eResults

SOLUTION BRIEF

THE DIFFERENCES BETWEEN BACKUP AND BUSINESS CONTINUITY

USING RECOVERY TIME OBJECTIVES TO BETTER PLAN FOR BUSINESS CONTINUITY

SMBs & SMEs rarely have the IT budgets and available staff resources as their large enterprise counterparts. However, like larger organizations, protecting their data and ensuring they can recover rapidly after a disaster or other event that compromises their data and IT systems is of equal importance.

Figure 1: Reasons for IT Downtime

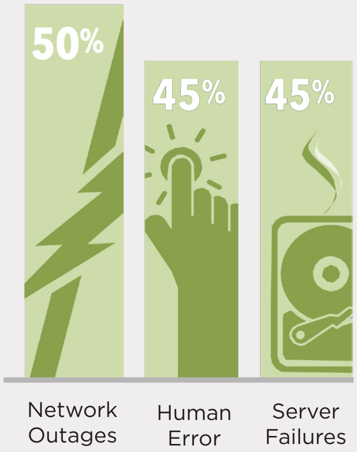
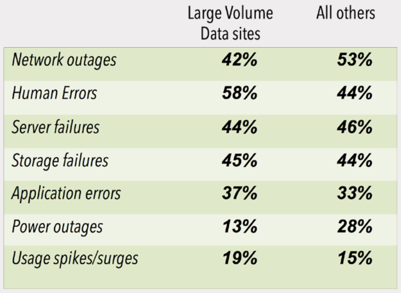


Figure 2: Downtime by data volume



	Large Volume Data sites	All others
Network outages	42%	53%
Human Errors	58%	44%
Server failures	44%	46%
Storage failures	45%	44%
Application errors	37%	33%
Power outages	13%	28%
Usage spikes/surges	19%	15%

This white paper reviews what is at stake when businesses fail to adequately protect and manage data as well plan for recovery. We will discuss the relevance of planning in terms of business continuity rather than simple data backup and furthermore, we'll look at how to calculate the all-important Recovery Time Objective (RTO) and Recovery Point Objective (RPO) so that you can architect the appropriate plan for your business, and get what you need you need from your backup and business continuity vendor.

Downtime is real. It's not a question of if, but when business will lose data. Moreover, it is very costly. According to research by the Aberdeen Group[1], it's a staggering $163,674 per hour on average. Of course, the exact cost depends on company size however the study reveals that even small companies lose approximately $8,581 per hour; medium companies $215,638 per hour; and large enterprises a whopping $686,250 for every hour of downtime.

Regardless...businesses need to plan for downtime.

So what causes downtime? It turns out that employees are greater culprits than major disasters such as fires and floods. As it turns out, these and other disasters account for just 10 percent of downtime [2]. The leading casuses ? Network outages (50 percent) and human error (45 percent) [3]   .. **See Figure 1**.

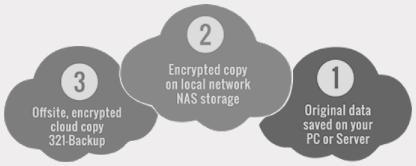
1. "Downtime and Data Loss: How Much Can You Afford?" Aberdeen Group, 2013.
2. "Enterprise Data and the Cost of Downtime," Independent Oracle User Group, July 2012.
3. "Enterprise Data and the Cost of Downtime," Independent Oracle User Group, July 2012

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 has limitations as well. Time to restore can be inhibited by internet bandwidth. Restores tend to be more time-consuming.

The answer? Easy as 3-2-1. 3 copies of your data, 2 Local (1 in production plus a local backup and 1 offsite (CLOUD) back up. Data is first copied and stored on a local device allowing fast and easy restore from that device. In addition, data is also replicated in the cloud. So if anything happens to the production servers or local device, an off- site copies of your data is stored on the cloud allowing for Disaster recovery to cloud servers all while removing the burden of managing copies of your data off-site physically.


3
Offsite, encrypted cloud copy 321-Backup
2
Encrypted copy on local network NAS storage
1
Original data saved on your PC or Server

Reviewing at the cause of downtime by data volume alone, the No.1 culprit is human error, at 58 percent. **(See Figure 2.)**

Putting off a backup and DRP plan because you consider yourself safe from major disasters is a false security. It's far more likely that a server will malfunction, or an employee will hit the delete key on an important document than any major disaster might throw at you.

What's at Stake?

No business can afford to be complacent...period! Two-and-a-half quintillion bytes of data are generated daily. 90 percent of all data in existence today was created in the last two years[5]. The portion of this data that has been generated and is stored by small business is not insignificant. Just consider the number of servers, desktops and laptops that the typical small business must manage. It all adds up to a lot of data to protect.

Consider the facts: 75 percent of SMB/SMEs have no disaster recovery plan with only 25 percent being "extremely confident" that they can restore data should an event occur that destroys their data[6]. 50 percent of SMBs back up less than 60 percent of their data. The remaining 40 percent? No protection at all[7].

The cost?...Plenty. 35 percent of SMBs lost as much as $500,000 over the past three years due to downtime. 5 percent lost up to $1 million. And 3 percent lost more than $1 million[8]. **(See Figure 3.)**

Employees	**< 1,000**	**1,000-10,000**	**> 10,000**
No costs incurred	17%	20%	8%
< $500,000	35	39	29
$500,000 – $1,000,000	5	9	8
> $1,000,000	3	3	10
Don't know/unsure	24	29	46

Figure 3: Total Cost of Downtime: Source IOUG, July 2012

So what happens when disaster strikes? Businesses scramble and race against the clock while they attempt to retrieve important data. According to IDC, it takes and average of seven hours to resume normal operations after a data loss incident, with 18 percent of IT managers saying that it takes 11 to 24 hours or even longer[9].

The Aberdeen Group concur with similar numbers when comparing best in class companies with average and "laggards" in the area of data backups. Multiply even the average amount of time it takes to recover from a downtime event (5.18 hours) times the average cost of downtime, and you've got a whopping bill to pay by any standard. **(See Figure 4.)**

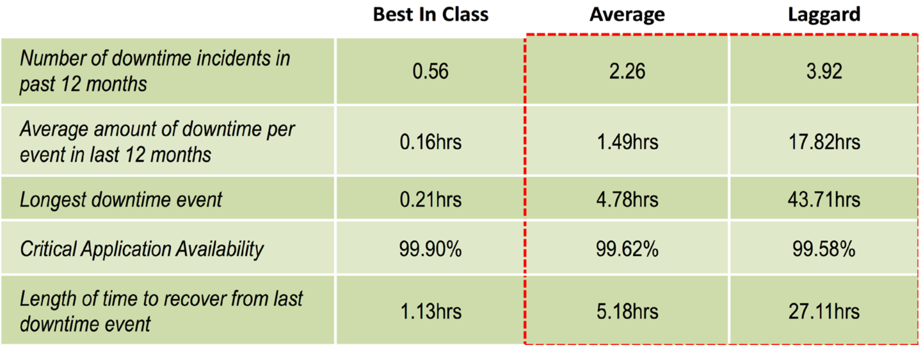
61%

of SMBs still ship backup tapes to a storage facility or another office

4. “Enterprise Data and the Cost of Downtime,” Independent Oracle User Group, July 2012.
5. “Small Business? Look to Big Data,” Curt Finch, The International Community for Project Managers, Jan. 2014.
6. Symantec 2012 SMB Disaster Preparedness Survey, 2012.
7. Symantec 2011 SMB Disaster Preparedness Survey, 2011.

8 “Enterprise Data and the Cost of Downtime,” Independent Oracle User Group, July 2012.

9 “Wanted: Better Backup,” IDG Research Services, May 2012Have at least three copies of your data.



	Best In Class	Average	Laggard
Number of downtime incidents in past 12 months	0.56	2.26	3.92
Average amount of downtime per event in last 12 months	0.16hrs	1.49hrs	17.82hrs
Longest downtime event	0.21hrs	4.78hrs	43.71hrs
Critical Application Availability	99.90%	99.62%	99.58%
Length of time to recover from last downtime event	1.13hrs	5.18hrs	27.11hrs

Figure 4: Downtime figures for SMBs in the case of data loss:

Source Aberdeen Group, May 2013

It should come a no surprise that 40 percent of all businesses close their doors permanently after a disaster, or major data loss - according to the Federal Emergency Management Agency (FEMA).

The U.S. Small Business Administration (SBA) indicates that more than 90 percent of businesses fail within two years after being struck by a disaster

Yet, SMB/SMEs fail to protect themselves! Shockingly 61% still ship tapes off to a storage facility or another location. A surprising number, considering that tape technology that is more than four decades old and the processes for saving data to tape, storing it to a remote location, and retrieving it in case recovery is needed are extremely time consuming. 13% percent don’t do anything at all. But, interestingly enough, 19% are already using some sort of cloud-based data backup[10]. **(See Figure 5.)**

Full Image Versus File-Only Backup for Business Continuity

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

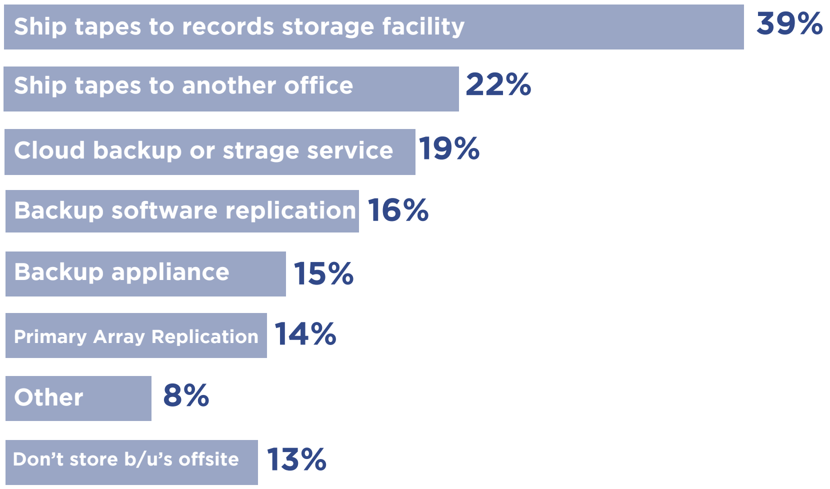


Figure 5: Methods for sending backup data offsite:

Source Information Week

Data backup versus business continuity: what’s the difference?

Data backup, Disaster recovery, Business Continuity...these terms are often used and interchanged when it comes to discussing data protection.

To be clear, data backup simply addresses the issue copying and making data safe and retrieving it in case of loss or failure.

Business continuity however, is about protecting the business at a higher level. It demands that we know the answer to: how quickly can I get my business operating again in case of system failure?

Having a robust data backup plan is a good first step. But in the event of a major failure, you have to get that data and system state of your servers back and restored quickly enough so your business doesn’t suffer. Remember that hardware failure is the No. 1 cause of lost data— if a server fails chances are you will be unable to quickly get back to work especially if you only had file-level backup. To recover the server needs to be replaced, all software re-installed, data re-installed followed by the whole system beingconfigured with the required settings and preferences. This process can take hours or even days. In the meantime, your business and users are at a stand still.

Much or all of this can be avoided by implementing a proper disaster recovery and business continuity plan. Doing so will identify the Recovery Time Objective (RTO), and Recovery Point Objective (RPO) for the business.

Calculating your RTO and RPO will give you the financial insight needed to justify a business continuity purchase

RTO (Recovery Time Objective): The duration of time within which a business must be restored after a disaster or disruption to avoid unacceptable consequences associated with a break in business continuity.

RPO (Recovery Point Objective): 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 begins to experience serious trouble and financial loss. Similarly, specifying the RPO, you know how often you need to perform backups, because you know how much data you can afford to lose without damaging your business. You may have an RTO of a day, and an RPO of an hour. Or your RTO might be measured in hours and your RPO in minutes. Calculating these numbers will help you understand what type of data backup solution you need **(See Figure 6)**.

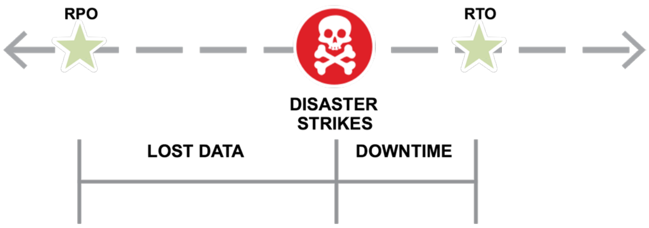


Figure 6: The difference between RTO and RPO

Once RPO and RTO are determined, it’s time to calculate how much downtime and lost data will actually cost you. Although several factors contribute to this a few simple questions will assist:

How many employees would be affected if critical data were unavailable?
What is the average wage of the affected employee (per hour)?
What is the per-hour overhead cost of the affected employees?
How much revenue would be lost per hour as a result of the unavailability of data?

Adding up the average per-hour wage, the per-hour overhead, and the per-hour revenue numbers provides a rough estimate of data loss cost to the business.

Funding and budget constraints are often obstacles for a business to implement a business continuity solution however, calculating your RTO will give you the financial validation needed to justify its purchase and maintenance.

Visibility into the real costs associated with data loss gives SMBs & SMEs a better understanding of the vulnerability and risks associated with data loss. Knowing this puts your backup solution into perspective.

About eResults

eResults is committed to helping small and medium sized businesses better understand the benefits of cloud computing to help them achieve their business goals.

eResults is 100% Canadian, and all of our cloud assets are located in Canadian Tier 3 certified data centers. This provides our customers with peace of mind knowing where their data or their client's data resides. We offer a full suite of cloud services from servers, backup, file sync and archive, through to virtual desktops and hosted Microsoft solutions.

Contact us today to learn how eResults can provide you with the partnership and peace of mind that you're looking for.

What To Look for in a Business Continuity Vendor

When comparing vendors for a backup solution, SMBs say that reliability (33 percent) and price (29 percent) top the list of factors that drive their choices. But they should consider other factors as well.

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).

Hybrid cloud backup—As discussed above, taking a hybrid approach fixes the vulnerabilities that a cloud-only or local-only possess.

Image-based backup—Make sure that the backup solution takes images of all your data and systems, and doesn't simply copy the files alone.

DRP testing and validation. Make sure your vendor provides testing capabilities for your back

Backup verification. What good is a backup if it's not working? Demand proof

Conclusion

Ensuring your business can resume operating in case of a disaster is just as essential to SMBs & SMEs as it is to the largest enterprises. For that reason a business continuity plan using data backup is an essential requirement that SMBs & SMEs should deploy. There are several Data backup solutions available. Deploying a solution that incorporates a local and Cloud component provides the recovery assurances that every business needs.

A hybrid backup provides the best of all worlds: data can be recovered quickly from a local device for the most common causes of data loss, but at the same time data is safely stored in the cloud for more extreme events in which the local device is destroyed or unavailable.

Publication Date: June 2020