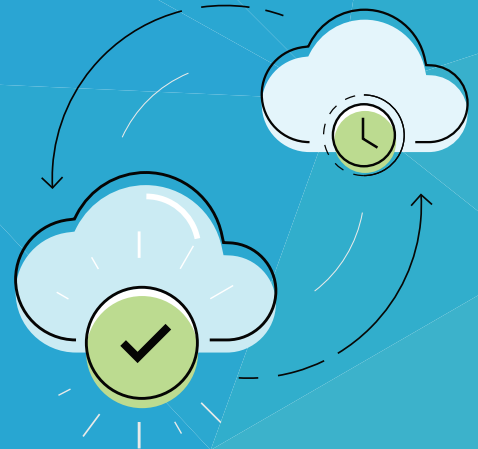datto

Backup Vs Business Continuity

Plan Better for Your Business

Data protection solutions are essential for businesses of all sizes to implement, regardless of size, industry and geographic location. In this white paper, we'll discuss the importance of business continuity rather than simply backup. We'll also explain how to quickly evaluate your internal recovery process and downtime costs to ensure you find the best solution for your needs.

Introduction

Downtime is real and it's costly. How costly exactly? Depending on the size of the organisation, the cost per hour of downtime is anywhere from £7,000-£700,000. The average UK business is down for 27 hours a year (the highest in Europe) which costs the UK economy over £2billion. The numbers speak for themselves.

What causes downtime? Network outages and human error account for 50% and 45% of downtime, respectively. Meanwhile, natural disasters account for just 10 percent of downtime. In the last few years, malware has also become increasingly common, and strains of Ransomware hold business data hostage until a Ransomware is paid.

When you look at the cause of downtime by data volume, the #1 culprit is, once again, human error, at 58%. As it turns out, businesses should be more wary of their own employees and less of natural disasters.

If you've been putting off data protection because your organisation is located far from a flood plain,, be warned: the bigger threat to your data is inside of your company, not the great outdoors.

What's at stake?

2.5 quintillion bytes of data are generated daily. And 90% of the total data in existence was created within the past few years, a significant portion of which has been generated by small businesses. Considering all the servers, desktops, and laptops that the typical SMBs manage, it adds up to a lot of data to protect.

Yet nearly 75% of SMBs operate without a disaster recovery plan and only 25% are "extremely confident" that they can restore data if it was compromised. Only 50% of SMBs back up less than 60% of their data. The remaining 40%? No protection for it whatsoever.
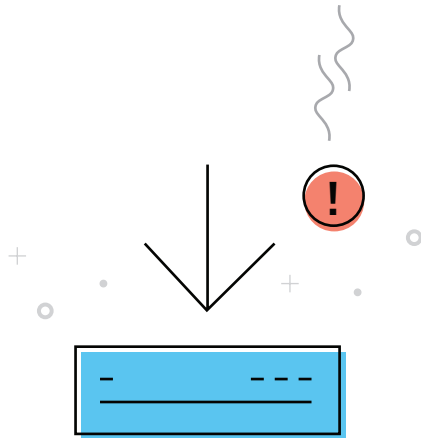
How much does this cost? Over the past few years, 35% of SMBs lost as much as £300K due to downtime. An unlucky 3% lost over £750k.

Ransomware alone cost British businesses over £4.5 million in 2016 - and as many as 25% of those that paid a ransom didn't get their data back.

What happens when disaster strikes? Businesses must scramble to retrieve important data. According to IDG, it takes around 7 hours to resume normal operations after a data loss incident, with 18% of IT managers saying that it takes 11 to 24 hours, or even longer.

The Aberdeen Group found comparable numbers when comparing best-in-class companies with "average" and "laggards" in the matter of downtime and recovery. Multiply even the average amount of time it takes to recover from a downtime event (5.18 hours) by the average cost of downtime, and you've got a large bill to pay by any standard.

These costs arise from lost man-hours, reduced productivity,, recovery fees, lost customers (existing or potential), damage to your reputation, and distracted or frustrated staff and other stakeholders.

What are SMBs doing to protect themselves? Over 60% of them still ship tapes to a storage facility or another office, a surprising number, considering the technology is over four decades old and the storage and retrieval processes are extremely cumbersome. Meanwhile, nearly 20% are already using some sort of cloud-based data backup.

Local or cloud backup? The answer lies in between

Using local backup for business continuity works well for quick restores. Because the data is right there, it's fast and easy to restore back to its original location and keep the business humming. But what happens if the power goes out? If the device fails? Or if it is stolen or destroyed in a natural or man-made disaster? You might think the cloud looks more attractive for all these reasons. But cloud-only backup is risky because you can't control the bandwidth. Restores tend to be difficult and time-consuming. After all, the cloud can fail, too.

How does a hybrid-cloud solution work? Your data is first copied and stored on a local device. That way, if something happens, you can do a fast and easy restore from that device. But then your data is also replicated in the cloud. So if anything happens to that device, you've got off-site cloud copies of your data—without having to worry about moving copies of your data off-site physically.

Over the past few years, 35% of small businesses have lost as much as £300K due to downtime.

More than 90% of Small businesses fail within two years after being struck by a disaster.

Data backup vs business continuity: what's the difference?

Data backup answers the questions: is my data safe? Can I get it back in case of a failure?

Business continuity, on the other hand, involves thinking about the business at a higher-level and asks: how quickly can I get my business operating again in case of system failure?

Thinking about data backup is a good first step. Business continuity is equally important to consider as it ensures your organization is able to get back up and running in a timely matter if disaster strikes. For example, if your server dies, you wouldn't be able to quickly get back to work if you only had file-level backup. Your server would need to be replaced, software and data re-installed, and the whole system would need to be configured with your settings and preferences. This process could take days. Can your business afford to lose that time?

When talking about business continuity, we think in terms of Recovery Time Objective (RTO), and Recovery Point Objective (RPO).

RTO: The Recovery Time Objective is the duration of time within which a business must be restored after a disruption to avoid unacceptable consequences.

RPO: The Recovery Point Objective is the maximum tolerable period of time in which data might be lost due to a disaster.

By calculating your desired RTO, you have determined the maximum time that you can be without your data before your business is at risk. Alternatively, by specifying the RPO, you know how often you need to perform backups. You may have an RTO of a day, and an RPO of an hour depending on what your business requires. But calculating these numbers will help you understand what type of data backup solution you need. (See Figure 6).

Once you determine your RPO and RTO, it's time to calculate how much downtime and lost data will actually cost you. Simply add up the average per-hour wage, the per-hour overhead, and the per-hour revenue numbers and you have how much a data loss will cost you.

Alternatively, check out this free, easy-to-use online RTO Calculator for instant RPO, RTO and downtime costs.

Given that budget constraints can be a challenge for many businesses, obtaining these costs provides a financial validation to justify the purchase and maintenance of a business continuity solution.

Image versus file-only backup

There are two well-known types of backup solutions: file- and image-based.

A file-based backup does exactly what it sounds like: you choose which files you want to back up, and those files are saved, to an on-site device or to the cloud, whichever type of solution you have chosen. But only the files you choose are saved. What if you forget to save a key file?

Image-based backup, on the other hand, captures an image of your data in its environment. Thus you have exact replications of what is stored on a server—

Local or cloud backup? The answer lies in between. A hybrid cloud leverages the advantages of local backup and the security of the cloud.

Calculating the real costs of data loss will provide you with the financial validation needed to justify a business

including the operating system, configurations, settings, and preferences. If a server goes down, you can restore it in minutes, rather than the hours or days it would take to requisition a new server, and install and configure the operating system.

What to look for in a business continuity solution

To sum up what we've learned today, here are some key things to look for when seeking a business continuity solution:

Hybrid cloud backup—A hybrid approach fixes the vulnerabilities that a cloud-only or local-only possess.

Superior RTO and RPO—Think in terms of business continuity rather than simply backup, and calculate how much downtime your business can endure and still survive (RTO) as well as how much data you can afford to lose (RPO).

Image-based backup—Make sure that the backup solution takes images of all data and systems rather than simply copying the files.

Conclusion

While most small businesses may not have the same size IT budget as larger enterprises, the risks facing their business data are the same. Data backup solutions come in all different flavors. No matter what solution you chose, implementing data backup and business continuity should be a priority for your organisation.

About Datto

Datto provides business continuity solutions to secure the essential business data for thousands of companies around the world. Our integrated suite of services include our market leading data backup and disaster recovery (BDR) offerings, our advanced Cloud-to-Cloud (C2C) backup services for leading SaaS applications, and our innovative network continuity solutions. All delivered as managed services primarily through Managed Service Providers (MSPs) for the data protection needs of small and midsized businesses or distributed locations of large enterprises.

Data Backup and Disaster Recovery (BDR)

Datto's BDR solutions serve a rapidly expanding market of over 5,000 MSPs worldwide. The company's 250+ PB purpose-built cloud and family of software and hardware devices provide backup and recovery for locally stored business data. Our market leading SIRIS 3 is the first data protection platform that protects any physical, virtual and cloud infrastructure running on Windows, Mac or Linux. With our Instant Virtualization technology, businesses can be up and operational within seconds after an incident. The company's BDR products comprise Datto SIRIS, Datto ALTO, and Datto NAS.

Cloud-to-Cloud (C2C) Data Protection Services

Datto's C2C solutions protect the essential business data generated by the leading SaaS applications including Microsoft Office 365, Google Apps, and Salesforce.

Founded in 2007 by Austin McChord in Norwalk, Connecticut, Datto now employees close to 800 people located in 9 offices throughout the world. Datto remains privately held and has received two rounds of investments from leading private equity firms General Catalyst and TCV.

For more information go to datto.com/uk/

datto