BUSINESS UPTIME & DATA-LOSS THREATS

TOP 4 THREATS TO BUSINESS UPTIME & DATA RECOVERABILITY

ISOCNET

Overview

Running a business involves dealing with unforeseen setbacks and interruptions that may lead to downtime and productivity dips. Implementing a strategy to manage such setbacks and ensure business operations run smoothly with minimal disruption is referred to as business continuity.

Events like a pandemic, natural disaster, power outage, hardware failure or employee negligence, can disrupt operations. Business continuity involves advanced planning and preparation that focuses on ensuring that an organization is able to operate critical business processes even in the wake of a data-loss incident.

Two key components that work cohesively as part of an organization's business continuity plan are:

- Backup
- Disaster recovery

After an incident, your organization should get back up and running as well as recover critical data as soon as possible to prevent unnecessary productivity and revenue losses.

Defining Terms

Backup

is the process of creating secondary copies of business-critical data that can be used to restore the original file in the event of data loss. It's important to note that while backup can't prevent a data-loss event, it can help an organization restore lost data after a data corruption or deletion event.

Disaster recovery

on the other hand, may be described as a set of policies, tools and procedures focused on protecting an organization from the adverse impacts of disasters like data corruption events or accidental deletions. The major aim of a disaster-recovery plan is to ensure the smooth running of critical functions during and after an emergency event in order to minimize business disruption.

A comprehensive backup solution is the foundation ***of all business continuity and disaster recovery (BCDR)*** plans. BCDR combines a set of approaches or processes that help an organization recover from a disaster so it can resume its routine business operations as soon as possible.

Deploying an effective ***backup and disaster recovery (BDR)*** solution is imperative to ensure minimal loss of data and productivity even after severe disasters and business disruptions.
A comprehensive BDR solution not only helps restore any lost data but also ensures that a business can quickly get back on its feet after a setback.

With more businesses embracing long-term remote or hybrid work models that require their employees to work remotely for some or all of the time, having the right BDR solution and business continuity plan is becoming increasingly essential.

We'll discuss more on that later. For now, let's examine why many businesses fail to realize the importance of BDR.

Chapter 1
Why Organizations Overlook BDR

Cybercriminals are having a field day with security gaps arising from distributed work environments. With remote workforces becoming the norm, businesses are now exposed to greater risk of data loss than ever before. This may be attributed to the fact that remote workers do not follow security protocols as closely as they should (62%) and home networks are less secure than office networks.[1]

Unfortunately, there are several businesses out there that still do not believe in investing in BDR. In fact, 51% of organizations across the globe do not have a business continuity plan in place to deal with unforeseen contingencies.[2]

Misinformation might be a key reason why businesses often overlook BDR and fail to understand that they need to back up their cloud data as well. When it comes to ***software as a services (SaaS)*** applications, most organizations believe that their SaaS provider has them covered for backup and recovery. However, there are significant limitations with regards to what is provided.

SaaS providers practice a “shared responsibility” model when it comes to data protection. While SaaS vendors protect their customers from network, storage, server and application failure, vendors are not responsible for protecting data from user and admin failures as well as against cybersecurity attacks originating at the user level.

> 51% of organizations across the globe do not have a business continuity plan in place to deal with unforeseen contingencies.

Chapter 2

Top 4 Threats to Business Uptime & Data Protection

The Many Faces of a Security Incident

While backup and security are two separate issues, data could certainly need to be restored in the event of a data-loss incident. A backup solution can make that happen.

With that caveat addressed, there are several ways a security incident can occur and cause operational disruptions/downtime and partial or total data loss. Such incidents can be costly for both small and large organizations. Some of the most common security incidents that most businesses are exposed to include:

- Cyberattacks
- Insider threats
- Human error/negligence
- Natural calamity
- Power outage
- Hardware failure

Do you know what the most cited causes of IT downtime within the last 12 months were? Hardware failure was right at the top at 20%, closely followed by connectivity issues at 16.75% and cyberattacks at 12.75%. Cloud outages contributed to 7.25% of downtime while another 5.75% of downtime was caused due to extreme weather conditions such as flooding.[3]

Work From Home

Post pandemic, most organizations plan on implementing hybrid work policies whereby a part of or all of their workforce will continue to work remotely. It is estimated that by 2025, roughly 70% of the workforce will still be working remotely, a minimum of 5 days per month.[4] These decentralized work environments will significantly increase the attack surface and expose their critical data and systems to security vulnerabilities and cyberthreats.

Confusing Regulations

The last few years have triggered a tsunami of data security and protection regulations that are not only complicated to understand but have a tendency to change or grow frequently, making it difficult for businesses to keep up with them.

Security/Protection Misunderstandings

Most businesses have misconceptions about the security and protection of their SaaS application data, such as that housed in Microsoft 365® or Google Workspace. They do not understand the "shared responsibility" model that vendors follow. As such, when inevitable data-loss incidents occur, they are left feeling frustrated and filled with regret.

A recent report by VMWare reveals that destructive attacks — in which networks or data are destroyed — are up a whopping 102%.[5] As such, businesses can't afford to ignore the fact that the BDR risk landscape is expanding.

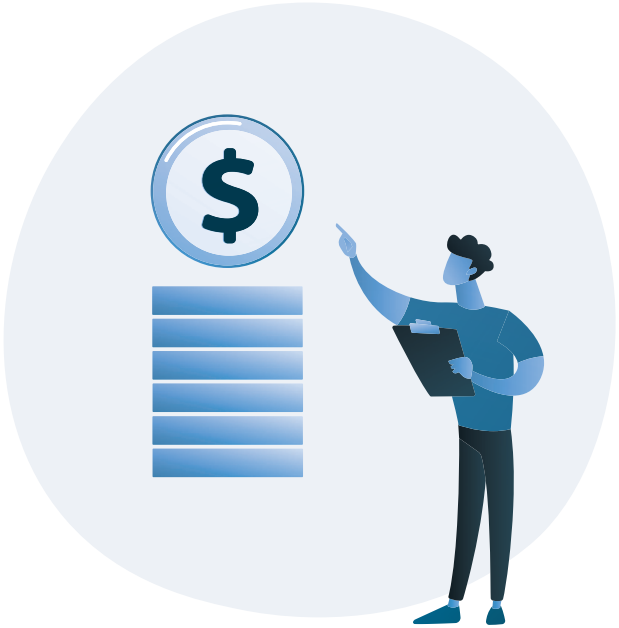
Chapter 3
The Cost of Ignoring BDR

Disaster-induced downtime or data loss not only disrupts your routine operations but also results in serious financial implications for your business. Something as inconsequential as an employee inadvertently clicking on an infected email, to an event as substantial as a global pandemic, can throw your entire business off course.

As per Ponemon, the average cost of a data breach stands at $3.86 million, with healthcare being the worst affected industry at $7.13 million. On average, a business takes a whopping 280 days to identify and contain a data breach. A shorter data breach lifecycle, however, will cost a company much less. The report highlights that a data breach with a lifecycle under 200 days will cost nearly $1 million less than one that takes more than 200 days to detect and contain.[6]

Pairing a comprehensive cybersecurity solution with a BDR solution will not only help you shorten the lifecycle of a potential data breach but also help your business get back on its feet quickly and save your organization millions in dealing with the aftermath of the disaster.

Deploy a robust backup and disaster recovery solution to quickly recover from data breaches and reduce the effective cost of each breach.



Chapter 4
Why a BDR Solution Is a Worthwhile Investment

Deploying a quality BDR solution is vital to ensure your business continues to run smoothly, even in the event of a security breach or data loss. While there are several ways you could lose your critical business data, backing it up with copies enables you to restore lost data from an earlier point in time, helping your business recover from setbacks faster.

On-premises backups help in creating copies of data and storing them in in-house storage devices such as network-attached storage, disk or tape backups and storage servers.

With most businesses embracing hybrid work models, their remote systems and off-network devices are now more exposed to potential cyberattacks and consequent data loss. That's why it is imperative to deploy a BDR solution that takes care of the data on your remote endpoints as well. It's important to note that while BDR alone does not prevent cyberattacks or accidental deletion, it can help you restore information after a data-loss incident occurs.

As per the 2020 Cloud Security Report, 69% of businesses believe that data loss/leakage is their top cloud security concern.[7] Organizations lose cloud data every day, even from Microsoft 365, Google Workspace and Salesforce. In fact, 77% of companies that use SaaS applications report suffering at least one data-loss incident within a 12-month period.

It goes without saying that securing your data in the cloud is indispensable to disaster-proofing your business. You need a BDR solution that helps back-up and restore your SaaS data and gets you back on your feet with just a few clicks.

BDR is an integral part of having an effective business continuity and organizational resilience plan in place.

Chapter 5
How to Build the Right BDR Solution

When looking for the right BDR solution for your business, you need to understand that there is no one-size-fits-all solution out there. Every business is unique and you need a solution that works the way you need it to. Here is a list of common features that you need to look for to ensure that you're investing in the right BDR solution:

- Instant recovery
- Automated testing to ensure that you're always disaster-ready
- Scalability to evolve with your company's growing needs
- SaaS backup without any costly overheads (hardware, installed software, network bandwidth)
- Automated backup in the background with the option of on-demand backups
- Quick data restoration to previous versions with 100% accuracy
- Proactive identification of recovery issues so you can spend your time on more profitable tasks

However, just having a BDR solution isn't enough. This solution must also fit into a comprehensive business continuity plan, and that plan needs to be regularly evaluated. Nearly 35% of businesses that report having a disaster recovery solution in place admit that they have not tested their recovery plan process in the last 12 months.[8] Testing your business continuity plan regularly is important to ensure that it still works.

> Testing your business continuity plan allows you to highlight potential problems and revise procedures to ensure that your business always runs smoothly.

Conclusion

Data backup and recovery isn't optional, especially when you're trying to compete with your peers, widen your customer base and improve profitability. That's why you need a managed cloud BDR solution that simplifies backup and disaster recovery. Knowing that your critical business data is in safe hands will not only give you peace of mind but also free you up to focus on growing your business.

To learn more about deploying
the right BDR solution for your business,
get in touch with us today!

CONTACT US: 859-525-8730

sales@Teamisoc.net

Sources

1. 2021 Data Exposure Report Insider Risk, Ponemon
2. Mercer Talent All Access Business Responses to the COVID-19 Outbreak Survey Findings
3. Data Health Check Survey 2020, Data Barracks https://datahealthcheck.databarracks.com/
4. This is the Future of Remote Work in 2021, Forbes
5. VMWare
6. Ponemon Institute's Cost of a Data Breach Report 2020
7. 2020 Cloud Security Report, ISC2
8. Data Health Check Survey 2020

859-525-8730 | sales@Teamisoc.net

Design - Development - Hosting - Online Marketing - O-365 - Data Center - Cloud - On-Site & Remote IT Management