

CYBER RISKS & LIABILITIES

The Importance of Data Backup and Recovery Plans for Businesses

In modern businesses, data is central to operations, customer management and decision-making. It is so integral to organizations that data loss from events like cyberattacks, hardware failures, failed cloud synchronizations, natural disasters and human errors can lead to significant disruptions, financial losses and compliance issues. Data loss events can also erode client trust and even precipitate business failure.

Organizations of all sizes are vulnerable to these risks, but having data backup and recovery plans can mitigate their exposures. This article explains what data backup and data recovery plans are, examines their benefits and provides tips for implementing them.

What Is a Data Backup Plan?

A data backup plan consists of policies and procedures that detail how to create copies of data and store them in a secure, separate location. There are different types of data backup methods, including:

- **Full backup**—This is when all data is copied. This method generally requires the most storage space but allows for a simpler, more efficient recovery.
- **Incremental backup**—This method involves copying only the data that has changed since the last backup of any type (e.g., full or incremental). This type of backup saves time and space but may create a more complicated recovery.
- **Differential backup**—This entails copying all changes since the last full backup, not just the most recent backup of any type. This is a middle-ground between full and incremental backup regarding time, storage space and recovery complexity.

When devising a data backup plan, there are also different storage options to consider:

- **Local backups** have data stored on-site with physical devices, such as external hard drives, flash drives and physical tape.
- **Off-site backups** have data stored in locations separate from the original data. This could be accomplished by saving the data on a cloud, having it hosted by a third party, or transporting the physical devices with the backup data to an off-site, secure location.

Many businesses are also adopting hybrid models that combine on-site storage for quick access with cloud storage for redundancy and disaster recovery.

What Is a Data Recovery Plan?

A data recovery plan details the process of restoring lost or damaged data from backup files after a data loss incident. After recovery, a system or database should be returned to its original state. For example, a business could reload files from cloud storage to restore its systems after a hardware failure, allowing it to resume normal operations.

Benefits of Data Backup and Recovery Plans

Having data backup and recovery plans can provide numerous benefits, including:

- **Minimal downtime and disruption**—These plans get operations back online faster by enabling quick restoration of data and systems after a disruption. They also help reduce financial losses by reducing the time a business's services are interrupted.
- **Protection against cyberthreats**—Data backup and recovery plans are crucial against ransomware and other cyberattacks. For example, in a ransomware attack, threat actors may deny a business access to its data until a ransom is paid. However, the



CYBER RISKS & LIABILITIES_

cybercriminals lose their leverage if the organization has backed up its data.

- **Enhanced compliance**—Many businesses are subject to regulations (e.g., General Data Protection Regulation, Health Insurance Portability and Accountability Act, Payment Card Industry Data Security Standard) requiring them to maintain secure data backups. Backup and recovery plans ensure businesses meet legal and regulatory obligations, preventing fines and penalties.
- **Preserved customer trust and reputation**—Data breaches and data loss events can cause prolonged service interruptions and damage customers' trust in an organization. Robust backup and recovery plans assist businesses in restoring services quickly, limiting reputational damage.
- **Cost savings**—The expenses of having data backup and recovery plans are usually significantly lower than recovering from a cybercrime, such as a data breach, which can lead to legal fees, fines and lost revenue due to business downtime.

Tips for Effective Data Backup and Recovery Plans

Businesses can implement several practices to ensure data backup and recovery plans are effective. The following are strategies they should consider:

- **Identify data to backup.** Businesses should determine the data that is necessary to back up by analyzing which data is critical to their operations or is needed to meet regulatory requirements. They should also determine how frequently backups should occur.
- **Follow the 3-2-1-1-0 backup rule.** The method guides effective storage parameters, building on the classic 3-2-1 rule: *Three* copies of the data (in addition to the original) are stored on *two* different types of storage media (e.g., cloud and external hard drive), with *one* copy stored off-site. Additionally, in the 3-2-1-1-0 rule, *one* of the backups should be offline to protect against cyber risks like ransomware. Finally, the "0" refers to ensuring *zero* errors through regular verification of backup integrity.

- **Encrypt data and implement access controls.** Backup data should be encrypted, and access to it should be limited. These actions add layers of protection against data breaches by cybercriminals.
- **Conduct regular testing.** Businesses should conduct periodic recovery drills to ensure their procedures are functional. They should also routinely validate the integrity and usability of backed-up data.
- **Automate and monitor processes.** Organizations should leverage technology to implement automated backup processes and reduce human error. They should also engage in continuous monitoring of these processes so they can quickly remedy any issues that arise.
- **Educate and communicate.** All staff should be regularly educated on the importance of data backup and recovery plans. Changes and updates to policies and procedures should also be effectively communicated.

Conclusion

Data backup and recovery plans are vital to businesses of all sizes, as they can reduce expenses and facilitate a swift recovery after a data loss event. Effective plans can also mitigate cyber risks, preserve customer trust and protect an organization's reputation. To maximize these benefits, businesses should continually evaluate their current systems and explore consulting services to enhance their backup and recovery procedures.

Contact us today for more information.
