7 RULES

EVEN THE MOST BASIC

BACKUP & DISASTER RECOVERY

PLAN MUST FOLLOW

INCLUDES A 7-POINT CHECKLIST FOR EVALUATING A SERVICE PROVIDER!

GRIT TECHNOLOGIES

7 RULES EVEN THE MOST BASIC BACKUP & DISASTER RECOVERY PLAN MUST FOLLOW

TABLE OF CONTENTS

Does the average small business really need a managed backup and disaster recovery plan?

That depends on how much money it's willing to lose...

If you do business in an industry regulated by security and privacy legislation, or store transaction details electronically, you're probably already aware of how critical secure and exhaustive backups are. But what about a business with a smaller IT footprint, like a mom-and-pop stationery shop? How essential is a backup and disaster recovery (BDR) plan to its operation?

The first step toward answering that question is defining "disaster." In this eBook, we define "disaster" as any crisis that causes IT downtime and interrupts standard business processes. These events run the gamut from mundane to catastrophic:

- Hazardous weather (floods, hurricanes, etc.)
- Hardware failures (overheated server, damaged desktops, etc.)
- Cyberattacks (ransomware, disk-wiping malware, etc.)
- Human error (deleted files, overwritten data, etc.)

A healthy BDR plan isn't limited to dealing with large-scale company-wide events. Instead, it helps you overcome any IT-related interruption of business operations and limit downtime costs, which usually start in the five-figure range.

A backup and disaster recovery plan is the first and most important step in any IT growth plan

Putting a dollar value on IT downtime

Every company is at risk of an IT disaster. So, the next question is: How much should be spent on prevention? If the cost of your BDR plan is higher than the savings it generates during a downtime event -- that's a disaster in and of itself. The trick to calculating the cost of an IT crisis is breaking down each department hour by hour.

The formula for calculating one hour of downtime is:

For example, if half of our imaginary stationary shop's revenue comes from in-store sales and half comes from people who found its website, one hour of IT-related lost revenue will be sales revenue divided by two (because in-store sales aren't affected). If two employees are processing online orders, lost productivity will be their combined hourly wages.

For recovery costs, you need to estimate how much money it will take to restore the affected systems. Do you work with an IT contractor? Recovery costs will be his or her hourly fee, plus the cost of whatever IT hardware and software is needed to get things working again. Think about reputational costs in terms of how many sales leads would notice a downtime event. If your website was down for two full days, how many leads would decide to cross your team off their list and how much lost revenue would that work out to be per hour?

Putting a dollar value on IT downtime

Calculate how much one hour of downtime will cost:

	+		+		+		=	sum ( )

Any of the disasters we listed on Page 1 will cause at least eight hours of downtime, probably closer to 24. Without the right support, even the "tiniest" disaster is going to cost you north of $10,000.

But we have good news! With the decreasing cost of cloud technology and the increasing prevalence of SMB-focused IT providers, you can reduce the cost of every variable in our downtime equation. All you need is a trustworthy managed IT services provider.

Your BDR plan will save your bacon only if it follows current best practices

How to judge a BDR plan as an IT novice

There are seven non-negotiables

RULE #1 Every file gets the 3-2-1 treatment

The first and most important rule of data backup has been around since the era of floppy disks. It goes like this: Every file your business creates should have at least **3 copies**, stored on at least **2 different types of media**, with at least **1 copy located somewhere other than your office**.

If you need to create and save an invoice, following the 3-2-1 rule might look like this:

- One copy is stored on an accountant's desktop computer
- One copy is stored on a removable drive (e.g., USB drive, hard drive, etc.)
- One copy is stored on an off-site cloud drive

In the case of an office fire, only two of the three copies are at risk of being destroyed. Similarly, if the network and the accountant's computer crashed, the invoice is still accessible from the removable drive.

RULE #2 Everyone has a copy of the BDR handbook -- even the janitor

It's common for people involved in emergency situations to be so shell-shocked that they struggle to communicate and remember basic information. That's why your BDR plan must include a document that provides clear instructions on how employees should respond to a disaster.

We recommend you store this document in the cloud and ask employees to bookmark it on their mobile devices. This way, if our stationary shop were blindsided by a ransomware infection, employees could *turn to your BDR handbook for whom to call and exactly what to say*.

RULE #3 Your plan can scale up overnight

Don't forget to factor in your long-term needs when selecting a BDR plan. It would be pretty awful if you spent a month and a couple thousand dollars installing the best backup solution available only to outgrow it a year later.

To avoid this, clarify storage and functionality limitations with vendors and IT providers before finalizing the deal, and ask the following questions:

- Will I ever need to archive old documents to make more room?
- If I need more space, how long will it take to upgrade my solution?
- What is the most storage I could receive with this solution?

Cloud backup solutions should be able to accommodate anything a small- or medium-sized business would ever need, but you need to confirm that the technicians supporting your plan are committed to quick turnarounds and reliable service. For example, we guarantee disaster response times in our service level agreements.

RULE #4 Security is as important as recovery

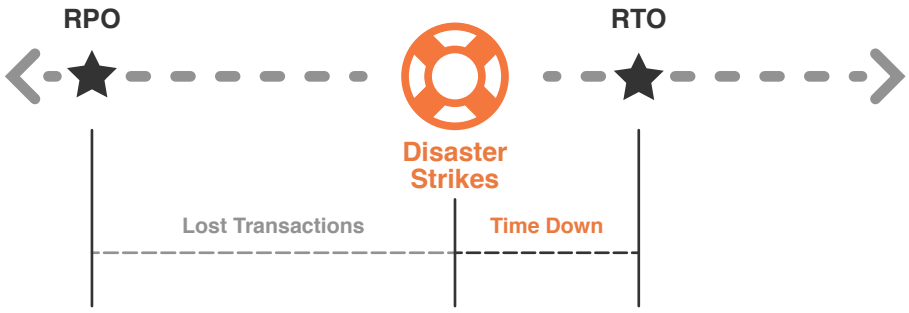
Cybersecurity must be a top priority in any BDR plan. If you are backing up data to the cloud, it should be protected by cutting-edge intrusion prevention tools, firewalls, and advanced encryption systems. We usually integrate our clients' backup plans with IT support so everything can be monitored together.

Ransomware infections can spread to your cloud backups if files are automatically synced to the cloud. So before you finalize your backup plan, make sure your provider offers 24/7 monitoring to stop the spread of malware infections.

RULE #5 There's an RPO that saves you dough

On-site and cloud storage solutions are getting cheaper every day, but not to the point where it always makes sense to create second-to-second backups. You might be able to save some money by scaling back to daily or even weekly backups.

To do this, your BDR plan needs to contain a **Recovery Point Objective (RPO)**. Measured in hours, your RPO will govern how recent your backups must be to avoid staggering losses. Could you survive losing all your data created in the past four hours? What about the past 48 hours? These business continuity needs should be clearly define and regularly updated.



RULE #6 Your plan is good to go when it has an RTO

Even if our imaginary mom-and-pop shop could justify creating backups in real time, that isn't the only objective that needs to be defined for a BDR plan to succeed. Business owners also need to define how much time it takes to restore data, regardless of how recent their backups are.

Your **Recovery Time Objective (RTO)** will be how much downtime you can handle, which means RTO is placed on the right hand side of the disaster timeline. This is where personalized IT support really shines. By creating our clients a backup plan from scratch, we ensure RTOs are measured in minutes and downtime is always within our clients' tolerances.

RULE #7

Everything gets tested, over and over again

Backup software vendor StorageCraft released a survey that says 33% of businesses with a BDR plan were still unprepared to handle a disaster. That's because the vast majority of small businesses create a plan, but never update or stress-test it.

Even annual reviews of your plan may not be enough. Just think of all the front-page stories about ransomware attacks written in the past 12 months. Testing a BDR plan is too technical and difficult for IT amateurs, which means regular checkups and reports from a professional are an absolute necessity in any managed BDR plan.

*These seven rules are just a baseline; the most important thing is that **your plan** reflects **your needs***

Checklist: Managed backups plans

Choosing the right BDR plan can be difficult, so we've put together a checklist to help you cross subpar providers off the list. In addition to the 24/7 technical support and uptime guarantees that come with most managed IT services plans, every BDR plan should have:

- [ ] Files stored in accordance with the 3-2-1 rule
- [ ] A disaster recovery handbook that helps employees relay the right information to the right people
- [ ] Clearly defined storage limits and procedures for upgrading your plan
- [ ] Security tools such as threat prevention software, firewalls, ransomware protection, and data encryption systems
- [ ] An RPO that is based on your business continuity needs
- [ ] An RTO that is based on your downtime tolerance
- [ ] Routine testing and reporting features

The best thing about this checklist is that it can also be used to audit existing plans. Every three months, print it out and make sure you still have recent and accurate information for each of the seven points above.

Once your plan has everything on this list, ask your provider, "Alright, how will you make my BDR plan better?"

7 RULES
EVEN THE MOST BASIC
BACKUP & DISASTER RECOVERY
PLAN MUST FOLLOW

The GRIT Technologies difference

There are seven non-negotiables

As a well-established managed IT services provider, we help our clients design and implement business continuity strategies that measure downtime in minutes. With one of our free consultations, we'll conduct an exhaustive IT risk assessment and outline the RTOs, RPOs, and BDR investments that will keep you in the black whether you're hit by a hurricane or hardware failure.

We'll store copies of your applications and data in a secure, failure-free cloud data center so your on-premises backups are never the only option. And our solutions are completely scalable, which means you can back up anything from a single file to an entire server.

All this and more is available for a low monthly subscription fee.

Want to know what we think your BDR plan should include?

Schedule your free consultation today!

Phone: Detroit Area 586.286.8324 / Grand Rapids Area 616.251.1117

Email: info@grittechs.com

GRIT TECHNOLOGIES

www.grittechs.com