SMBs and large enterprises alike need to protect their data—and make sure they can get back to business rapidly after a disaster or other event that compromises their data and systems.

In this whitepaper, we’ll discuss what’s at stake when it comes to not just protecting, but also managing, your data (hint: your business). We’ll explain why it’s important to think in terms of business continuity rather than simply data backup. And, we’ll look at how to calculate the all-important Recovery Time Objective and Recovery Point Objective, so you can get what you need from your business technology partner.

---

Whitepaper Contents

- The Numbers Don’t Lie: Companies Need to Plan for Downtime
- Key Topics to be Aware of
  - 1. What and How Much is Really at Stake
  - 2. The Difference between Data Backup and Business Continuity
  - 3. What to Look for in a True Business Continuity Solution
- Conclusion
Across all businesses, the per-hour cost of a data loss event is staggering. These numbers don’t lie: companies need to plan for downtime.

Downtime is real, and it’s costly. On average, 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.

What causes downtime? As it turns out, businesses should be more wary of their own employees than of natural disasters. Research shows that natural disasters account for just 10% of downtime. What are the leading culprits? Network outages (50%) and human error (45%).

So, if you’ve been putting protecting your data off because you consider yourself in a safe zone, you need to understand that it’s far more likely that a server will malfunction, or that someone will hit “DELETE” on an important document, than anything Mother Nature could throw at you.

When it comes to data and downtime, no business or organization can afford to be complacent, and must be aware of:

• What and How Much is Really at Stake
• The Difference Between Data Backup and Business Continuity
• What to Look for in a Business Continuity Solution

1. What and How Much is Really at Stake

2,500,000,000,000,000,000 (quintillion) bytes of data are generated daily. And, 90% of the total data in existence was created within the last two years. A not-insignificant portion of this has been generated—and is stored—by small businesses. Consider all the servers, desktops, and laptops that the typical small business must manage. It all adds up to a lot of data to protect.

Yet nearly 75% of SMBs possess no disaster recovery plan, and only 25% are “extremely confident” that they can restore data in the case of an event that destroys their data. And, 50% of SMBs back up less than 60% of their data. The remaining 40%? No protection for it whatsoever.

How much does this cost? Plenty—35% of SMBs lost as much as $500,000 over the past three years due to downtime, 5% lost up to $1 million, and 3% lost more than $1 million.
So, what happens when disaster strikes? Businesses must scramble. And, the clock is ticking while they attempt to retrieve important data. According to IDC, it takes, on average, seven 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 came up with comparable numbers when it compared best-in-class companies with average and “laggards” in the matter 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.

Small wonder that 40% of all businesses close their doors permanently after a disaster, according to FEMA. Similar statistics from the US Small Business Administration indicate that more than 90% of businesses fail within two years after being struck by a disaster.

What are SMBs doing to protect themselves? 61% still send tapes to a storage facility or another office—a surprising number, considering that this is a technology that is more than four decades old, and the processes for saving data to tape, removing it to a remote location, and retrieving it in case recovery is needed are extremely cumbersome. 13% don’t do anything at all, while 19% are already using some sort of cloud-based data backup.

61% of SMBs still ship backup tapes to a storage facility or another office.

2. The Difference Between Data Backup and Business Continuity

Although overlapping, these terms represent uniquely different mindsets when it comes to data protection.

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. But, in case of failure, you have to get that data back and restore it quickly enough, so your business doesn’t suffer. For example, if your server dies, you wouldn’t be able to quickly get back to work if you only had file-level backup. For you to start working again, your server would need to be replaced, all software re-installed, data re-installed, and then the whole system would need to be configured with your settings and preferences. This process could take hours or even days—and in the meantime, your users can’t get their jobs done.

If you’ve planned for business continuity, however, you’ve thought of all these things. You’ve thought in terms of Recovery Time Objective, and Recovery Point Objective.

- **Recovery Time Objective (RTO):** 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.

- **Recovery Point Objective (RPO):** 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 gets into serious trouble. Alternatively, by 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. It’s all up to you and what your business requires. Calculating these numbers will help you understand what type of backup solution you need.

**The Difference Between RPO and RTO**

<table>
<thead>
<tr>
<th>RPO</th>
<th>RTO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lost Data</td>
<td>Downtime</td>
</tr>
</tbody>
</table>

**Local or Cloud Backup? The answer lies somewhere 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’s 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.

The answer? A hybrid-cloud solution. The way this works: 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 offsite cloud copies of your data—without having to worry about moving copies of your data off-site physically.

---

No one knows technology solutions like Stratix.

![Local Device → Data Center](image)

---

[www.stratixsys.com](http://www.stratixsys.com)
Once you determine your RPO and RTO, it’s time to calculate how much downtime and lost data will actually cost you by calculating:

- 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 per-hour revenue would be lost if data were inaccessible?

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.

Given that funding and budget constraints can be the top challenge (43%) for a business to implement a business continuity solution, calculating your RTO will give you the validation needed to justify its purchase and maintenance.

Calculating the real costs associated with data loss gives SMBs a better understanding of the risks relating to business failure. And, thinking about your business in these terms puts your backup solution into perspective. The “it won’t happen to me” mindset simply doesn’t fly.

3. What to Look for in a true Business Continuity Solution

When comparing backup solutions, businesses say that reliability (33%) and price (29%) 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 cost related to downtime and data loss. Choose a solution that can guarantee top RTOs and RPOs.
- Hybrid Cloud Backup: As discussed, 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.
- Instant local and off-site virtualization.
- Screenshot backup verification—demand proof that the solution works.
- Images saved as VMDK for faster recovery times.
Calculating the real costs associated with data loss will give you a better understanding and put your backup solution into perspective. The “it won’t happen to me” mindset simply doesn’t fly.

Conclusion

Making sure your business can continue operating in case of a disaster is just as essential to SMBs as it is to the largest enterprises. For that reason, business continuity using data backup is an essential solution that all companies and organizations should deploy.

Data backup solutions come in all different flavors. Cloud-based solutions are increasingly popular, but they provide only a partial answer. On-site solutions also have their weaknesses.

The answer is a hybrid cloud. It provides the best of all worlds: you can recover data swiftly from a local device for the most common causes of data loss, but you have all your data safely stored in the cloud for more extreme events in which the local device is destroyed or unavailable.

Contact Stratix Systems for more information about our Proactive data backup and business continuity solutions.

Sources

This whitepaper is reprinted by Stratix Systems with express permission from Datto, Inc. All right reserved.

- Symantec 2012 SMB Disaster Preparedness Survey.
- “IT Trends: Disaster Recovery,” InformationWeek.