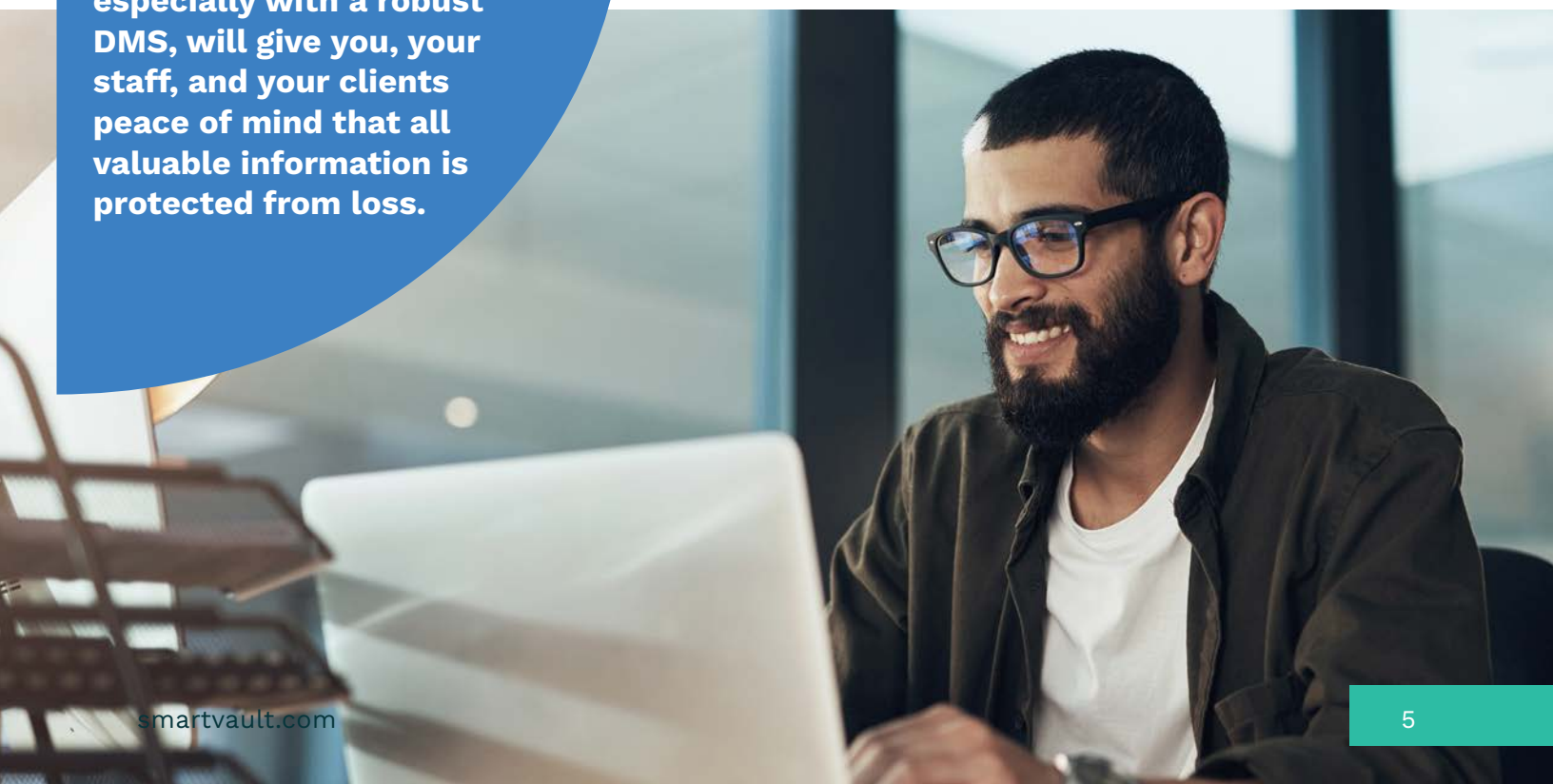
Johnston says many accounting professionals haven't updated their document storage solution since the 1990s because they either don't know how or are unaware of the new software programs that have replaced the previous clunky ones. This could be why, even today, many firms are still struggling with the mundane tasks of gathering client documents, tracking everything, and delivering accurate reports and analyses.

So, what exactly should you look for as you search for options? You'll need features like:

- Automated cloud backups for availability if your local systems are damaged, lost, attacked, stolen, etc.
- Version control and activity tracking to preserve document history and quickly access previous versions
- Encryption at rest and transit, as well as 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 find the documents you need quickly
- An integrated client portal for clients to collaborate with you and submit their documents online
- Integrations with the tax, accounting, and administrative programs your firm already uses

But data recovery isn't the only component you need to consider. The next section discusses why you need a comprehensive disaster recovery plan and how to create one specific for your practice.

Data recovery procedures, especially with a robust DMS, will give you, your staff, and your clients peace of mind that all valuable information is protected from loss.



Disaster Recovery Plan:

Your Recovery Blueprint

As we just covered: If you cannot access your data and documents (for a day or an extended time), you'll consequently experience lost productivity and revenue. Data backup is significant to recovery, but you'll need a complete disaster recovery plan to fully prepare.

So, what else do you need to consider? Your plan should help you:

1

prevent data loss events

2

prepare for any that may occur

3

quickly recover if you experience one

Ideally, your plan is centered around your document management system (DMS). Your DMS is the backbone of your preparations and recovery because it helps you securely store your files and quickly recover lost data.

The Goal of a Disaster Recovery Plan:

Minimize downtime and data loss by implementing backups and documented processes that can rapidly restore your business operations.

Critical Elements of Your Plan

A disaster recovery plan typically involves several key components:

Backups

Regularly backing up critical data and systems to the cloud. This ensures that a recent copy can be restored in case of loss or corruption.

Secondary Infrastructure

Having redundant infrastructure like servers, networks, and storage in a separate physical location. These redundant systems can take over if the primary infrastructure is damaged.

Restoration Procedures

Documented processes for restoring data and rebuilding systems. This includes prioritizing critical systems, data, and components for restoration.

Offsite Storage

Storing backup data offsite so that a single disaster – like an office fire – cannot affect both your primary and backup data. This is another reason why secure cloud storage is paramount.

Alternative Worksite

Identifying and equipping an alternative workspace to allow operations to resume if your primary office is inaccessible. Remote work capabilities, and ideally having your data in the cloud, lets this happen quickly.

Testing

Regularly testing the plan to validate it works. This includes simulated disasters and failure scenarios to exercise the response process.

Team Roles

Defining roles and responsibilities for response staff and providing appropriate training. This ensures accountability and effective coordination.

Checklist:

Create Your Disaster Recovery Plan

Here is a checklist of core components you can use as a starting point for your plan:

1. *Executive Summary*

- ☐ Write a brief overview of the plan's purpose, scope, roles, and key recovery strategies

2. *Business Impact Analysis*

- ☐ Identify critical business functions, recovery time objectives, and impacts of disruption
- ☐ Prioritize business processes and data for recovery
- ☐ Create a data map that lists all the systems you use today, what information is stored on each system (client and business data), and who can access these systems

3. *Roles and Responsibilities*

- ☐ Define roles and responsibilities before, during, and after a disaster
- ☐ Designate primary and backup personnel for each role
- ☐ Outline emergency decision-making hierarchy

4. *Communication Plan*

- ☐ Specify communication channels and protocols for status updates during disasters
- ☐ Define a plan and draft communications for employees, clients, vendors, media, stakeholders, regulators, etc.
- ☐ Ensure contact information for employees, vendors, and clients is up-to-date and that it's stored in the cloud so you can access it from anywhere

5. *Recovery Procedures*

- ☐ Document step-by-step procedures to recover IT systems, data, and infrastructure
- ☐ Include application-specific recovery steps
- ☐ Create a plan to access the physical location of the business to evaluate physical and/or network damage and determine safety and accessibility by employees
- ☐ Address strategies for alternate work locations, including remote work policies

6. *Vendor Contact List*

- ☐ Maintain updated contact info for vendors critical to recovery operations
- ☐ List may include cloud services, hardware vendors, ISPs, equipment suppliers, etc.

7. *Testing Plan*

- ☐ Schedule periodic plan testing, table-top exercises, and drills
- ☐ Test scenarios for different types of disasters
- ☐ Document lessons learned and update plan after each exercise

SmartVault

Recover Faster With a DMS

By leveraging a secure document management system for storing documents, you can have confidence that your data will remain protected and accessible after a data loss event or even during an unexpected disaster like an office fire. This allows you to rapidly resume operations and serve your clients again.

Over 30,000 accountants and their clients securely gather, store, share, and eSign documents in the cloud with SmartVault.

Online Document Storage

Standardize and centralize your business documents.

Secure File Sharing

Share files easy, compliant, and secure.

Branded Client Portal

Give clients a professional way to work with you.

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