IS YOUR BUSINESS READY FOR THE WORST?

WHATEVER FORM THEY TAKE,

DISASTERS WILL ALWAYS HAPPEN

Like it or not, the unexpected will always happen and you need to get ready for it.

Think about how much time you spend planning. You assess risks and you prepare for the worst. You pay for di˜erent types of insurance: medical, life , car, debt, etc. just to **make sure you're able to get through any unexpected situation. So, it only makes sense that you'd do the same thing for your business.**

Unfortunately, when it comes to planning for disaster recovery (DR), small business owners tend to postpone projects and not take action. The reasons di˜er , but keep this in mind: when disaster strikes, it can take a long time to resume your normal activities.

52% of small business owners surveyed said it would take at least three months to recover from a disaster. °

75% The survey also revealed that more than 75 percent don't have a disaster plan. °

° Nationwide Insurance, US Survey 2015

HOW MUCH
DOES A DISASTER REALLY COST A COMPANY?

The way a business handles disaster will determine its future. Ensuring the continuity of your company means you have to plan well upfront. A disaster recovery strategy cannot be built in a hurry, under pressure and without an assessment. To better understand why you should plan for disaster recovery, you have to know how data loss will a˜ect your business.

Here's what to expect when a company fails to keep its clients satisfied because of a disaster.

$35,730

Can you afford that kind of loss?

Small data breaches -- those with fewer than 100 files lost – can cost between $18,120 and $35,730. ¸

YOUR BUSINESS'S REPUTATION WILL TAKE A NOSEDIVE

You certainly know the power of word-of-mouth, especially when you have customers or partners promoting your services. It works the same way when you have detractors. News travels fast and your company's reputation can be badly harmed because you weren't able to deliver services as promised. When disaster strikes, customers may be supportive and patient for a few hours, especially if you've put everything in place in advance so you can provide them with minimal services. But in this era of social media you can't be sure your unhappy customers will keep the news to themselves.

POTENTIAL FUTURE CLIENTS WILL BE AFRAID TO DO BUSINESS WITH YOU

We all have big plans for our businesses and we see globalization and the Internet as opportunities to reach more customers. But there are also situations where you'd love to have the "right to be forgotten" online. Unfortunately, posts from unhappy clients may not be deleted after you've fixed their issue. And if you tend to delete negative comments on your own social media posts, you might end up with more negative press than sympathy. You have to see your online identity and reputation as a business card for many of your future clients.

¸ Verizon, 2015 Data Breach Investigations Report

UNSATISFIED CUSTOMERS WILL LEAVE YOU

It's not hard to understand. Today's customers aren't patient because they don't have to be. Your customers rely on you for specific products and services. When they can't have what they're paying for right away, they'll leave you for a better o˜er down the road. This means your company will tak e a big hit in revenue immediately. And it can become a long-term problem because these clients might never come back to you. The way you handle disasters can result in a big churn for your company!

YOUR EMPLOYEES WILL JUMP SHIP

Your employees will be unhappy because they'll be under pressure to satisfy disgruntled clients. They can feel helpless if their usual tools (emails, phones, software, etc.) are not available. This can also a˜ect their self-esteem. If your employees can't work because of a disaster that you didn't prepare for, they won't like it. Their salary and lifestyle will be at stake. Don't expect them to thank you for your negligence!

YOU WILL HAVE TO FIRE STAFF

As we mentioned earlier, client churn might cause your business to lose revenue. Consequently, you might to decrease salaries -- or worse – impose layo˜s. This means firing people who 've been loyal to you for many years. It's very easy to go from running a prosperous company to filing for bankruptcy. It's in your interest to avoid this situation!

ASK YOURSELF THE RIGHT QUESTIONS
ABOUT THREATS TO YOUR BUSINESS

Every company owner should ask themselves the following questions:

- [ ] **Which tools do we use every day?**
- [ ] **What kind of incident could harm our daily operations?**
- [ ] **Are we prepared if this incident occurs?**
- [ ] **How high is the probability that this incident could occur?**
- [ ] **What would be the impact of the incident on our company?**
- [ ] **Would we be able to continue to deliver services to our customers?**
- [ ] **How long could we continue to run in this situation?**
- [ ] **What is the minimal level of service I need to keep my clients satisfied?**
- [ ] **What would we need to do to get back to work?**
- [ ] **How would my clients react if my employees couldn't respond to their needs?**
- [ ] **Would my clients leave if this type of incident occurs?**
- [ ] **Would the company survive after an incident like this?**

Let's face it. Your company could be hit by a disaster one day and you should be prepared. Companies that have a disaster recovery plan spend less on recovery than those that don't. You shouldn't wait for a disaster to interrupt your activities.

84%

For 84% of SMBs, several days of IT downtime would result in moderate to catastrophic costs and loss. [1]

[1] Zetta, 2016 SMB R ecovery Readiness Study

SURVEY YOUR COMPANY:

ASSESS THE RISKS AND ANALYZE THEIR IMPACT

BUILD A REALISTIC LIST OF SITUATIONS THAT COULD STOP OR SLOW DOWN YOUR PRODUCTIVITY

Look around you and think about all the potential threats to your company's wellbeing. Imagine anything that could happen in the company o ces and outside , including at a provider's premises. The disaster could a ect equipment, buildings, an employee, a contractor or a service.

Here are a few examples of potential threats to your company's activities:

- Power outages
- Phone service outages
- Internet outages
- Local network outages
- Cyber attacks
- Computer failures
- Machinery failures
- Injuries
- Fires
- Drought
- Floods
- Low water levels
- Explosions
- Chemical leaks
- Road closures
- Earthquakes
- Storms
- Ice storms
- Hurricanes
- Tornadoes
- Employee strikes
- Plane crash
- Wars
- Bombings
- Fraud
- Lawsuit

Don't neglect anything. Take the case of a single employee who does the accounting for your company. If he or she were unavailable, even if the accounting software is up and running, no service related to accounting would be delivered to your clients. Is this a threat to your company? Yes, it is!

Remember, at this level, your task is not to think about any solutions, but just list the potential issues.

YOUR TASK:

BUILD YOUR OWN LIST OF POTENTIAL THREATS TO YOUR COMPANY

43% of companies experiencing disasters never reopen and 29% close within two years. ˇ

ˇ RSM US LLP, 2015

CLASSIFY EACH THREAT
IN YOUR LIST BASED ON THE DAMAGE IT COULD CAUSE

It's very important to determine the potential impact each threat can have on your business.
Let's say you have one computer used to display information in your oˆce lobby for visitors and clients. If this computer crashes, there's no real impact on the company because no oˆce activity has been impaired as a result. People seated in the lobby can still read magazines or company flyers while waiting for their appointments. The receptionist can provide information to guests if required.

But if the same thing happens and the a˜ected computer is the one that hosts the company' s online calendar, then you're in trouble. Your receptionist won't be able to have the appointment list ready in the morning. When a client arrives, she won't be able to tell who the person is supposed to meet. If a client calls to get an appointment, it will be impossible to confirm any schedule because the receptionist won't know who is free and when.

So, you see, listing a simple threat like "Desktop failure" won't be that helpful. Listing "Calendar server failure" makes more sense. This little precision will make a big di˜erence in your preparations.

So, how do you rank your threats? You need to use two metrics: probability and severity.

PROBABILITY

Probability is about answering a simple question: how likely is the event to happen?
You can rank this question from 0 to 5. Here's an example:

0 - Very low **1 - Low** **2 - Medium** **3 - High** **4 - Very high** **5 - Inevitable**

SEVERITY

A simple ranking can help. Here's an example of how to rank severity:

0 - 0 to 1 employees cannot work, with no impact on the company's overall activities.
1 - At least one employee cannot work, but the impact is limited to one small team. All services remain available to the clients.
2 - Multiple teams within the same department cannot work, but all services remain available to clients.
3 - Multiple teams within the same department cannot work and only basic services remain available to the clients.
4 - All company employees cannot work and no services are available to the clients. However, the situation is temporary.
5 - No employee can work. No services can be delivered. The company will be down for a while.

SCORE EACH THREAT

To get a consolidated list of your threats and rankings, you need to do the following. **For each threat, multiply the probability and the severity rankings. This will give you scores from 0 to 25.**

0 - 7 | Low **8 - 16 | Medium** **17 - 25 | High**

YOUR TASK:
ASSESS AND SCORE EACH THREAT IN YOUR LIST

ESTABLISH YOUR PRIORITIES

If you've followed all these steps, you should have a precise list of all threats to your company and their scores. You can use this as a business impact assessment (BIA).

The threats with the highest scores (17 to 25) become your top priorities for disaster recovery planning.

Note: This method will work for all your company services. In the following chapters, we will only focus on the IT services directly a˜ected by the threats.

Remember, disaster prevention is not the same as disaster recovery. Disaster prevention only mitigates the risk of downtime. **Disaster recovery makes sure that in case of downtime, you can get your IT services back online quickly.**

YOUR TASK:

ESTABLISH YOUR DISASTER RECOVERY TOP PRIORITIES

PLAN YOUR DISASTER RECOVERY

Note: Don't feel like you can do it yourself? Talk to a Managed Services Provider (MSP). MSPs have all the tools and the knowledge to advise you.

WHERE IS YOUR IT?

Companies will have di˜erent strategies to ensure the availability of their IT services. Some will build a redundant environment so there's no single point of failure. For example, instead of having a single server with an application and its database, they would have two dedicated servers for an application which share the load, plus two di˜erent servers for the database that replicate data continuously .

It's less likely that a small business would have the budget to a˜ord such a solution, so it' s not unusual to see a single server running email, applications and databases for the whole company. And the server will be hosted at the oˆce , sometimes in a location that is not physically protected. If that computer crashes, then the whole company stops.

This is why many small businesses have started considering cloud services to host their workload.

64% of SMBs are already using cloud-based software and the average number of applications in use is 3. [5]

Despite the global momentum to adopt the public cloud, not every SMB is ready for it. There are di˜erent reasons for this:

- Some SMBs are using legacy applications that cannot be easily moved to the cloud
- Others have regulatory constraints that force them to keep applications on-premises
- A few SMBs are reluctant to migrate an application to the cloud because of the costs involved

In fact, some business owners don't realize that they can lower the total cost of ownership (TCO) of a solution by running it in the cloud. TCO refers to the estimate of all direct and indirect costs associated with an asset or acquisition over its entire life cycle.

[5] BCSG, 2016, The small business revolution: trends in SMB cloud adoption,

BENEFITS OF THE CLOUD

If you still wonder why you should adopt the cloud, here are a few important reasons:

TECHNOLOGY INNOVATION

Whether they are well-established IT firms or new start-ups hitting the market, most vendors are now o˜ering their services in the cloud model. All components of business IT are available “as-a-service” and delivered through the Internet:

- Infrastructure (virtual servers and networks)
- Software (applications and databases)
- Platforms (development tools and more)
- Communication (voice over IP services like telephone and fax)
- Anything as a service

The providers will update their environment regularly (at no cost to you), so you can be sure you’re working with the best IT tools.

If a company wants to benefit from the last innovation, it’s all in the cloud!

TECHNICAL EXPERTISE

For small businesses, hiring highly-skilled IT professionals is sometimes out of reach. They need specific IT services but cannot a˜ord to pay someone to tak e care of them. Thanks to the cloud, all businesses can benefit from the level of service they want without having to hire an expert at all. Cloud o˜ers include managed services for maintenance and support, freeing the clients from any time-consuming task.

The cloud will also help you enhance your company’s quality of service. The provider’s service level agreements guarantee you’ll be able to access your services 24/7. In other words, they’ll always be available. If any maintenance is scheduled, it will be done outside usual working hours and you’ll be notified.

Finally, if you want better security for your business data, adopting the cloud is your best option. Top- rate providers are subject to high standards that oblige them to follow very strict rules. If you use it correctly, the cloud guarantees both privacy and security.

Thanks to the cloud, you can focus on generating revenue for your business. You won’t have to worry about maintaining your IT.

FLEXIBILITY AND SCALABILITY

Cloud services are easier to integrate in a budget because of the flexibility and scalability they o˜er.

Cloud services are operational expenditures rather than capital expenditures. They do not require an upfront investment. If you want to start using a cloud product today, you can just sign up and activate it right away. You’ll pay for the service consumed at the end of the billing cycle (usually monthly).

You can scale your cloud services up or down as needed. This is perfect if your usage is not linear and you require more IT resources some weeks than others. This means you can choose the level of performance you need for your application or server. Your bills will always match your actual consumption.

With cloud services, your bills reflect your needs.

HOW TO MAKE SURE YOU GET BACK ON YOUR FEET

As we've seen earlier, when a company is hit by a disaster, it can a˜ect its incapacity to serve clients. Whether the incapacity is partial or total, **your objective should be to restore services as soon as possible.**

Getting your IT services back to normal can mean di˜erent things depending on the situation. Here are a few examples:

- Restart a computer
- Restart one or more applications/databases on the computer
- Re-establish network connectivity
- Reconnect to the Internet
- Reinstall a computer
- Restart activities from another place or another server
- Remotely wipe data on a stolen or lost mobile device
- Get a fresh copy of data to replace corrupted files
- Move your computers to a safer place
- Build a new oˆce
- Rent a new oˆce

Not all situations can be solved within a few minutes or hours. Some might require days, weeks or even months. But in the meantime, you need to maintain your services as much as possible. **Whether you're running your services from the cloud or from local servers:**

1. **You may rely on a temporary solution** before you totally restore your services. But this solution needs to deliver a relatively normal level of service, which means **your data must be up to date**.

2. To restore your services completely, you need to get back to a state where your services are fully operational. If this means you have to reinstall computers, **you need reliable copies of your files and databases to rebuild everything.**

In all cases, you need to make sure you have a usable copy of the last data processed before an incident occurred. The best way to get this is with backup.

DO YOU KNOW ABOUT BACKUP?

All businesses are dependent on technology, but each of them manages its IT di˜erently . However, there's a common element when it comes to preparing for a disaster: backup.

WHAT IS BACKUP?

Backup refers to the copying and archiving of computer data so it may be used to restore the original version after a data loss event. Data backup is vital for maintaining business continuity.

A company can back up files, databases or full computer systems. The data can be backed up continuously or following a schedule (overnight for example).

E.g.: One can decide to do a full backup of the receptionist's desktop. It will copy the operating system files, user profiles, all documents, browser favorites, application configurations... everything on the hard drive(s).

HOW TO BACK UP?

Backing up data usually requires:

- Some backup software installed on a server
- Backup "agents" (also software) installed on the computers containing the original data
- Storage to keep the data copies

Some small businesses will use Dropbox, Google Drive or OneDrive to sync work files to the cloud, and they will consider this as their backup. **Let's be clear, these file sync and share products cannot be considered a reliable backup solution.**

WHAT WILL BACKUP SOFTWARE HELP YOU DO?

Backup software protects critical data and enables its recovery within a business's recovery time objective (RTO). RTO is the maximum tolerable length of time that a computer, system, network, or application can be down after a failure or disaster occurs.

There are specific solutions made for data backup and archiving. **They will not only help you restore single files but also make it possible to completely rebuild your IT environment in case it crashes.**

Not all backup solutions are capable of completely restoring a computer system or other complex system configurations. Therefore, **business owners should be very careful in selecting the right backup solution that responds to their company's needs.**

E.g.: If the receptionist's computer crashes, a new desktop can be installed and the full backup of the faulty desktop will be restored on the new one. The receptionist will then have access to the same environment as if nothing happened.

WHAT TYPE OF STORAGE IS USED FOR BACKUP?

Cloud Storage
The trendiest solution is cloud storage. It's not just trendy because of the buzz surrounding it. It's trendy because of the benefits. We told you about those benefits earlier in this document.

Hard Drives
Local hard drives can be used for backup, but because they are not portable media, they are not a fully reliable solution. For safety, your backups need to be stored in a di˜erent place than the original data. L ocal storage won't help you achieve that.

Tapes
Tape-based backup systems have been in use for a long time. Tape is magnetic media that can be read or written through a drive or a library. It's the preferred method of long-term storage and it's portable.

Despite the low cost and portability of tape, fewer businesses are choosing it because of the total cost of ownership (TCO). Tape requires manipulation because the media must be loaded to a drive to read or write data, and moved to other premises for safety. This means a resource should be assigned to the task, which adds costs to managing the solution.

Note: Some small businesses have been using floppy disks, CDs or DVDs to save their data, at the expense of security and reliability. Optical media should never be used to store business data in the long term. Floppy disks are obsolete.

TESTING BACKUPS IS VERY IMPORTANT

Recovery is the most important aspect of a backup solution. If you can back up easily, but restoring is fastidious or does not work, then your solution is useless.

Not only that, even if your backup solution is adapted to your needs, you should always test and document your disaster recovery process. You cannot wait for the disaster to happen to ensure your plan works!

A recent survey[6] revealed to which extent SMBs fail to monitor and proof their disaster recovery solution:
- 33% reported that they rarely test their DR plan
- 62% only test their DR plan once a year or less

Testing backups will help optimize your recovery point objective (RPO). RPO is the age of files that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down because of a hardware, program, or communications failure.

E.g.: By testing your restore process, you can determine that it would take three hours to restore the receptionist's desktop.

Note: Do you feel lost in the process? Talk to a Managed Services Provider (MSP). MSPs have all the tools and knowledge to support you.

[6] Zetta, 2016 SMB Recovery Readiness Study

WHAT'S THE BEST
BACKUP SOLUTION FOR AN SMB?

All businesses have to prepare themselves for disasters. While the impacts of a disaster can di˜er from one company to another, it's important for decision makers to develop a disaster recover strategy adapted to their business size and model.

The concepts of business continuity and disaster recovery (BCDR) may seem complicated to the small business owner. But, remember this. Information technology is the force behind a lot of modern companies and decisions makers will have to pay more attention to business risk assessment and disaster recovery planning. They should have a basic understanding of BCDR.

Implementing a backup solution is mandatory for any business.

Statistics[7] show that **34% of SMB buyers have adopted cloud-based business continuity and disaster recovery**. Here's why:

- Cloud-based solutions will improve data protection and business continuity
- They improve the overall reliability of IT systems
- They help save costs by reducing capital expenses and operational expenses

The perfect strategy combines local backup and cloud backup to optimize the recovery time and cover most scenarios. This is called hybrid backup.

[7] Intronis, 2013 State of the Cloud Backup