precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

CYBER DIGITAL WORLD

NEWSLETTER

Volume: 18 February 2023

The importance of Data backup and recovery policy in organizations

Dr. Ronald Walcott
Managing Director

With data becoming more and more crucial to the operation of businesses, and the volume data increasing exponentially daily, organizations have to recognize how important it is for them to have secondary sources of their information ready to go in the event that the main store of data becomes unavailable or compromised.

Most organizations, their IT departments regularly backup data, systems, network configurations data, databases, and other information resources. However, the question is still up in air, does it have data backup and recovery policies in place?

WHAT CONSTITUTES A BACKUP AND RECOVERY POLICY?

A backup policy is a policy which defines the importance of data and systems backups, and the ground rules for planning, executing and validating backups to ensure that critical data to the business operations is backed up to a secure storage media which is located in a secure location. This ensures that information from business applications (MS SQL, Oracle) and user files is copied to disk and/or tape to ensure recoverability in the event of deletion, system disruption or corrupted files.

WHAT SHOULD AN ORGANIZATION BACKUP?

Organizations should aim to backup all information and data that is essential to the daily operations of the organization. Some of these are data files, databases, utility programs, VMs, cybersecurity software, network and network perimeter software. These are all essential to the everyday operations of organizations and should be backed up on a regular schedule(at least once every 6 months). Software is not the only thing that needs to be backed up. The software components listed previously are only operated through the use of hardware devices. Therefore, it is also extremely important to have back up devices to continue operating in the event that one of these devices go down or become compromised. Some of these devices are, servers, switches, routers, desktops, laptops, etc. There is one alternative to having these devices physically, by having these devices replicated in an alternative location, for example, on the cloud, to ensure their rapid recovery if the devices become physically inoperable.

Organizations employ a few different backup types. Some of these backup types are as follows:

- Incremental Backups – This type of backup only backs up data that has been changed since the last back up was done.
- Differential Backups – this back up, backs up all the data that was backed up since the last full backup.

Benefits of having best practice backup and recovery policies implemented.

- Incremental backups can be done and completed fairly quickly and doesn't consume a lot of space in comparison to a full back up or differential back up.

- Having good recovery policies makes the backup process easier, more efficient and also ensures the times restart of business functions in the event that recovery of data is needed.
- Protects against cyberattacks.
- Good policy and practice also ensures that the correct back up types and methods are used for the correct circumstance.
- It minimized downtime and saves the company money.

Drawbacks of having backups and recovery policies implemented.

- If only tapes are used to back up data, in a situation where recovery is required, the process becomes a lot more time consuming and complex. However, these can be mitigated using high-speed disks.
- Even if differential backups remove some of the recovery burdens that can occur when restoring from an incremental backup, if the application environment is often subject to daily data changes, the backup window could become elongated.
- Differentials will consume more backup resources, because each differential backup copy moves and stores all the changed data since the prior full backup.

WHAT SHOULD ORGANIZATIONS CONSIDER WHEN DEVELOPING A RELIABLE BACKUP/RECOVERY POLICY?

As we noted earlier, back up policies are important to ensure that there is a consistent and reliable method for recovering data. Good practice states that a company's IT department should take ownership of backing up all data. If this is not done, it is possible that essential and critical business data, needed for everyday business functions might be lost at some point and the IT department would be held responsible for the lack of measures in place to recover to a point of operability.

Here are a few things an organization should consider when developing backup/recovery policies:

- **Technologies used for backing up, recovering and restoring data**.

  Organizations need to evaluate what works best for their purposes and their budget and choose the right back up methods and tools that effectively works for them.
- The type of data and systems being backed up.
- Procedures for ensuring that critical data is securely stored in the event of compromise.

  Organizations must always have backups of information that is critical to the organization's function. This would allow the business to continue its functions even if they have been attacked or compromised and reduce their overall losses.

Upcoming Events

ISMG ENGAGE
March 7, 2023
Toronto

CYBERSECURITY SUMMIT: NORTH AMERICA-EAST
March 21, 2023
New York

ISMG ENGAGE
April 19th, 2023
Washington, DC

Frequently Asked Questions:

IS IT COSTLY TO BACK UP DATA?

It can be costly or affordable. It depends on the medium used to back up the data and obviously how much data needs to be backed up.

HOW DO YOU ENSURE THAT BACKUP/RECOVERY POLICY IS BEING FOLLOWED?

Having employees follow policies all the time can be difficult. However, it is important for policies to be in place and followed to ensure that the company is protected. We can ensure that policy is being followed by enforcing adherence by having penalties for non-compliance. These penalties can either be in the form of warnings or more stern action depending on the severity.

WHAT ARE SOME COMMON WAYS BUSINESSES LOSE THEIR DATA?

- System failure.
- Human Error.
- Cyberattacks.
- Natural Disasters

Headline News

DDOS Attacks Becoming more potent, shorter in duration.

US, India and East Asia Were Top Targets in 2022, Microsoft reporter says. Tech giant Microsoft says it observed distributed denial-of-services attacks become shorter in duration in 2022 while also becoming more potent and capable of larger impact. The U.S., India and East Asia topped the targeted regions for DDoS attacks, among others, and internet of things devices remained the preferred choice to launch these attacks, according to Microsoft's DDoS trends report for 2022.

DDoS attacks in 2022, on average, lasted for less than an hour, and attacks that lasted for 1 or 2 minutes made up for one-fourth of the total attacks last year.

The tech giant says the attacks were shorter because bad actors need fewer resources to carry them out and security teams are finding it harder to defend against them with legacy DDoS controls. "Attackers often use multiple short attacks over a span of multiple hours to make the most impact while using the fewest number of resources," Microsoft says.

An average of 1,435 DDoS attacks were observed daily, and the highest number was 2,215 attacks, recorded on Sept. 22. The volume of DDoS attacks during the holiday season increased considerably until the last week of December

Source: www.databreachtoday.com