Connectability

The Toronto Business Owner's Guide To Backup & Disaster Recovery

Business Continuity, Disaster Recovery & Cloud Backup:

What They Are, Why You Need Them, and How They Can Prevent Data Loss, Extended Downtime, and Cyber Security Attacks

Dedicated To Your Success
info@connectability.com | (416) 966-3306

The Toronto Business Owners' Guide To Backup, Disaster Recovery & Cloud Storage

Business Continuity, Disaster Recovery & Cloud Backup:

What They Are, Why You Need Them, and How They Can Prevent Data Loss, Extended Downtime, and Cyber Security Attacks

Read this guide and you'll discover:

- The 5 most common types of Backup solutions and the pros and cons of each
- How a Business Continuity & Disaster Recovery (BCDR) Solution works, and how it can prevent data loss, downtime and hacker attacks
- What some backup vendors exclude that could end up costing you a bundle in the long run.
- The hidden truth about SharePoint, Google Drive and Dropbox, and what you need to do to reduce your risk.
- Key questions you need to be able to answer about your backups. If you can't then you've chosen the wrong solution.

Provided as an educational service by:
Ted Shafran
President
Connectability Inc.
970 Lawrence Avenue West, Suite 402
Toronto, ON M6A 3B6
(416) 966-3306
www.connectability.com

Retention and Cost Are Just Two Small Considerations. The Big Question Is: **"How Fast Can I Be Up And Running In An Emergency."**

From The Desk Of: Ted Shafran
President,
Connectability Inc.

Dear Colleague,

How effectively are you protecting your company's data? Do you know how quickly you can be back up and running in the event of an emergency? Do you have protections in place to prevent hacker attacks, data theft, and downtime?

If these questions make you nervous, don't worry, you're not alone. That's actually one of the main reasons I wrote this report: a lot of CEO's, CFO's, GM's and Office Managers know that they should be concerned about protecting and preserving their data, but they just don't know enough to find the right solution – at the right price.

My name is Ted Shafran, and I am the President of Connectability and author of *"The Business Owner's Common-Sense Guide To Trouble-Free IT".* We've been delivering IT Support, backup services and cybersecurity protections to businesses in the Greater Toronto Area for over 25 years. You may not have heard of us before, but I'm sure you're familiar with one or more of the other businesses who trust us to manage their technology. A few of their comments are enclosed.

When prospective customers first speak with us, they almost always have questions about their backups. Some companies are most concerned with backing up their on-premises or cloud hosted servers, while other businesses don't require a server and are more concerned about protecting data in cloud applications like SharePoint, Google Drive and Dropbox. And for some, backing up and preserving their ERP data is the critical element. So, the type of backup you need is going to be very specific to your organization's needs, the quantity of data to back up, and your unique uptime objectives.

Regardless of where you store and access your data, it's imperative that you've covered all your bases, and that all company data can be restored quickly in the event of a disaster. Failing to do so could result in data loss, lost sales, extended downtime, data theft, bad PR or even being forced to close your doors for good.

Ultimately, the goal of this report is to help you make the most informed decision possible, so you end up with the right backup solution for your business. A decision that will limit downtime, reduce cybersecurity exposure and improve recoverability, all within a budget that is right for you.

Dedicated to your success,

What Backup Options Do I Have?

There are HUNDREDS of different options out there when it comes to backing up your data. There are consumer-grade options, business grade-options, and enterprise-grade options reserved for the Fortune 500's. And every article you read will tell you something different. There is so much information out there that it's become very difficult for business leaders to make an informed decision.

Even more confusing, there are different backup solutions depending on where you store your company's data – further complicating the situation. The truth is, there isn't one single backup solution that is right for every business. Every company is different, so it's important to evaluate options based on your unique circumstances.

For the purposes of this section, I will be focusing entirely on backing up your server data. We will take a look at backing up cloud applications (like SharePoint and Google Drive) in a separate section of this report.

The 5 Most Common Types of Backup And The Pros & Cons Of Each

On-Premises Backup:

Back in the "bad old days" of computing, if you needed to back up your server, you had no choice but to use tape drives. The issue with tape drives is that they have a 100% failure rate, meaning that over time, all tape drives will fail eventually. As a result, this method of backup was frequently unreliable. You had to regularly test the tapes to confirm they could be restored in an emergency. And if it came time to actually restore this data, the process was slow and involved. Worse still, tape backups have a shelf life – they decay over time.

Nowadays, many businesses use external hard drives to secure their data – largely because these solutions are inexpensive and easy to use. Unfortunately, it's easy to corrupt an external drive. All it takes is one drop, a small spill, or an employee leaving the drive in an overheated car and all that data could be gone forever. Plus, if you don't take these drives offsite regularly, the backups won't protect you if you experience a fire, flood, overheating, a power surge, or robbery or vandalism.

A more robust on-premises backup solution is a Network attached storage (NAS) device. These are much more reliable than an external hard drive, and they have much greater capacity, but they also leave you vulnerable to the same environmental disasters that I mentioned above. Unless this data is taken offsite regularly, it could all be destroyed by a natural disaster, theft, or a disgruntled employee.

So, while an on-premises solution is a good starting point, it certainly doesn't offer the level of reliability, redundancy and recoverability that most modern businesses require.

Cloud-Based File-Level Backup:

The next level of backup is a cloud-based data backup. Instead of backing up your data onto your own equipment, you store the backups on infrastructure owned by the backup vendor. And although it might seem counter intuitive to store your data on someone else's equipment, there are several benefits.

1. **Redundancy.** Assuming you've chosen the right vendor, when you store your data in the cloud, there's a very good chance that your information is being mirrored to a redundant data centre. If one data centre experiences a natural disaster like a fire or flood, or a major hardware failure, your information is still safe and sound in another location. Most businesses can't say the same about data stored in their offices.

2. **Security.** Many companies that offer backup services are very large, and therefore have substantial resources to invest into physical security (cameras, fingerprint scanners, retinal scanners, key cards, and 24 hour armed guards), and virtual security, with advanced firewalls to protect the perimeter of their networks, along with enterprise-grade antivirus, antimalware, and anti-spyware tools. Chances are your information is more secure in the cloud than it is on your own network.

3. **Cost.** Over the past decade, cloud backup prices have dropped considerably. What was once a high-end solution available only to Fortune 500 companies is now more accessible than ever. Many backup solutions even include unlimited storage, so you don't have to worry about cleaning up and deleting old backups.

4. **Automation.** Unlike an on-premises backup, you no longer need to check the status of your backups every day, swap drives, take them off-site, etc. Backups are performed on an automated, scheduled basis, so you don't need to worry about missing a backup. It's all done automatically in the background. Better still, you never need to worry about hard drive malfunctions, drops, or theft.

There are obviously a lot of benefits to a file-level, cloud-based backup solution. Unfortunately, there are also some pitfalls. First off, downtime and recovery after a disaster. If you experience a data breach, Ransomware, or a hardware failure, it could take

some time to get back up and running. I'll use the example of a hardware failure. If you experienced a server failure, your data is still saved in the cloud, so you won't lose any information. However, you will have to determine where to restore that data. That usually means purchasing a replacement server, configuring that server, reloading all of your software, and finally downloading your cloud data onto the server. Depending on the speed of your Internet connection and the amount of data you have, it could take anywhere from a few hours, up to a week or more to restore your data. Plus, you first need to order the replacement hardware before you can begin to restore your information. So even if you ignore the cost of downtime (lost productivity, frustrated employees, lost sales, lost opportunities, etc.), you could still be out thousands or even tens of thousands of dollars in IT support and recovery fees. If you are concerned about downtime, this probably isn't the right solution for your business.

Cloud-Based Full-Image Backup:

The next step up would be Cloud-Based *Full-Image* backups. A file-level backup is responsible for backing up the data files on your server, while a full-image backup is responsible for taking a "snapshot" of your entire system, *including* data files, the Operating System, software programs, users, permissions, and OS configurations.
In the event of a hardware failure, natural disaster or even a robbery, a full-image backup will allow you to get up and running much more quickly than with a file-level solution. Because the "image" contains your *entire* system, your IT team will spend far less time rebuilding your infrastructure from scratch and can instead focus on restoring your data right away.

That said, the timeline for restoring your data is still dependent on the speed of your Internet connection, and the amount of data you need to recover. A full-image backup is a significant step up from a file-based backup and offers you the ability to get up and running more quickly. Just make sure you have a fast Internet connection. Otherwise you could be down for hours or even days while your data restores.

Business Continuity & Disaster Recovery:

The final tier of backup, and the one we recommend to businesses who rely heavily on server infrastructure, and have tight uptime objectives, is called **Business Continuity and Disaster Recovery**, or **BCDR**.

Before I go into the pros of a BCDR solution, let me briefly explain what it does. Very simply, a BCDR solution provides multiple layers of redundancy. Let's say you and your team access files through your on-premises server. A BCDR is a physical appliance that is installed in your office and is configured to backup all of your on-premises server data. Once the backup is completed on the appliance, all of your data is then copied to a secure cloud repository for storage. Now your data is backed up both in your office, and in the cloud. So, let's say you arrive at your office on Monday morning and discover your server won't boot up due to a faulty drive. Well, thankfully the BCDR appliance can double as a

server. Your IT provider can boot your server directly from the device and BOOM, you're back to work in minutes.

But what about a disaster like a fire, flood, or even theft? Well, because your data is mirrored to the cloud, you can actually boot up your server *in the cloud* in a matter of minutes. So regardless of what disaster befalls you, you've minimized downtime, lost productivity and lost sales.

From there, the process of recovery is easy. Even in the worst case - if your office was destroyed - your data is still safe, secure and accessible from the cloud. And while you work from the cloud copy, your IT provider will work to rebuild your server infrastructure, and then restore your data.

The benefits are obvious: immediate recovery, significantly reduced downtime, and the peace of mind of knowing that you're always protected against cyber threats, hardware failures and natural disasters. Plus, because your backups are stored redundantly, even if someone were to access your company network and corrupt your on-site backups, you would still have all your data in the cloud.

To be frank, from our perspective, the only downside associated with a BCDR solution is cost. Pricing is largely based on the amount of data to be backed up, and if you have a lot of data the costs can rise quickly. But if you have a lot of archival data, we recommend backing that up to a cloud repository – ONCE. It can then be excluded from future backups, thereby reducing your monthly costs. In order to get started with BCDR, there is a one-time purchase fee for the device, along with an ongoing monthly fee for the backup. That said, if your operations depend on minimizing downtime, then a BCDR device might be the only solution that will meet your needs.

Database Backup:

While Databases can be backed up using any of the methods covered above, we generally recommend a hybrid approach. We will cover this further below, but basically, because Databases contain constantly changing information, you need to make sure your backup is suited to your specific database. But due to the size of many databases, recovery from the cloud can sometimes take hours or even days. Considering how critical databases are, we recommend taking a step further to make sure you can recover as quickly as possible. We'll touch on this more in another section of this report.

Why BCDR?

Let's start off with some tough questions.

- What would you do if your data disappeared overnight?

- How long could your business survive? How would your customers react?
- What about your employees?
- Have you developed a disaster recovery plan outlining how every member of your team should respond in an emergency?
- What are your reporting requirements? Do you need to notify your clients or the government?
- What is your liability?

If you don't know the answers to these questions, then it's very possible that the backup solution you are using **won't meet your needs** when push comes to shove.

I went into a bit of detail on Business Continuity & Disaster Recovery solutions in the summary above, but in order to fully explain why a BCDR is the most effective solution, I will have to go into a bit more detail about how they work, and how they can help prevent data loss, extended downtime, and even cyber-attacks.

A BCDR solution can be used to back up files, configuration information, operating systems and applications from your on-premises or collocated server. In effect, it acts as a multi-step full-image backup. It involves two components:

1) A physical device, and
2) Cloud storage

The physical device is connected to your company network (or the network backbone if your server is in a Colo) and backs up your entire server contents. If a drive fails on your server, or the operating system becomes corrupt, the backup device can take over and act as a temporary server. Your team can continue to work, even though your server isn't operational. All you have to do is call your IT provider and they will boot up the device. You can then continue to work as if nothing had happened. No more panic, extended downtime, or frustration.

The data on that device is simultaneously backed up to the cloud. So if your entire office were flooded, or someone backed a truck through your front entrance and took off with all of your computer equipment, you would still be able to access your data directly in the cloud. You can load a virtual server directly from the cloud and operate as normal until your infrastructure is fully restored. Once again, you just need to notify your IT provider, and they can boot your server in the cloud and show your how to access it.

By now it's probably pretty clear how a BCDR device can prevent extended downtime and data loss, but what about cyber-threats? How can a backup device prevent something like Ransomware? Or mitigate the effects of a phishing attack? It's actually surprisingly simple. In case you're not familiar with it, Ransomware is a type of Malware that hackers and cyber criminals install on a computer or server within your network, which then spreads to encrypt all of the files on your network. From there, a hacker will ask you to pay a ransom.

Generally, that ransom is somewhere in the vicinity of $30,000 - $50,000 although it can sometimes be much more.

If you refuse to pay, one of two things are likely to happens:

1) You never see your data again
2) They will publish your data so it's publicly accessible

But even if you DO pay the ransom, there's no guarantee you will get your data back. These are cyber criminals and hackers, located in countries with lax data security and hacking regulations, and no interest in enforcing laws from other countries. So you aren't exactly dealing with the most trustworthy group. Even if you do pay the ransom and they decrypt your data, what's to say that they won't do it again later? Or notify one of their pals to do the same? If you pay, you are just notifying cyber criminals that you have the money and willingness to pay.

Whether or not to pay isn't the question. The real question is, how can you restore your data without paying the Ransom? With a BCDR solution, you NEVER have to worry about this. Simply ask your IT provider to boot up the BCDR appliance, and you can access your server data. In the meantime, they will wipe your infected systems, and restore from the most up-to-date data on the appliance.

We have a saying that "The best cyber security protection is a strong backup." With a BCDR solution at your disposal, your most important resource is protected – your confidential company data.

What Backup Vendors Don't Tell You That Could End Up Costing A Bundle:

There are a TON of backup vendors out there – each of them claiming to be the right solution for your needs. While there are many solid backup providers (and we work with several of them) there are also some secrets they won't tell you that could end up costing you down the road.

The biggest and nastiest secret is that many cloud backup providers throttle data retrieval speeds. Even though your backup provider has multiple, high-speed Internet connections and might be able to restore your files at 1 Gbps, they will generally "throttle" their connection so that bandwidth is divided between multiple clients. In a lot of cases, they will allow you to retrieve some portion of your data at full speed, after which you're at their mercy. If you have a lot of data, that could result in hours or days of additional downtime. So, make sure you understand this in writing before you choose a cloud backup vendor.

Another important factor to consider is the cost of retrieval. While some providers include retrieval as a part of their backup services, many vendors (including Amazon) actually charge a separate fee for retrieving/restoring your data should you need it. And if you have a lot of data, those costs can be substantial. Make sure understand the cost of retrieval before signing on the dotted line. You certainly don't want to add insult to injury if you experience a disaster.

Finally, make sure you prioritize testing those backups. This is a concern with pretty much ANY form of backup, but it's still worth mentioning. While a cloud-based backup runs automatically on a fixed schedule, that doesn't necessarily mean that your data is recoverable. We've seen situations where a business HAS a backup in place, but they've never tested it. When it came time to restore their data (i.e. in an emergency) they realized that the backups were incomplete and therefore unusable. Most backup vendors won't tell you this, but whichever solution you choose, you can't just "set it and forget it". You NEED an IT Provider, or an in-house IT team to monitor it regularly and periodically test those backups.

What About Databases?

As I mentioned above, we believe that databases require a separate approach. While ANY cloud or onsite solution CAN back up your database, we recommend doing your research first. The problem with database backups is that if you just make a copy of the database file or files, you could be capturing that backup in the middle of a transaction. And that means that – if you need to restore that database – you could easily end up with incomplete information or even broken transactions.

Fortunately, there are several good options for protecting your valuable business data. If you're using Microsoft SQL Server or several other database products, most of them have built-in backup utilities that will perform and verify reliable database backups that can then be copied to the cloud. But in our experience, that's only part of the solution. You also want to make sure you have an on-site copy of your data.

Our recommendation: direct the built-in backup utility to store to a local copy on your server which will then be copied to your BCDR device. The intent is to create two identical copies of your data. One that lives in the cloud, and one that lives on-site. That way you can immediately restore your data whether you experience a technical disruption like a hard drive failure, or an office destroying emergency like a natural disaster. In either case, you can be back up and running fast.

The Hidden Truth about SharePoint, Google Drive and Dropbox And How You Can Reduce Your Risk

So far, this report has primarily focused on backing up your server infrastructure, since that is where many companies store their most critical data. However, as businesses become more geographically dispersed and begin moving to a partial work-from-home model, many organizations have made the decision to replace their on-premises server infrastructure with a cloud-hosted model such as SharePoint, Google Drive and Dropbox to manage their file sharing needs.

Since many businesses are already using Office 365 or Google Workspace, it makes sense to take advantage of all of the productivity tools they offer. Why pay to maintain a server if all you really need is a secure way to share, edit, and store your files? It makes total sense.

These tools are growing in adoption and functionality every day. But unfortunately, there is a hidden secret that Google and Microsoft don't advertise. Let's start with Microsoft. SharePoint is widely used for file storage and sharing. But if you or one of your employees accidentally or intentionally deletes a file and you don't realize it for more than 93 days, that data is gone forever. However, even if you *do* realize that the file has been deleted sooner, it's impossible to recover a single file. Instead, you would be forced to restore the ENTIRE SharePoint site. So, let's say a critical file is deleted at 2 pm on Monday afternoon and no one realizes until Wednesday at noon. If you need to restore it, you'll be forced to select the most current backup that contains that file, thereby overwriting any files that have been changed since.

The situation isn't much different using Google Drive. And let me start with one caveat: Google offers a backup product *Vault* with certain Google Workspace subscriptions, but if you are on a Frontline or G Suite Basic plan, that tool is *not* included. If you HAVE Vault, you can configure it so that your data is retained indefinitely. But if your subscription doesn't include Vault, you might want to consider backing this data up separately. If someone on your team deletes a file or folder from Google Drive, and no one realized for 30 days or more, that information is likely gone forever.

Microsoft and Google do maintain secure backups of all your information (emails, files, users, etc.), but this is primarily for their use. In the case of a deletion, chances are that neither company will be particularly accommodating about restoring your data. And even if they can assist, they can't restore individual files, even if they want to.

If you use a file-sharing or file-sync application to store your files and collaborate, make sure you understand their data retention policies. If you don't know what happens when files are deleted, you need to get clarity ASAP.

We recommend that ALL businesses that use file-sharing apps have file-level cloud backup in place. Otherwise, you could experience significant data loss.

What About My Emails? How Do I Protect Those?

As we just explained, Microsoft and Google don't actually "back up" your data in the traditional sense. While they retain your data for a period of time, recovery is difficult and only possible in certain scenarios. Unfortunately, the same thing applies to emails within Microsoft 365 and Google Workspace.

If you, or one of your employees deletes an email, a folder, or even an entire email account, that data is only available for 30 days. But if you terminate an employee (or an employee leaves) and you only realize months later that they deleted critical emails, you are out of luck.

Thankfully, the solutions mentioned above for backing up SharePoint and Google Drive can also back up your Gmail and Exchange. With these solutions, you can recover any individual files or emails that have been deleted – from any point in time.

7 Questions You MUST Have Answers To Before Selecting A Backup For Your Business:

Now that you know where your information resides, what backup options are available, and the pros and cons of each, it's time to start evaluating your current backup to ensure it can meet your needs, should you be forced to recover.

Depending on how you store your data now, some of these questions might not be relevant, but I will clarify that as well.

Here are the **7 questions** you need to answer before selecting a backup for your business:

Q1: Where is our data stored?
Our Answer: This is the FIRST question you should be asking. A lot of businesses assume that all company data is being backed up to the on-premises server or NAS, only to discover that employees regularly save document to their desktops, personal cloud apps like Dropbox, and cloud sharing applications like SharePoint and Google Drive. Your job is to understand EVERY place that data is stored.

Q2: How much downtime can we afford?
Our Answer: While some businesses can afford to be down for a few hours up to a few days with minimal impact on their bottom line, there are many organizations that would be forced to shutter their businesses for good in the same circumstances. You need to know what an hour of downtime costs your business. And while there are direct costs like the work of your IT provider, there are also several other costs that are more difficult to quantify. For example: lost sales, lost productivity, lost opportunities, employee and client

frustration, and negative PR. While some backup solutions may *seem* expensive, you might be surprised to find that an hour of downtime costs far more than the backup.

Q3: Based on the amount of data we have; how long would it take to recover from a hardware failure? (Assuming you have an onsite server or NAS device)
Our Answer: This question is difficult to answer without specific information about your environment. How much data are we talking about? What kind of physical infrastructure do you have (NAS device, on-premises server)? What are your Internet speeds? What Internet speeds does your backup vendor offer? Does your backup vendor "throttle" the speed of restores, or do you get full bandwidth? Does your backup vendor offer the option to send you a hard drive with all of your data to make restoration faster? You need to know how long you should expect to wait in an emergency, so if the backup vendor you choose can't (or won't) figure out your estimated downtime, then we recommend going elsewhere.

Q4: Based on the amount of data we have, how long would it take to recover from a natural disaster, such as a fire, flood, or tornado?
Our Answer: This question isn't relevant if your server is hosted in the cloud by a 3rd party or if it is hosted in a colocation center. This is more for organizations that rely on on-premises infrastructure. If your equipment is hosted by a 3rd party, a natural disaster should have limited impact on your ability to access your systems. Your staff might need instructions on how to access company systems from home, but there is no actual "downtime" to speak of. But if you house your own equipment and it is destroyed, how can you go about getting your data back? Unless you have a Business Continuity solution, you would need to find and purchase new hardware, and then restore your backups onto those devices. So, make sure you know how long it will take to purchase and configure the hardware, restore your data from the cloud, and deploy it in your office. If the timeline is too long, it's worth considering whether a BCDR solution is the right fit for your organization.

Q5: What backups do we currently have? Do these meet our recoverability/up-time objective?
Our Answer: Once you determine where your data is stored and how much downtime you can afford, you will need to assess whether your current backups can meet your recovery objective. If not, it's time to investigate a more robust solution.

Q6: Can a BCDR backup protect me against Ransomware?
Our Answer: The short answer is that a BCDR solution CAN prevent you from experiencing Ransomware. However, it doesn't "protect" your data; that's the responsibility of your various cyber security protections like firewalls, spam filtering, antivirus software, and threat detection tools. That said, a Business Continuity solution WILL allow you to recover data from before the attack. One of the solutions we use (from a company called Datto) can

actually identify WHEN a Ransomware attack occurred, so that you can restore the most recent data from just before the attack. That way, even if your current backups are compromised, you can still safely restore a recent copy of your data.

Q7: How will the backup vendor ensure that my backups are running? How do I know that my backups will be accessible in an emergency?
Our Answer: This depends as much on your IT provider as it does on the backup provider you select. Your Managed Services Provider / IT Support Provider should be monitoring your backups daily for any issues. If there is a problem, it should be addressed immediately. Unfortunately, just because a backup is "running" doesn't mean that it is "recoverable" in an emergency. Any IT Provider worth their salt will test your backups on a regular basis to confirm that they are accessible. At Connectability, we believe that our MOST important duty to our customers is to protect your critical business data. To do so, we conduct "test restores" of our clients backups on a monthly or quarterly basis (depending on your service plan). That way, you can rest easy knowing that your data is there should you need it.

5 Mistakes To Avoid When Choosing A Backup Vendor

1) **Choosing the lowest cost solution.** While cost is obviously an important consideration for every business, it shouldn't be the first thing you consider when choosing a backup for your business. While one solution may seem less expensive, it's important that you consider the costs to your organization if you experience downtime. Can the solution you've chosen meet your recovery objectives? If not, how much downtime will you experience, and how much will it cost you?

2) **Choosing to manage external backups yourself.** Everyone wants to save a few bucks and limit complexity. To that end, we've seen businesses monitor and manage their own backup protection using a series of rotating external hard drives. I cautioned against this earlier in this report, but we see this so often that it bears repeating. External hard drives and thumb drives are NOT a reliable means of backup. Even if your team is disciplined enough to swap drives on a regular basis, and bring them offsite, it is far too easy to drop a hard drive, or spill a drink on it, or even leave it in a hot car by accident. Bottom line: if you value your data, an external hard drive alone is NOT going to give you the redundancy your need. Even assuming that your backups do work, every time you save a backup, you are overwriting previous copies of your data. So, for example, let's say you rotate your drives on a bi-weekly basis. What happens if someone deletes a file and you don't realize for 3 weeks? Unfortunately, you'd be out of luck.

3) **Choosing a provider before understanding the costs of downtime.** When evaluating providers, make sure you understand what an hour of downtime costs you. Not just in terms of the money you lose on missed orders and the costs of recovery, but also the cost of lost productivity, employee and customer frustrations, lost trust, and bad PR. If your employees can't work, how much does that cost you directly? When we work through these calculations with our clients, they're often shocked at how much an hour of downtime REALLY costs their business. If you know how much downtime costs you, and how long it will take to recovery using each solution, you can determine the direct financial impact of choosing one solution over another.

4) **Choosing a provider without considering one or more data sources**. It's obviously a good idea to make sure that your primary data sources are backed up. Whether you use a cloud storage application like SharePoint or Google Drive, or on-premises equipment like a Server or NAS drive, you need to secure that data. But just because you've backed up your main data source, it doesn't mean you're out of the woods yet. Your server data might be backed up, but that doesn't mean your emails are protected. If an employee accidentally (or maliciously) deletes critical email communications and you don't realize, it's possible to lose that information forever. And since every business is different, everyone's backup needs are different. Make sure you consider every possible data source before crossing this off your list.

5) **Choosing a provider without understanding your compliance requirements.** If your business operates in a regulated industry, there are most likely specific compliance requirements that you are legally bound to meet. For example, businesses in Financial Services, Food and Drug production and healthcare must follow stringent data protection guidelines and compliance requirements. For example, you may be required to keep backup data in Canada. You might also be required to retain data for a specific length of time, or even to keep a certain number of revisions of your data before deleting. This depends entirely on your industry, but you will want to know your requirements before choosing a backup tool.

A Final Word…

I hope you have found this guide helpful in shedding some light on what to look for when choosing a provider to back up your company's critical data. As I mentioned in the opening of this report, my purpose in providing this information was to help you make an informed decision and avoid getting burned by the many consumer-grade backup options out there.

If you have any additional comments or questions, we welcome them! Have an idea to make this guide even more helpful? Let us know! And, of course, if you are looking for someone

you can trust to take over the care and maintenance of "all things digital" in your office, we'd love the opportunity to
EARN your business.

Below you will find information on how to request a FREE Backup & Disaster Recovery Assessment. This is, of course, provided for free, with no obligation and no expectations on our part. I want to be clear that this is NOT a bait-and-switch offer or a trick to get you to buy something. My reputation for running an honest and trustworthy business is something I hold very dear. I would never jeopardize that in any way. So why are we offering something like this for free?

Two reasons:

1. We are simply offering this service as a risk-free "get to know us" offer to people we haven't had the pleasure of doing business with. Again, our goal is to allow you to make a more informed and confident decision – and offering this is one way we can help you better evaluate us.
2. This will allow us to determine if we even CAN help you. Obviously, we can't help everyone, and our services might not be a good fit for you. Conducting this Assessment enables us to do a small project for you to help you evaluate whether or not we're the right company for you without risking your money.

Looking forward to your call!

The Team at Connectability,
Phone: 416-966-3306
Web: www.connectability.com

FREE Backup & Disaster Recovery Assessment For All Prospective Clients Who Want To Put Us To The Test!

As a prospective customer, we would like to offer you a FREE Backup & Disaster Recovery Assessment ($697 value). During this assessment we will perform a comprehensive audit of your network to understand where you store company data, identify any gaps in storage or protection, and provide recommendations to fill those gaps.

We will:

- Discuss your recoverability objective so we know how much downtime your business can withstand
- Review your server configuration to understand where data is stored and how it is backed up and protected
- Assess your current backups to ensure they are working correctly

- Conduct a test restore to ensure your data can *truly* be accessed in an emergency, such as a hardware failure or natural disaster
- Assess any other data stores (ie. NAS drives, cloud storage solutions, email, etc.) to confirm they are backed up. If not, we will document any gaps
- Discuss any compliance requirement your organization must meet and review your current infrastructure
- Review your physical environment for environmental issues like flammable materials in your server room, loose or cut cables, dust, water leaks, and extreme heat.

Why Should You Care About This?

Because most businesses can't survive long without their data. We have seen FAR too many experiences where a business is down for days, or even weeks at a time simply because they thought that all of their data was backed up and easily recoverable, only to discover that the backup wasn't working, it can't be restored, or it takes far longer to restore than they thought.

There are numerous checks and updates that should be done on a regular basis to ensure your data is securely stored, backed up effectively, accessible in an emergency, and recoverable in a short period of time.

At the end of this assessment, you will know, with certainty, whether you can get back up and running quickly in an emergency. If not, we will provide customized recommendations for closing any gaps we've identified.

The worst time to test your backups is when you need them. With our FREE Backup & Disaster Recovery Assessment, you will help your organization minimize downtime, while at the same time improving your cybersecurity.

How To Request Your FREE Backup Health Check?

Connecting with us is easy! Call us at: 416-966-3306, email info@connectability.com or go to our website to schedule a meeting. Visit our website at:
https://www.connectability.com/backupassessment/

Just enter your information and someone from our team will be in touch with you as soon as possible to schedule. That's it!

Read On To Hear What Our Clients Have To Say:

"Try Connectability if you want to sleep well at night and not worry about your IT support expenses fluctuating every month."

The biggest benefit of working with Connectability is that we are no longer dependent on the availability of our small in-house IT infrastructure and support team to have a comfortable feeling that our IT is taken care of. Connectability truly works as an in-house employee would in the sense that we don't need to go through an SOW process each time we have an initiative: project work is often undertaken as part of their monthly services. Try Connectability if you want to sleep well at night and not worry about your IT support expenses fluctuating every month. The CEO really cares about client satisfaction and is very approachable.

Michael Issaev,
Chief Technology Officer
Patient News

"Connectability was a great discovery! They're responsive, professional, and…

Always looking for new productivity and cybersecurity tools for their clients. If you're looking for reliable IT support services for your business we highly recommend you give Connectability a call!"

Ari Weinberg,
President
O'Doughs

"Since we've started working with Connectability, they've put my worries about our technology to rest."

I don't have to worry about our security, and I know that if we have issues that our IT staff can't solve, we have someone to turn to. Connectability is the first IT provider we've worked with and all I can say is that they are totally worth it for the peace of mind. They have freed up our IT staff so they can focus on the programming work which supports our clients and operations."

Liz Gayford
Chief Financial Officer
Creative Outdoor Advertising