Acronis

WHITE PAPER

Comprehensive guide to data recovery

Table of contents

Executive summary

This white paper provides a thorough overview of the key components and best practices for data recovery, including data backup strategies and data recovery software solutions. It highlights regular backup as a method to avoid data loss and outlines various data recovery techniques, noting their advantages and disadvantages. This whitepaper will help ITOps professionals and organizations of all sizes gain valuable insights into the appropriate recovery strategy to implement in case of data loss.

Introduction

Data loss can be catastrophic in today's digital age, where data is integral to businesses and individuals. Several scenarios can result in data loss — physical failure of the storage media, accidental deletion, virus infection, or even software corruption. Data loss is costly both financially and in terms of reputation. According to a survey by Verizon, small businesses are extremely vulnerable to cyberattacks and many do not survive even one incident. Irrecoverable loss of sensitive and confidential data can also result in devastating regulatory implications, damaging the company's public confidence and incurring potentially massive fines.

Data recovery aims to ensure that lost data is retrievable. It requires deep technical expertise and state-of-the-art tools. Therefore, organizations must hire adhoc data recovery experts who deeply understand its intricacies. This white paper will be helpful for in-house IT professionals and provide organizations with an overview of the entire process.

What is data recovery?

Recovering lost data is possible. The process entails retrieving any lost or corrupted data that lived on hard drives, flash drives and memory cards. Any data not written on such storage devices cannot be recovered from them. Therefore, data recovery entails not just data retrieval, but also effective backup to minimize the possibilities of data loss.

Why is data recovery essential?

When data loss occurs, data is destroyed or deleted. The effects of data loss can thus range from inconvenience to a complete shutdown of operations. The fines, legal sanctions, loss of customer trust and other consequences of permanent data loss can be challenging to recover from.

Data recovery helps businesses return to normal operations as quickly as possible after a disaster. Without it, businesses may need to spend significant amounts of time and money recreating lost data. In some cases, businesses may even lose revenue due to the inability to access important information. Data recovery, therefore, saves organizations from these ditches by enabling them to restore critical data to its previous state.

Types of data loss

Data loss can be logical or physical, both of which we discuss below.

Logical data loss

Logical data loss is software based. It occurs due to software errors, viruses, malware, system crashes and power outages. Logical data loss results in decreased productivity, downtime and financial loss; organizations can also lose important customer information or financial records.

Physical data loss

Physical data loss occurs due to natural disasters, theft, hardware failures and accidents. It results from damage to physical media such as hard disks, USB drives and other storage devices. Physical data loss often results in irrecoverable and permanent data loss.

Common causes of data loss

Evaluating the cause of the data loss is critical to effective data recovery. The following are the most common reasons behind organizations suffering data loss.

Human error

Human error can be accidental or intentional. It manifests as accidental deletion, drive or file system misformatting, incorrectly changing a system's settings, or accidentally sharing confidential information. Intentional human errors, such as malicious or insider threats, also abound. Adequate training and information security policies are the most efficient methods to prevent data loss from human error.

Hardware failure

This occurs due to mechanical or electrical damage to the storage device, logical failures like corruption in the file system, or firmware or software issues. It can also be due to the read / write head crashing, which renders hard drives, flash drives and other hardware storage devices inaccessible.

Natural disasters

Natural disasters such as floods, fires, tornadoes, earthquakes and hurricanes can cause significant damage to physical storage devices and result in data loss. Natural disasters can also cause extended power outages, which may result in the loss of unsaved data. While it is impossible to prevent natural disasters, ensuring that data is regularly backed up and stored in multiple remote locations can be helpful.

Malware and viruses

Malware and viruses are malicious software programs that infect devices to steal data or render it unusable. They can be spread via email attachments, infected websites, or removable media; they can also be disguised as legitimate software. Malware and viruses result in system downtime, stolen credentials and financial fraud.

Ransomware is a type of malware that encrypts data and holds it hostage until a ransom is paid. Other types of malware, such as keyloggers or spyware, can also track keystrokes or access confidential information, leading to data loss.

An up-to-date antivirus software program and regular data backup are useful techniques to prevent data loss due to malware and viruses.

Software corruption

This occurs when there are bugs in your software or operating system (OS). Corrupted software causes

system crashes. Although software corruption is not preventable, a reliable backup solution can help restore important data in any case.

Routine system maintenance and regularly updating software can also lower the risks of software corruption.

How does data recovery work?

Data recovery relies on numerous factors. These include the cause of the data loss, the severity of the damage, the type of storage device and the choice of tools and techniques. The first step in data recovery is to determine the cause of data loss, which could be any of those mentioned earlier, such as hardware malfunction, software issues, viruses, accidental deletion or physical damage to the storage device.

Once the cause has been identified, the recovery process can be customized accordingly.

The next step involves scanning the storage device, identifying the lost data, reconstructing the file system and repairing damaged files. In this step, you need to implement specialized recovery tools. These scan the drive sector by sector for lost data, then search for data that matches the user's criteria.

Data recovery also involves assessing the extent of the damage to the storage device. The damage could be minor — a few bad sectors or damaged file allocation tables. In such cases, the recovery process is usually successful, and the data can be fully restored. However, if the damage is substantial and major, such as a physical head crash on a hard drive, it may not be possible to recover all the data.

Data recovery techniques

Data recovery techniques refer to the different methods and processes used to retrieve lost, deleted, corrupted or inaccessible data from storage devices (hard drives, solid-state drives, flash drives, memory cards). Some common data recovery techniques include the following.

Hard drive data recovery

This technique recovers data via the repair or replacement of damaged components. For example, a hard drive with a damaged read / write head may need to be replaced to access the data stored on the drive. A main advantage of this method is that it is a relatively cost-effective way to recover data compared to other techniques, such as on-site recovery.

Although it is also relatively easier to execute, there is a risk of causing further damage to the hard drive. This is because the recovery process involves physically accessing the drive, which can lead to additional problems if not done correctly. Also, some data may be lost forever if portions of the data have been overwritten or if the damage to the hard drive is too severe.

RAID data recovery

RAID (redundant array of independent disks) is a specialized process that involves restoring data from damaged or corrupted RAID systems. This technique allows for the recovery of data even if one or more disks have failed. This is because RAID systems are designed to store data across multiple disks for redundancy, which means the data can be reconstructed even if one or more disks are damaged.

However, this data recovery technique can be more complex and costly than other methods. RAID systems are typically used in high-volume storage environments, which

means there may be a lot of data to recover. Additionally, not all data may be retrievable — especially if the damage to the RAID system is severe. RAID data recovery should therefore be done by experienced professionals with a strong understanding of how RAID systems work.

SSD data recovery

SSD (solid-state drive) data recovery is a technique used for recovering data from damaged or corrupted SSDs. One of the main advantages here is that SSDs are generally more reliable and durable than hard drives, which makes them less likely to experience failures.

Additionally, even if the SSD has suffered physical damage, there is a chance that most or all of the data can still be retrieved. SSD data recovery can be more difficult due to the complex architecture of SSDs and will require specialized tools and tactics.

Flash drive data recovery

Flash drive data recovery entails retrieving data from a failed or corrupt USB flash drive. It is a quick and cost-effective process. Flash drives are widely used for storing data, so there is a high demand for this type of data recovery. However, there may be limitations on what can be recovered — particularly if the flash drive has suffered physical damage. If the damage is severe or the computer does not recognize the flash drive, the data may not be recoverable.

Cloud-based data recovery

This technique involves retrieving data from a remote server, like a backup service such as Google Drive or iCloud. Data can be recovered remotely by connecting to the affected device over the internet. This is especially useful when recovering data from physically inaccessible devices, such as those damaged by a natural disaster.

Cloud-based data recovery is a quick and easy way to access and restore data from a backup. There is also no risk of causing further damage to a physical device, as the data is stored remotely. It can, however, be slower than recovering data from a local device. There may also be limitations on what can be recovered — particularly if the backed-up data is incomplete or contains errors.

On-site data recovery

This technique requires physically accessing the device containing the lost data to retrieve it. It is often used for more complex data recovery scenarios, such as those involving RAID arrays or other complex storage configurations.

If performed correctly, on-site recovery allows for greater control over the recovery process, and data can be retrieved more quickly. It is, however, more expensive than other data recovery methods. There is also the risk of causing further damage to the device — particularly when the device's interior needs to be disassembled.

Software-based data recovery

This entails using specialized software tools and utilities to fetch lost or deleted data by scanning the storage device and delivering data in a usable form. The data is then copied for saving. These tools are designed to search for and recover files that have been accidentally deleted, corrupted or lost due to hardware or software failure.

Software-based data recovery is less expensive than other recovery techniques and can be done quickly without physical access to the device. However, if the recovery process isn't done correctly using the right software for the device, there's a chance the recovery can be unsuccessful. Also, if the data is encrypted, password protected or compressed, software-based data recovery may not be possible.

Data recovery software: A beginner's guide

Although most data recovery solutions use either metadata analysis or the raw recovery method, some combine both. In the raw recovery method, specialized software is used to retrieve data that are intact on the storage device and have not been overwritten.

Metadata is simply information about data. Recovery solutions use metadata to identify where storage devices house data files and record their properties and hierarchy in the directory. The recovery solution then processes and uses this metadata to restore damaged files per each sector of the storage device.

Metadata analysis eases the recovery of files using preset information like names, folders, and date and time stamps. Depending on the file system's directory hierarchy, you could even use metadata analysis to rebuild the entire system. To prevent the loss of crucial metadata, refrain from using file system repair tools, as they may modify the metadata.

When metadata analysis does not provide the desired result, the data is scanned by their names to discover the file signature. A file signature or pattern can be used to check the file that the data belongs to. Using the identified signature, recovered files are tagged and reassigned to new folders.

Data recovery best practices

There are a few key best practices you should follow for effective and swift data recovery.

Regular backups

Automate a backup schedule for important files. A regular backup schedule is the first step to successful data recovery, as it provides a reliable way of restoring lost data with minimal effort.

Test backups regularly

Check backups regularly to ensure that you can easily restore data. This involves attempting to restore data from the backup copies. If that is successful, you know the backup function is working properly. Backup tests should be performed at regular intervals — quarterly or biannually.

Create a disaster recovery plan

A disaster recovery plan is a repository of procedures to be followed in the event of data loss. It contains crucial details for recovery. Ensure that all employees are aware of their responsibilities as dictated by the plan.

Stop using affected devices

Using the device or media holding lost or corrupted data can result in data being overwritten, thus impeding your ability to recover it. You should, however, keep track of error messages and unusual behavior from your storage device.

Use a data recovery solution

When choosing a professional data recovery provider, it's important to select a company that specializes in the type of data loss you have experienced or are working on. It's also essential to consider the company's reputation, personnel experience and customer-service orientation.

Preparing for data recovery — A checklist

Make sure to tick these nine boxes to properly prepare for data recovery:

- Identify critical data and prioritize recovery efforts.
- Stop the use of the affected device or media.
- Get a list of the lost files to understand the extent of the data loss.
- Make a backup of any remaining data on the affected storage device.
- Document the cause and circumstances of the data loss.
- Note any error messages or unusual behavior on the affected device.
- Gather any necessary hardware or software tools for the recovery process.
- Protect the affected storage device from further damage or data loss.
- Choose a reputable data recovery provider.

Step-by-step process for data recovery

Four steps are involved in data recovery: evaluation, recovery, verification and delivery. Below is an overview of each.

Evaluation

A detailed record of what happened to your organization's or client's system serves as the north star to discovering the cause of the data loss and just how extensive it was. Things to consider including in your report are:

This is in no way an exhaustive list. Do not leave any information out. The smallest detail may be key to achieving effective data recovery.

Recovery

Having discovered the cause of data loss through evaluation, the next step is to recover the data. If your organization has an existing backup system, you can easily retrieve data from the backup storage. If not, you might need a specialized software or hardware tool.

Before proceeding with a recovery, stop using the affected device to prevent further data loss or damage. Next, choose the appropriate data recovery technique based on the storage device type and the cause of the data loss.

Take necessary precautions to protect the storage device and data during recovery. Use specialized data recovery software or tools to scan and retrieve lost or damaged data. And finally, restore any recovered data to a safe storage location.

Verification

After data recovery, the process of assessing how complete and accurate the data is must begin. You will need to perform a series of tests to confirm the file types, names and content of the recovered data. You will also have to verify the integrity of the recovered data to ensure it has not been corrupted or damaged during the recovery process.

You will also need to monitor the device for some time to find out if there are any further issues.

Delivery

Sending any recovered data to the client or your own organization involves transferring the data to a new and safe device or media in a usable format. You will need to work with the client or your organization's staff to ensure they have access to the recovered data and are satisfied with the outcome of the data recovery process.

Selecting a data recovery tool: A guide

Choosing the right data recovery solution will ensure a more complete and effective recovery. There are four aspects to consider when shopping for the best tool for your organization.

Compatibility with your system

If you are using Windows, choose a Windows-compliant data recovery software. The same applies if you are using a Mac or Linux system. Verify compatibility by checking the system requirements on the provider's website.

Compatibility also extends to the type of media you are retrieving data from. For example, if you are recovering data from a hard drive, you must choose software compatible with your type of hard drive. Some software may only work with certain brands or types of drives. Other factors to consider include the file system on the media you are recovering data from and any encryption that may be in place.

Ease of Use

Recovering data can be a complex process. You will want software that is easy to use and doesn't require a lot of technical knowledge to operate. Prioritize data recovery tools with simple, user-friendly interfaces. Some software uses a wizard-based approach, which is helpful for nontechnical users.

Another factor to consider is the software's scanning capabilities. A quick scan will be faster but less thorough, while a deep scan will scan the entire media for recoverable data. Choose software that offers both so you can choose the scan that suits your needs on a case-by-case basis.

Cost

The pricing of data recovery software ranges from free to several hundred dollars. While free software may be tempting, it is usually limited in features and recovery capabilities. Paid software, on the other hard, is usually more comprehensive and offers better results.

Check with your budget department as well as your IT team. Also, look for software that offers a trial period or a demo version so that you can test the software before purchasing.

Customer support

You may run into issues during the recovery process, and you will want to be able to reach out for help. Look for software that offers support through email, phone or live chat. Some data recovery tools even offer remote assistance.

Additionally, choose software that offers documentation and tutorials to help you better understand the recovery process and how to use the software. This can save you time, prevent frustration and allow you to retrieve your data more effectively. Consider reading reviews from other users to get a sense of the level of customer support offered by the provider.

Conclusion

Although a major setback for businesses and enterprises, data loss does not have to be permanent. Data recovery helps businesses continue operating without significant losses.

Acronis Cyber Protect is a reliable data recovery solution designed to meet the data recovery needs of all organizations, irrespective of the cause of data loss. It offers AI-based anti-malware protection, backup scheduling and seamless cyber protection. Try it today!

About Acronis

Acronis unifies data protection and cybersecurity to deliver integrated, automated cyber protection that solves the safety, accessibility, privacy, authenticity, and security (SAPAS) challenges of the modern digital world. With flexible deployment models that fit the demands of service providers and IT professionals, Acronis provides superior cyber protection for data, applications, and systems with innovative next-generation antivirus, backup, disaster recovery, and endpoint protection management solutions powered by AI.
Founded in Singapore and headquartered in Switzerland, Acronis now has over 2,000 employees and offices in 34 locations worldwide. Learn more at acronis.com.