LEVERAGING CLOUD & ON-PREMISE BACKUPS

TO LOWER COSTS AND IMPROVE EFFICIENCY

CONTENTS:

INTRODUCTION

Data and files have always been the backbones of businesses, for as long as businesses have existed. Once upon a time, our organisational data was physically held in filing cabinets or piled in boxes in a dingy room in the back of the office. Back then, company data was constantly in danger of going missing, being incorrectly filed, or was at the mercy of natural disasters.

We've come a long way from filing cabinets and physical documents. These days, most of our data is stored on servers, hard drives, or in the cloud. But with these technological advancements, our data is now under more threat than ever. Not only do we also experience data loss due to natural disasters and incorrect filing (how many times have you thought 'now where on earth did I save that document!?'), we must also defend against ransomware/malware attacks, accidental deletions/damage, server outages, and a whole host of other potential threats that are waiting to snatch away your data and remove it from existence, oftentimes with devastating results. Just take a look at some of these statistics from Infrascale and Varonis:

Business continuity and data loss statistics:

37% of SMBs have lost data in the cloud

30% of businesses lose data due to server outages

Roughly **1 out of 100** hard drives fail yearly

Ransomware is responsible for **27%** of malware incidents

28% of ransomware attacks resulted in data loss

60% of small businesses close within **6 months** of major cyber attacks

WHAT CAUSES DATA LOSS?

As mentioned, there are a number of ways your data can disappear from the ether, with the most common being:

HUMAN ERROR:

Humans make mistakes. Sometimes they're little mistakes that can easily be rectified and other times they're big ones (such as hard deleting folders or files). No matter the size of the mistake, human error can result in overwriting important files and deleting information that is essential to your business.

Human error can also result in other forms of data loss such as spillage, drops, or other accidents that could damage devices/servers.

EXTERNAL SECURITY THREATS:

Viruses, malware and ransomware are the biggest threats to your data. Malware can slow down your systems, and steal or corrupt your data. Worse still, ransomware does the same with the added threat of holding your data ransom until you pay a hefty fee.

OUTAGES:

Power outages can completely halt business operations by shutting your systems and devices down without warning. This not only results in the loss of unsaved data but can also corrupt files due to improper shutdown procedures.

THEFT:

Many businesses assign laptops to their employees and allow them to take their devices with them when they leave the office. This, of course, can result in the loss or theft of company property. If their unbacked-up files on lost or stolen devices, you can say goodbye to those files forever.

HOW TO PROTECT YOUR DATA

So how do we lessen the impact in the event of data loss? The biggest defence against human error and external threats is to BACK UP YOUR DATA. And I don't just mean save your files on a hard drive or a USB and tuck it away into a 'safe' place - that solution is simply not viable for organisations storing valuable data.

As a business owner, you absolutely need a diligent backup program with multiple backup and recovery points. This brings us to the 3-2-1 backup rule.

THE 3-2-1 BACKUP RULE

3 COPIES OF DATA

2 TYPES OF MEDIA STORAGE

1 OFFSITE COPY

WHAT'S THE 3-2-1 BACKUP RULE?

The 3-2-1 backup rule has met with some controversy in recent years, with some claiming it is outdated, while others insisting that it is still relevant and useful for today's landscape.

The truth of the matter is that although the 3-2-1 may be the bare minimum for organisational backup plans, it still sets a solid foundation for the prevention of data loss.

The rule goes like this:

3 COPIES OF YOUR DATA

2 BACKUPS ON DIFFERENT MEDIA (for example, on your computer, external hard drive, or on-premise server)

1 BACKUP OFFSITE (e.g. in the cloud, or in an offsite server or data centre)

Following the 3-2-1 backup rule, it is advised that businesses should have both an on-premise and cloud-based backup solution.

Let's delve into what these solutions are.

ON-PREMISE BACKUPS

Every business likely uses some form of on-premise (or on-site) backups. On-premise backups simply refer to the storing of data locally on various devices. These devices can include hard drives, disks, USBs, network attached storage (NAS), or servers.

SECURITY:

Businesses in highly regulated industries (such as healthcare or finance) prefer on-premise backups because the solution ensures no third party has access to critical data or information. Furthermore, onsite backups mean data is rarely sent out over the internet, and stays secure behind your firewall.

CONTROL:

In a similar vein, because your data is stored onsite you have complete control over your backups. You can choose when data is backed up, how often backups occur, and what/when information gets backed up. Also, you can scale up or down with hardware as your business develops and changes.

ACCESSIBILITY:

Having your data stored on-premise means you can quickly access files whether you are on-line or offline.

SCALABILITY/COSTS:

On-premise backup solutions are often scalable, but the costs depend on how much data you need to store. In most instances, there may be significant costs involved up-front – particularly if you need to purchase a NAS or server. However, self-managing your on-site backup system can be cost-efficient in the long run as you will not need to pay a monthly fee to a third party.

On the other hand, if you require a complex backup system, it can become costly to maintain and upgrade as you will need an inhouse IT technician or a Managed Service Provider (MSP) managing your servers.

RISKS:

Because your backup solution is physically stored in your office, the major risks involved are due to irreparable damage to the system (whether accidental or purposeful) and disasters (floods, fires, etc.).

CLOUD BACKUPS

Most businesses across the globe are now implementing cloud-based backup solutions to further protect their data. Cloud backups refers to the process of digitally storing a copy of data in an off-site location (in the cloud). Whether private or through a third party, cloud backups do offer many benefits that you cannot get with on-premise backups.

SECURITY:

The level of security depends on whether you're relying on a third party or a private cloud solution. Private cloud is maintained on a private network where the hardware/software is dedicated to a single organisation – it is a secure and high-performance solution available for businesses that need data stored within a secure environment. This solution would suit highly regulated organisations.

On the other hand, third-party vendors may not be suitable for businesses that house confidential data, as your critical data may be accessed by the vendor. However, for most businesses this isn't a problem. Good third-party vendors offer safe and reliable backup solutions that provide more than adequate security for your data.

In both instances, cloud backup solutions have the added benefit of being out of reach from natural disasters or damage that could occur to on-premise systems.

CONTROL:

Most cloud backup vendors offer businesses complete control over their data, with automated backups, multiple recovery points, and immutable storage.

ACCESSIBILITY:

Generally speaking, cloud backups are user-friendly and accessible from anywhere, at any time. However, in periods of outages (i.e. with your internet or backup provider) your data may become momentarily inaccessible, resulting in downtime.

SCALABILITY/COSTS:

Similar to security, the cost of cloud solutions depends on a number of things, like whether you require private or public cloud, but generally you are only charged for the space and bandwidth you require. The major benefit in this realm is the flexibility and ease with which you can scale your backups, and the lack of maintenance costs – there are generally no up-front costs (except perhaps in the case of private cloud), and maintenance of the cloud servers is the vendor's responsibility.

RISKS:

Like any solution, cloud backups aren't perfect. They are still at risk of data loss due to malware and ransomware infections, particularly if you have not set up recent and recurring disaster recovery points.

WHY NOT BOTH?

Why not both indeed! Leveraging both on-premise and cloud-based backups gives your business the best of both worlds; on-premise backups that are secure and easily accessible, plus the added security and peace of mind of having cloud backups to fall back on in the event of damage/disaster in your office.

Referring back to the 3-2-1 rule, leveraging both cloud and on-premise backups give you the ultimate security. While this may seem costly, utilising both forms of backups can save your business in the long run by improving efficiency, reducing downtime, and perhaps most importantly; saving your skin in the event of a malware or ransomware attack, which commonly costs businesses millions of dollars to rectify.

We wholeheartedly believe that preparing for data loss isn't paranoia; it's good business practice! As the saying goes, you're better safe than sorry, and when it comes to your data, safety should always be at the forefront of your mind.

OUR BACKUP SOLUTIONS:

CLOUD SOLUTIONS

✓ VEEAM

✓ BARRACUDA

✓ NEXTDC

✓ PRIVATE CLOUD

✓ HYBRID CLOUD

ON-PREMISE

✓ SYNOLOGY

✓ BARRACUDA

✓ VMware

✓ SERVER CONFIGURATION

✓ NAS CONFIGURATION