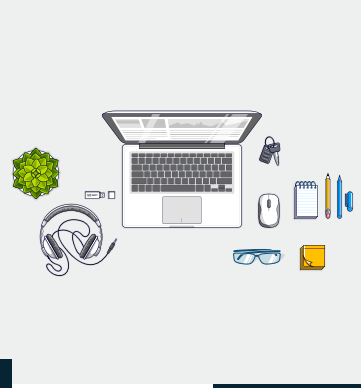
SPANNING
A Kaseya COMPANY

7 Key Steps to Quick Data Recovery

CONTENTS



Introduction

In today's always-on business environment, data loss due to human error, cyberattack or natural disaster can have a devastating impact on your business. Besides the time and effort required to restore information, it can result in huge financial losses, lost customers, and could potentially put you out of business for good.

Data loss is inevitable. Businesses lose four million files daily, which is equivalent to 44 files every second. Data loss can be caused by hardware or software failure, cyberattacks, malicious insiders or human mistakes. According to a study conducted by researchers from Stanford University and cybersecurity firm Tessian, 88% of data breaches occur due to employee mistakes.

Cybercrimes are increasing at an alarming rate. The FBI reported a whopping 300% increase in reported cybercrimes since the onset of the COVID-19 crisis. The number of cyberattacks peaked at a record-breaking 925 attacks a week per organization at the end of 2021. Cyberattacks are becoming more advanced, unpredictable and can occur at any time. As rampant cyberattacks continue to wreak havoc on all businesses across industries, security experts expect the frequency and intensity to further increase in 2022 and beyond.

According to the Ponemon Institute and IBM's Cost of a Data Breach Report 2021, the average total cost of a data breach reached $4.24 million in 2021. The report indicates a 10% year-over-year increase in average total cost, which is the highest ever recorded in the 17-year history of the report. Cybersecurity Ventures estimates global cybercrime costs to reach $10.5 trillion annually by 2025.

With so much at stake, developing a robust data backup and recovery strategy seems obvious. Unfortunately, more than 50% of organizations across the globe don't have a business continuity plan. Modern companies rely heavily on information to conduct day-to-day operations. As such, a data breach incident could not only hinder critical processes, but also bring your business to a grinding halt. A comprehensive data backup and recovery strategy, on the other hand, can help your business stay afloat and enable business continuity when crises do occur.

This eBook will shed light on the common causes of data loss, the importance of data recovery for businesses and the seven key steps to quick data recovery. It will help your organization prepare for cybersecurity incidents that result in data loss.

Common causes of data loss

Data loss incidents occur when information is either destroyed, corrupted, deleted, unreadable or inaccessible. There are several factors that could lead to data loss, and each poses a unique data recovery challenge. Listed below are some common causes of data loss:

User error

It goes without saying that humans make mistakes. Accidental deletion of files, physical damage due to inattentiveness and configuration errors due to inexperience are some common mistakes made by users.

Hardware and software failures

Hardware failure is responsible for data loss in 40% of cases. Hardware, such as a hard disk drives, can malfunction or fail due to misuse, rough handling, dropping a computer or laptop, overheating or dust accumulation.

Software failure is also one of the leading causes of data loss. For example, a file editing software may fail to save or update files, resulting in files being corrupted or damaged in the process. An antivirus software may sometimes wrongly identify a "safe" file as malware and delete it. There are numerous instances where an error during the backup process has resulted in data loss.

Viruses and malware

New variants of viruses and malware appear every day that increase the risk of data loss. Viruses and malware can cause serious trouble since an infection on a single machine can quickly spread to other systems, ultimately taking down the entire IT system.

Theft

Mobility has become synonymous with the modern workplace. With employees increasingly working while on the move on their laptops, smartphones and tablets rather than PCs, these mobile devices can pose a serious threat to data loss if left unattended.

Power failure

Sudden power outages can shut down your company's IT systems temporarily as well as lead to loss of unsaved work. Power failures can damage hardware and other components resulting in data loss. Improper software shutdowns due to unexpected power failure can also result in the loss of valuable data.

Consequences of data loss

No business is immune to data loss. It can strike at any time and have disastrous impacts on your business. Here are five major consequences of data loss:

Productivity disruption

Data loss due to an unplanned power outage, hardware/software failure, virus or cyberattack will have a direct impact on employee productivity. It may take hours or even days to recover lost data, which leads to downtime and lost sales.

Financial loss

Downtime due to data loss means your business isn't making any money. This coupled with the cost of recovering your lost data can add up to a substantial loss of revenue.

Tarnished brand image

One of the major disadvantages of doing business in the digital age is that news travels at lightning-speed. The news of your company suffering a data loss incident can cause irreparable damage to your company's reputation.

Exposure of confidential information

Data loss resulting from negligence or theft can expose sensitive information like customer data, employee records, etc. Failing to comply with data protection and privacy laws like the European Union's (EU's) General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), etc, can result in hefty fines. The affected customers can also take legal action against your company.

Loss of customer loyalty

Discontent customers, especially those whose data has been compromised, can't trust your company with their sensitive personal data. Continuing to do business with your company would mean putting their data at risk. Winning back lost clients will require a significant amount of time, effort and resources.

Best practices to prevent data loss

Data loss is not a matter of if but when. That's why it's critical to make sure your precious data is securely backed up, protected and available for recovery in case of emergencies. Here are some effective ways to prevent data loss:

Back up data

Human mistakes are bound to happen and cyberattacks are rampant. Having a backup copy of your mission-critical data will ensure your business never stops when disruptive incidents do occur.

Control access to company data

Limit employee access to only those files and folders that are needed to accomplish their day-to-day tasks. This will help reduce the risk of accidental deletion and unauthorized access to confidential data. You must train your employees about data confidentiality and how it should be shared.

Use antivirus and antimalware programs

Using antivirus and antimalware software can go a long way toward preventing viruses and malware from infecting your systems and network. Make sure to keep your antivirus and antimalware programs up to date so they run effectively.

Patch your software and operating system

Make sure to install the latest OS and software versions as soon as they are made available by vendors. This will reduce the risk of bugs and system errors that could lead to data loss.

Develop a data loss prevention (DLP) strategy

DLP refers to the tools and techniques that help network administrators monitor and manage the data being transmitted. This helps prevent employees from sending confidential data outside an organization. DLP technologies help protect your data while it is in use, in motion and at rest.

Bonus preventive measures

As a preventative measure, it is crucial to stop data loss before it occurs by ensuring your organization leverages layered strategies such as:

1. Credentials Exposure Monitoring: A solution that combines human and machine intelligence with powerful search capabilities to scour the dark web to identify, analyze and proactively monitor for an organization's compromised credentials 24/7/365, alerting you to troubleshoot quickly.

2. Security awareness training: Transform your biggest attack surface into your biggest defensive asset with engaging content and customizable materials.

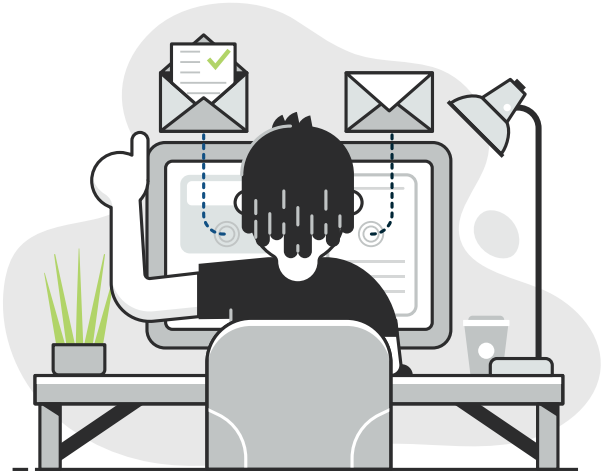
3. Phishing defense leveraging AI: An automated phishing defense platform that protects you from cybercriminals posing as trusted contacts.

Importance of backing up your data

Data loss can cause serious damage to any business. When disaster strikes, you last resort is your backed up data. By securely backing up your data, you can quickly restore and recover from any unforeseen disruptive events. Having a copy of your valuable assets is vital to ensure business continuity and protect your business against data loss or corruption due to cyberattacks or IT failure.

A data backup and recovery plan can help your organization prepare for unpredictable events. It enhances an organization's ability to continue business operations with little or no disruption and minimizes the risk in the event of a natural or man-made disaster.

Organizations without a backup and recovery plan cannot survive or recover from a major data loss event. In fact, the effects of a large-scale data loss incident can shut down operations permanently. Having a reliable data backup and recovery solution in your tech stack can help your organization reduce overall risk, quickly get back up and running after an outage or disruption, mitigate the risk of data loss and protect against reputational damage.



Why back up SaaS data?

Businesses are rapidly adopting cloud platforms to improve efficiency and agility, and the global pandemic has only accelerated this move. It's no surprise that almost 70% of organizations currently using cloud services plan to increase their cloud spending.

Since the beginning of the COVID-19 pandemic, companies have been adopting SaaS platforms, such as Microsoft 365, Google Workspace and Salesforce, at an astounding pace. The 2020 State of SaaSOps report reveals that businesses today use an average of 80 IT-sanctioned apps, and 70% of the business apps they use are SaaS-based. As of 2021, around 50% of all corporate data is stored in the cloud. As reliance on SaaS applications continues to grow, they will hold even greater volumes of sensitive business and customer information.

A backup and recovery solution is key to ensuring the safety of your sensitive data. Every day organizations are at risk of losing data from a variety of incidents — malware attacks, programmatic errors, malicious insiders, and most commonly, simple human error — just to name a few. Even though SaaS application vendors provide you protection from error on their end, it is ultimately your responsibility to safeguard your data against yourself and your end users.

Why is it important to think about data recovery?

The ability to quickly recover from a catastrophic incident can minimize the negative effects of downtime and data loss on your business. Here are the top three reasons why a data recovery strategy is now more important than ever:

1. Rising risk

- More than 90% of cyberattacks enter an organization via email. Email is a core business tool for modern organizations and also the weapon of choice for cybercriminals to launch sophisticated attacks.
- According to the FBI, there has been a 400% increase year-over-year in phishing attacks.
- An estimated 60% of businesses impacted by a phishing attack lose unrecoverable data.
- About 60% of employees fail a spear phishing email attack.

2. Rising costs

- The IBM Cost of a Data Breach Report 2021 revealed the average total cost of a data breach increased to an astounding $4.24 million in 2021.
- There has been a 243% year-over-year increase in ransomware remediation costs.

3. Rising probability

- More than 75% of companies that use SaaS applications suffered a data loss incident over a 12-month period.

7 KEY STEPS TO QUICK DATA RECOVERY

1. Know your RTO and RPO

- Ensure your recovery plan includes what your expectations are for Recovery Time Objective (RTO) and Recovery Point Objective (RPO).
- RTO and RPO are two important metrics that help quantify the potential losses following a disaster. They help to take the guesswork out of business continuity planning and enable you to prepare better for unforeseen disruptive events.

2. Document your plan

- Knowing what to do when an incident occurs allows IT to act rather than react. Using a solution like IT Glue can help ensure you have a list of things to do when a data loss incident does occur.

3. Audit the scope of the impact

- Have a process in place to ascertain what data was lost.
- Survey your users to understand all aspects of data loss.

4. Have a backup solution

- That provides end-to-end data protection and makes recovery quick and effortless.
- That empowers administrators as well as users to restore data and get back to work in just a few clicks.

5. Stay on top of communication

- Ensure there is consistent and clear communication to impacted internal stakeholders and list out action items for them if needed, so they understand what to do.
- If the data loss incident is a result of malicious acts like ransomware, communicate it to the FBI or your nation's appropriate authorities.

6. Regularly check your backups

- Provided you are backing up data, ensure that someone is actually verifying that all the data is being backed up.

7. Ensure that roles and responsibilities are clearly defined

- Who will restore the data?
- Backup solutions like Spanning allow for self-restore. However, each organization should define the scope of restoration in terms of end user responsibility versus IT.
- Recovering lost data can be cumbersome, time-consuming and require specific expertise. However, with a comprehensive solution like Spanning, even your end users can find and restore data in just a few clicks.

SPANNING
A Kaseya COMPANY

CHECK OUT SPANNING

Equip your business with a SaaS backup solution, which takes just minutes to install, manage and use.

Protect your business from common causes of data loss with Spanning Backup

Spanning Backup provides end-to-end data protection solutions for Microsoft 365, Google Workspace and Salesforce, with advanced capabilities to help prevent, anticipate and mitigate risks associated with cyberthreats and data loss. Its powerful yet easy-to-use capabilities empower administrators and employees to quickly find and restore lost data in matter of minutes. The end user self-service functionality reduces the IT burden and enhances productivity.

With Spanning Backup, your business can maintain sustained business operations and stay afloat even during times of crisis.