MICRODATA'S

Micro/Outlook

Why Cloud Backup isn't Disaster Recovery Protection

Everyone understands that backing up company data is a good idea. And most organizations have at least looked at the idea of backing up to the Cloud with a product like *Mozy, Carbonite, Acronis*, or *iDrive*. Backing up to the Cloud is appealing as there's no need for local drives, tapes, or software. But most business owners and managers don't understand that a **Cloud or on-premises backup isn't a disaster recovery solution**. This is something that you don't want to learn in the midst of an actual disaster, so today I'm going to take a few minutes to explain the difference between backups and a real disaster recovery solution. I've also got a special offer for MicroData's SafeGuard Disaster Recovery solution that I'll tell you more about.

What is a DR Solution?

The fundamental purpose of any disaster recovery solution is that it has to be able to get your business back to work, and quickly. And it has to function in any type of disaster. Most people typically think about a disaster as a fire, but a DR solution has to cover <u>all</u> possibilities that can disrupt your business operation for more than a hour or two. So the list should include:

- Fire

- Floods (including/burst frozen pipes)

- Physical building damage from hurricanes, heavy snow loads, etc.

- Buildings becoming unusable due to lack of heat/water/power

FREE Dark Web Scans Through March 31

92% of businesses tested in 2017 had key employee passwords and/or sensitive *Personally Identifiable Information* for sale on the Dark Web.

Your business may have the latest firewalls, security suites, end-user training, and 24x7 monitoring, but it's all <u>useless</u> if someone has account information and a password and just logs in.

The **Dark Web** is the shopping market for cyber criminals that want to buy compromised data such as:

- Your users' network and computer login credentials

- Bank account and credit card numbers

- Social Security numbers

- Patient and customer information

MicroData's **Dark Web Guardian** service continuously searches hundreds of sites on the Dark Web 24x7 and alert you when a compromise is found allowing you to act before damage is done.

To learn more, contact us today at 978.921.0990 or on the web at microdata.com

Inside this issue:

March 2019

This monthly publication is provided courtesy of Glenn Mores, President & CEO of MicroData of Beverly Massachusetts.

Our Mission: To Provide Phenomenal IT Support to companies throughout the Eastern Massachusetts/Southern NH area.

- Extended electrical outage (ice storms, hurricanes, building transformer failures, construction accidents, etc)

- Server/network equipment failure

- Server/network equipment/data damage due to malicious employee action

- Data loss due to malware/ransomware

And here in New England we've experienced our share of <u>all</u> these calamities so it's really a question of when, not if, the next disaster will occur.

So let's look at how disaster recovery would work out assuming you've got a good backup. If you <u>don't at least</u> have a good backup statistics show it's unlikely your business will survive.

Disaster Recovery from a Backup

Let's say your business has a single server and it dies. Maybe an electrical storm created a surge and fried its circuitry. Or maybe it's now locked down with ransomware and you either have to pay $10,000 in Bitcoin to **maybe** get your data back or start restoring from backups (assuming they weren't also infected). But whatever the reason, the box itself isn't usable. And let's say you've been smart and you have an off-site Cloud backup that has a complete server image that can be restored (and not just individual files). What does your recovery look like?

In this case, probably 3-5 days is a realistic timeframe. First, you need to get that Cloud backup back—all of it. Downloading it isn't an option as **it can take days**. This is just a reality of a Cloud backup—backing up or restoring a few files is no big deal but the services are SLOW for large quantities

of data. So maybe you'll pay to have the Cloud backup vendor put all the data onto an external USB hard drive and FedEx it to you. Plan on at least 2 days for that.

And while you're waiting for your data you need to get replacement hardware. Server, networking, and high-end workstation hardware isn't available at any local retail store so you'll have to order replacements online. Maybe with overnight shipping you'll be able to get it in a day or two, but it can be a challenge as manufacturers like Dell & HP often only build systems as customers place orders.

And don't forget any software you need. Did you have to order media from vendors and have it shipped to you or worse, did you need to schedule with a vendor to install and configure their application?

Cloud or on-premises backup <u>isn't</u> a disaster recovery protection solution

So let's assume it's Day 3 and you have everything you need. Now the IT pro's have to come in and assemble it all, install the new server operating system & applications and/or restore the backup data, and then test and debug everything.

It's easy to see how this could take a week—or more.

And what if your offices aren't usable? Just this fall we had gas fires in North Andover and Lawrence and even companies that didn't have any problems with gas found their electricity off for 4 days and many had no heat or hot water for <u>weeks</u>. How will your recovery timeframe be impacted if you need to get everyone to a temporary workspace? What about networking wiring, & Internet service? **You could easily be looking at weeks to restore operations.**

Recovery with a Real Disaster Recovery Solution

Same scenario: you have a server that dies. But since you have MicroData's *SafeGuard Disaster Recovery Service*, you make a quick call to MicroData and they access a special computer system they installed at your location as part of SafeGuard. 15 minutes later a *Virtual Server* copy of your failed server (as of just before the disaster) is up and running and all your users go back to work. You can take your time sorting out whatever the problem was.

But what if it's worse? Let's say water pipes froze and burst and you not only have to get out of your building for 2 weeks while damage is repaired, but your server and even that MicroData special computer system have been destroyed.

It's no problem.

Within 15 minutes MicroData brings up a *Virtual Cloud Server* of your failed system and using a small application we provide to your users, they can work from <u>any</u> computer and access that Virtual Cloud Server and all your data. So employees could work from home, rented office space, or even a Starbucks. All that's needed is any computer and an Internet connection.

The Best Part

Truly the best part is that a real Disaster Recovery solution like MicroData's SafeGuard often costs no more than a plain old backup solution like Carbonite.

And through March 31, we're offering SafeGuard to new customers with 50% off the one-time setup charge.

To learn more, contact us at 978.921.0990 or online at **microdata.com/disaster**

Leadership and the Art of Performance

Leadership is a role, a part you play in front of many audiences. It's a part that comes with many expected and unexpected demands. Finding the balance, what you are truly responsible for versus what you assume responsibility for, is the difference between whether or not you succumb to the Leadership Killer.

In the classical (and stereotypical) view of leadership, you're expected to carry yourself with a commanding presence so that people know you're "in charge." You're expected to have more experience and knowledge than those you're leading and to have timely and accurate answers to their many questions. You are presumed to be strong to the point of being unshakeable and invulnerable. When things get dicey, you're supposed to push interference out of the way and say, "I got this!"

During a conversation about the pressures of leading others, an executive vice president of an electrical company commented, "What makes leadership so hard is that everyone needs you to play a different part. Some employees respond best when you treat them as equals. But with others, if you do that you'll lose their respect. They work best following a chain of command, and they respond better when you give them explicit directives. Some want you to be an authority figure, some want you to be a coach, some want you to be a friend. And you may not even actually be any of those things, but to keep them motivated, you try to play the part they expect."

As he suggests, the leadership role requires versatility. Sometimes it calls for you to be tough, direct, and blatantly honest. Other times it requires you to be compassionate, caring, and friendly. It makes no difference that you're authentic disposition is; the role of leadership sometimes demands that you act against who you actually are. This is not unlike being an actor when some parts require that you "play against type."

The danger of over-attending to the role of leader is that you may start to lose sight of your true self. Some leaders get so wrapped up in the performance that they don't know how to step out of it. They stay in a constant state of theatrics, pretending to be invulnerable, strong, and in control. All the while their true self goes unnourished, and, before long, they become the proverbial man in the gray flannel suit, a shell of a human being, all work and no soul.

This is what the Killer wants. Hubris's work will be much easier if you have no sense of self, no depth and dimension, and no sense of identity beyond your leadership role. Hubris will be in a much better position to shape and define you when you have no earthly idea who you are outside of your role of leader.

Check your performance level. As a leader, put your role in perspective by considering:

- Who are your stakeholders?

- Which people are relying upon YOU?

- Who can't do a good job unless YOU do a good job?

- Who do YOU depend on to do your job effectively?

- How are your relationships with the people who have a stake in your being an effective leader?

- Which connections deserve more attention?

Tech Tips

Android Tech Tips

The Android environment is now the most popular computing platform in the world. Google is always making tweaks and manufacturers like Samsung and LG add their own touches on top, so here are some tips we especially like.

Find My Phone

We've all lost track of a phone some point. Rather than ransacking your house, just use Google's 'Find my phone' tool. Just open up any browser, log in with your Google account, then go to google.com and type in 'Find my phone'.

Do Not Disturb Settings

You'll find the settings for this feature either in your volume popup when you hit the toggle or by going into the system settings for notifications

← Do Not Disturb

(usually Sound and Notification). It will be called Do Not Disturb on most devices. In this menu, you can choose when DND is toggled on automatically, what is blocked, and if any contacts are allowed to ring through anyway.

"OK Google" Voice Match

Google search is at the heart of all Android phones, and you can start searching at any time just by saying "OK Google." This works on the home screen and in the search box automatically.

Use Power Saving Modes

All Android phones have power saving modes of some sort -- sometimes two or three of them. Head to the battery menu (usually just Settings > Battery) on most phones to see these settings. For example, Samsung offers a regular power saving mode that reduces screen brightness and slows the CPU, then there's also an ultra power saver that locks the device to just a few essential applications.

© MARK ANDERSON

"According to all the big data we've gathered, our discussions about big data are up 72% this year alone."