

WHITEPAPER

How a Solid Data Disaster Backup and Recovery Plan Can Save Your Business

https://ntwo.com/

Thanks to the widespread use of information technology in business, data has become a critical asset. For this reason, business data needs to be protected, and ensuring data availabilityty and integrity is a big part of realizing data security.

Backing up data is the process of duplicating business data and storing copies in secure locations. In the case of a data disaster or loss, the backed-up copies can be used to restore the original data, securing business continuity.

“According to Shred-it Data Protection Report 2019, human error and insider threats are to blame for the majority of data loss and data breach cases.”

Common Causes of Data Loss

Businesses can lose data in many different ways – some of which are malicious, while others stem from user errors and carelessness. Below is a list of five of the most common causes of data loss and data corruption.

Human Error

According to Shred-it Data Protection Report 2019, human error and insider threats are to blame for the majority of data loss and data breach cases. Other recent studies and surveys have also supported the fact that humans are the weakest link in terms of
data security.

Data is highly sensitive, and even small mistakes when handling data can lead to catastrophic losses. Some of these careless mistakes include:

- Data entry errors
- Incorrect system configurations
- Accidental deletions
- Malicious or accidental damage of computer and IT hardware
- Poor cybersecurity practices

Natural Disasters

Although it may seem unlikely, natural disasters are among the primary causes of data loss. Adverse weather elements such as tornadoes, hurricanes, lightning storms, strong winds, earthquakes, and other natural disasters not only cause property and infrastructure damage but also pose a serious threat to digital assets.

Businesses that house their data in physical on-prem data facilities are often at risk of losing their data to natural disasters. Unfortunately, natural disasters are not preventable and may even be hard to predict. However, it helps to anticipate such cases by having a dependable data backup and recovery plan.

Hardware or Software Failure

Computing resources – both hardware and software resources – are not totally dependable. Like other machines and tools, they are prone to misfires. For instance, the average mechanical hard drive failure rate is between 1 and
2 percent, depending on the capacity, manufacturer, and usage level.

Other hardware components can also behave unpredictably, leading to data loss. Malfunctions in software such as ERPs and data management systems can also interfere with data integrity and availability.



Cyberattacks

Cybercrime is another leading cause of data loss in businesses all over the globe. Cyberattacks are now more prevalent and devastating than ever before. In fact, cybercrime as a whole hasincreased by a whopping 600% since the beginning of the Covid-19 global pandemic.

A cyberattack can wipe out an organization's entire data store in a single sweep. Attackers often ask for a ransom in order to restore the data (a promise that is not always fulfilled), and some sell it to bidders on the black market.

Theft and Accidents

Data loss can also be caused by the theft of physical IT hardware such as servers and workstations. Accidents like fires and water leaks can also permanently damage data storage hardware, obliterating all the bits of information that reside in such systems.

Risks of Data Loss

Unforeseen data loss in a business, regardless of the cause, can have severe consequences for the enterprise. This is the reason why companies spare no expense in working to prevent data loss. Here are three of the risks associated.

Monetary Losses

Data is a valuable business asset. In fact, most businesses rely on data to power their entire enterprise, and so the loss of data translates to monetary damages. Data loss halts IT operation, which is devastating for an IT-dependent business. The average cost of IT downtime at an astonishing $5,600 per minute. The total cost of downtime includes losses due to low productivity, any applicable fees, and the cost of restoring normal business operations.

“The average cost of IT downtime at an astonishing $5,600 per minute.”

Loss of Business

Besides monetary losses, businesses also tarnish their brand reputation and credibility after losing valuable customer data. The bad publicity and damaged reputation cause businesses to lose customers’ trust and, eventually, their trade altogether. The majority of businesses that suffer data losses never recover from the impact, and end up shutting up shop for good within a year.

Legal Implications

Legal compliance is a great motivator for observing data security and availability. Some international, federal, and state data laws require businesses to maintain consistent availability of data, which in most cases means having a dependable data backup and disaster recovery plan. Failure to comply with data guidelines results in heavy fines and penalties.

How to Implement a Backup and Disaster Recovery (BDR) Plan

Data disasters can happen when you least expect them, and they leave severe business devastation in their wake. A backup and recovery plan should be the backbone of your data security strategy to guarantee instant data availability in case of a disaster. Here’s what you need to know about formulating a BDR plan.

Start With a Reliable Backup and Restoration System

The first step to creating a BDR plan is deciding how to securely store important data in a recoverable fashion. Ideally, you should store your backup data in a few different media and locations, and use backup systems that don't suffer from common data loss risks. Secure backup options available to businesses include:

- Cloud storage
- VM backups
- On-site backup
- Hard storage

Involve Your Employees in the BDR Plan

We saw earlier that employees can be responsible for data loss. This is why, when creating a BDR plan, it's crucial to have these employees on board. Train your staff in the importance of data security, practices that help prevent data loss, and their roles and responsibilities in ensuring data availability. It's also important to prepare your employees for the possibility of data disasters, so they learn how to handle a data crisis without worsening the situation.



Define Protocols to Deal With the Aftermath

After a data loss incident and a successful recovery, you should carefully review the case to identify the fault and gather useful information to prevent such an event from recurring. Put in place a set of protocols to figure out exactly what caused the data loss, how it happened, and to rule out the danger of such a breach happening again.

Make Sure You Have a Plan

Every business needs a robust BDR plan as part of its broader IT security strategy. Entrepreneurs and business owners often ignore the importance of a BDR system until it becomes necessary. There are so many ways in which a business can lose its valuable data, and on top of that, the implications are severe.

With all this in mind, it's time to secure your business' future, even in the event of severe data loss, which is sometimes unavoidable. Get in touch with us to learn how we can assist your business in coming up with a solid BDR plan.

Contact Us

https://ntwo.com/
337-474-4249 | 409-724-0440
2950 Country Club
Lake Charles, LA 70605