Backup vs. Business Continuity: Using RTO to Better Plan for Your Business

Executive Summary

Ambulatory healthcare practices don't have the same IT budgets and staffs as larger hospitals. Yet just like larger hospitals and clinics they need to protect their data—and make sure they can get back to see patients rapidly after a disaster or other event that compromises their data and systems. Getting and keeping access to the medical record for all patients is necessary for patient safety, malpractice concerns, and to meet state medical record retention law requirements.

In this white paper, we'll discuss what's at stake when it comes to not just protecting, but also managing, your data (hint: your practice). 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 (RTO) and Recovery Point Objective (RPO) so that you can get what you need from your business continuity vendor.

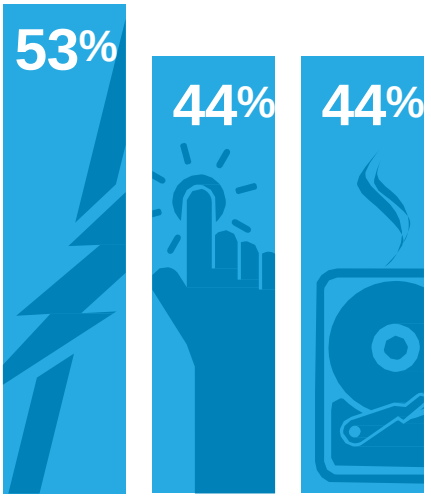
Introduction

Downtime is real, and it's costly. Across all businesses, it's a staggering $163,674 per hour, according to research by the Aberdeen Group.1 Of course, the exact cost depended on company size: 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. The numbers speak for themselves: you need to plan for downtime. What causes downtime? As it turns out, businesses should be more wary of their own employees than of natural disasters. Although hurricanes, tornadoes, and the like do their fair share of damage, research shows that natural disasters account for just 10 percent of downtime.2 The leading culprits? Network outages (53%) and human error (44%). (See Figure 1.)

	"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%***

Figure 2: Downtime by data volume

So what's even more frightening than a hurricane? When you look at cause of downtime by data volume alone, the No. 1 culprit is human error, at 58 percent. (See Figure 2.) 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 the delete key on an important document than anything Mother Nature could throw at you. No business any- where can afford to be complacent.



#1 – *Network outages*
#2 - *Human error*
#3 - *Server failures*
Figure 1: Reasons for downtime

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.

What's at Stake?

Two-and-a-half quintillion bytes of data are generated daily. And 90 percent of the total data in existence was created within the last two years.[5] A not-insignificant portion of this has been generated—and is stored—by small businesses and with the EMR push from healthcare organizations as well. Consider all the servers, desktops, and laptops that the typical medical office must manage. It all adds up to a lot of data to protect.

Yet nearly 75 percent of SMBs possess no disaster recovery plan, and only 25 percent are "extremely confident" that they can restore data in the case of an event that destroys their data.[6] And 50 percent of SMBs back up less than 60 percent of their data. The remaining 40 percent? No protection for it whatsoever.[7]

How much does this cost? Plenty. Thirty-five percent of SMBs lost as much as $500,000 over the past three years due to downtime. Five percent lost up to $1 million. And 3 percent lost more than $1 million.[8] (See Figure 3.)

	< 1,000	1,000 to 10,000	> 10,000
No costs incurred	17%	20%	8%
< $500,000	35%	39%	29%
Between $500,000 and $1 million	5%	9%	8%
> $1 million	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? Practices 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 percent of IT managers saying that it takes 11 to 24 hours, or even longer.[9]

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. (See Figure 4.)

	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	0.16 hrs.	1.49 hrs.	17.82 hrs.
Longest downtime event	0.21 hrs.	4.78 hrs.	43.71 hrs.
Critical application availability	99.90%	99.62%	99.58%
Length of time to recover from last downtime event	1.13 hrs.	5.18 hrs.	27.11 hrs.

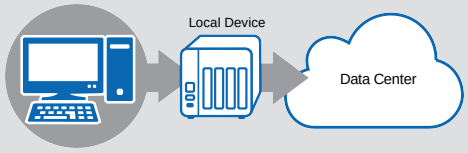
Figure 4: Downtime figures for SMBs in the case of data loss

Source: Aberdeen Group, May 2013

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.

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 off-site cloud copies of your data—without having to worry about moving copies of your data off-site physically.



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 2012

Small wonder that 40 percent of all businesses close their doors permanently after a disaster, according to the Federal Emergency Management Agency (FEMA). Similar statistics from the U.S. Small Business Administration (SBA) indicate that more than 90 percent of businesses fail within two years after being struck by a disaster.

What are practices and SMBs doing to protect themselves? Sixty-one percent still ship tapes off 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. Thirteen percent don't do anything at all. But, interestingly enough, 19 percent are already using some sort of cloud-based data backup.[10] (See Figure 5.)

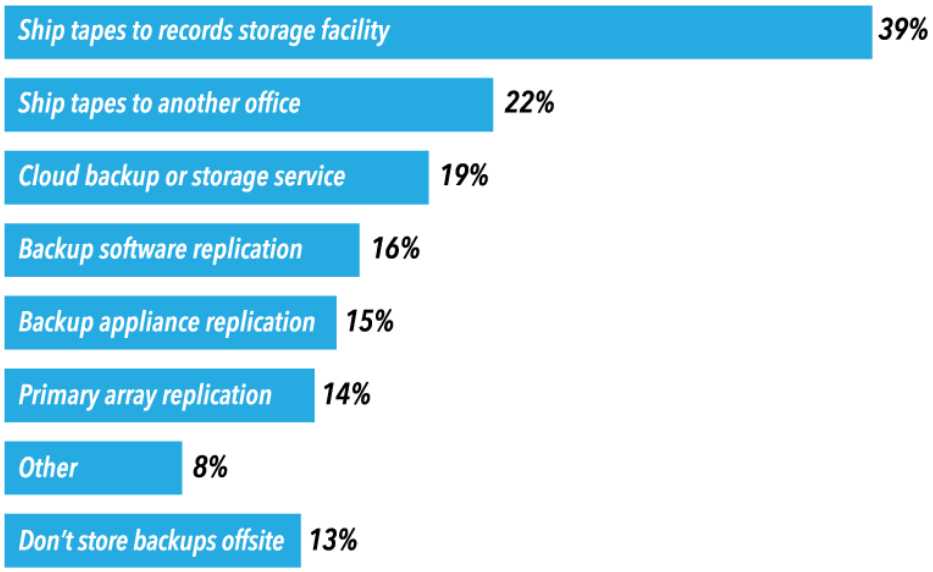


Figure 5: Methods for sending backup data offsite *(Multiple responses allowed)*

Source: InformationWeek

61%

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

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

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 practice at a higher level, and asks: how quickly can I get my practice 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—and remember, hardware failure is the No. 1 cause of lost data—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.

10. "IT Trends: Disaster Recovery," InformationWeek, July 2013.

If you've planned for business continuity, however, you've thought of all these things. You've thought in terms of Recovery Time Objective (RTO), and Recovery Point Objective (RPO).

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 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. But calculating these numbers will help you understand what type of data backup solution you need (See Figure 6).

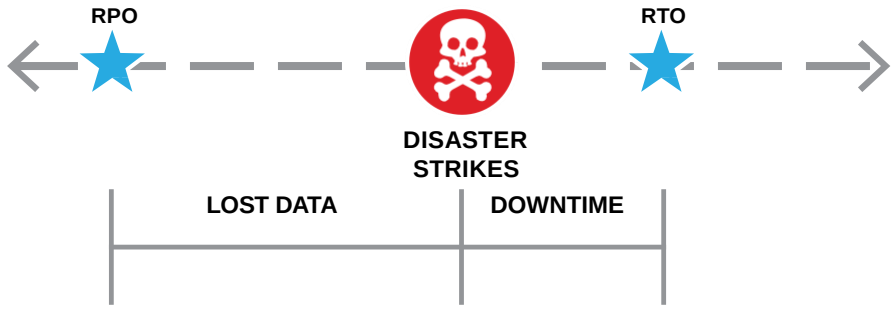


Figure 6: The difference between RPO and RTO

Once you determine your RPO and RTO, it's time to calculate how much downtime and lost data will actually cost you.

Answer the following questions:

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

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 percent) for a practice to implement a business continuity solution, calculating your RTO will give you the financial validation needed to justify its purchase and maintenance.[11]

Calculating the real costs associated with data loss gives practices a better understanding of the risks relating to systems and network 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.

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.

11. "Enterprise Data and the Cost of Downtime," Independent Oracle User Group, July 2012.

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 (RFO). Choose a vendor that can guarantee top RTOs and RPOs.
- 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.
- Instant local and off-site virtualization.
- Screenshot backup verification. What good is a backup if it's not working? Demand proof.
- Images saved as VMDK for faster recovery times

Conclusion

Making sure your practice can continue operating in case of a disaster is just as essential to your practice as it is to the largest hospitals. For that reason, business continuity using data backup is an essential solution that practices 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.

Calculating RTO and RPO made easy with Datto's online RTO Calculator

Easy to access and easy to use Go to http://tools.dattobackup.com/rto

About Datto

Datto Inc. is the preferred provider of hybrid cloud-based backup, disaster recovery (BDR) and Business Continuity solutions for the Channel, available in both physical and virtual platforms. Datto provides best-in-class technology and 24/7/365 Tech Support to its 8,000 partners worldwide.

The Datto product line is comprised of Datto SIRIS 2, Datto ALTO XL, Datto ALTO 2, and Datto NAS. Its solutions serve the needs of business of every size, with options ranging from 150GB to 100TB. Unique feature sets include instant local and off-site virtualization, Screenshot Backup Verification, Inverse Chain Technology, and End-to-End Encryption.

Datto Partners sell the solutions to a wide range of vertical markets including: small business, healthcare, financial, education, banking, legal, manufacturing, retail, and municipal.

Calculating your RTO will give you the financial validation needed to justify [a business continuity] purchase.

Isn't it time you take a proactive approach to protecting your practices critical patient data?

MEDICUS IT
100 North Point Center
East Suite 150
Alpharetta, GA 30022
(678) 495-5900
www.medicusIT.com