Disasters happen.
Is your business ready?

Guidance for preparing your business to withstand the unexpected

Table of Contents

executive summary

We've all heard the saying "an ounce of prevention is worth a pound of cure," but how many of us have really taken this adage to heart when it comes to preparing our businesses for possible disasters?

It's easy to brush this task aside when more pressing, immediate business demands clamor for our attention, but the fact is that disasters do happen and when they occur, businesses suffer.

The U.S. Department of Labor estimates more than 40 percent of businesses never reopen following a disaster and, of the remaining companies, at least 25 percent will close in two years. What's more, with fewer resources than larger corporations, small and medium-sized businesses (SMBs) have a harder time recovering from virtual and physical disasters than their larger counterparts and are at a greater risk for not rebounding after catastrophe strikes.

44%

believe IT downtime can damage staff morale, and 35% report it can harm customer loyalty

The U.S. Department of Labor estimates more than 40 percent of businesses never reopen following a disaster. Of the remaining companies, at least 25 percent will close within two years.

executive summary

Dramatic occurrences like hurricanes and tornados might come to mind when you ponder disaster preparedness. If your business isn't in a hot spot for either of these weather events, you might consider yourself safe from most disasters. Yet, it is still prudent to prepare for disaster, because other occurrences such as fires and floods, as well as virtual crises brought on by cybercrime or network failures, are liable to take place anywhere businesses exist.

> By developing a disaster preparedness plan and implementing technologies that support business continuity, SMBs can give themselves solid footing and a strong defense in the wake of disaster. Yes, doing so requires effort and investment, but when faced with the reality that your business might not make it through a disaster, is it really something you can afford to delay or neglect altogether.

66%

of companies do not have a disaster recovery strategy in place

What will you learn

This guide will help you prepare your business to withstand the impacts of disaster and will also help you understand:

- Why there are different precautions to take for physical and virtual disasters
- How to properly protect your business and alleviate the consequences of disasters
- How to differentiate between disaster recovery and disaster preparedness
- How to begin your own disaster preparedness plan

Establishing your preparation plan: Your virtual and physical “GO Bag”

Every business suffers an average of 10 hours of downtime per year, during which time employees are only able to work at 63 percent of their usual productivity.

You probably didn’t hesitate to develop a business plan when starting your company to ensure for the growth of your business. Similarly, preparing your business for possible disaster demands not just an awareness of the potential threats and measures for protection, but an actual plan that dictates how your business will respond to disaster.

When developing a preparation plan, first determine the potential disasters that could affect your business, keeping in mind that, while some disasters are physical (i.e. floods, tornados, etc.), others can be virtual (i.e. network shutdowns, cybercrime, etc.). Referring to the quiz later in this guide might help bring to mind terms and concepts integral to your plan.

50%

of organizations revealed that IT outages can damage a company’s reputation

You also might want to think through how a physical disaster could impact your market. Some SMBs may find that they need greater agility in terms of products and services provided. For instance, if your business provides lawn service but doesn't assist in tree removal, perhaps it's wise to consider expanding your offerings to meet market demands for storm recovery. Consider if you run a small hardware store but don't sell generators, you might be missing out on a major business opportunity should widespread power outages occur in your region. Or if you have employees who would be unable to reach the office if a natural disaster strikes, consider how productivity would continue if they are outfitted with telework capabilities. Additionally, you should ask yourself if your business' current technology infrastructure can handle potential market fluctuations.

To assist you in the development of your plan, following are some tips and guidance pertaining to two different, but equally important, areas of consideration related to disaster preparedness and disaster recovery – your technology and your business itself. It's important to realize that in many cases, having the right measures in place can help your business avoid disaster in the first place, while other tactics will aid you in getting your business up and running again if disaster strikes.

technology strategy

Cloud-based software for storage and more – Explore cloud-based software solutions designed for SMBs. Cloud-based software enables you to store information in a secure, offsite location and access it anywhere you have an Internet connection. Cost-effective for SMBs, cloud-based software often comes with enterprise-class capabilities, making it a wise investment regardless of whether or not your business encounters disaster.

Online backup options – If you don't store all of your data in the cloud, consider investing in an online backup solution that will safeguard all important data stored on your hard drive and make it easily accessible in the event of disaster. Also, if you and your workers store critical data on mobile devices, make sure that data also is protected by your online backup solution.

Keep your technology updated – Maintaining updated technology might prevent a virtual disaster from ever happening in the first place, since updates usually provide security patches and new protective features. Install updates whenever prompted to do so; or, adjust your PC's setting to install updates automatically.

Hard drive replications – If you can't or don't wish to invest in an online backup solution, regularly replicate your hard drive (ideally on a weekly basis), using a detached disk drive. However, keep in mind that in order to make this method fail proof, you'll need to remove the disk drive from the premises each night, in the event that a physical disaster occurs and you aren't able to retrieve it in time.

Encryption matters – If your operating system enables you to encrypt files and folders, by all means take advantage of this feature. Encryption makes data indecipherable to unauthorized users and can help prevent virtual disasters should corporate laptops or other computing devices get lost or stolen.

Map your environment – Be sure you or someone within your company has an understanding of all the important systems in your network environment. If you don't have a network, still take the time to identify all of your critical systems. Determine how long, if at all, those systems can be down during a rebuild in order to ensure you can still operate and maintain customers.

Pull out your policies – Though reading through all the fine print can be overwhelming, it's important that you thoroughly understand your insurance plans and policies. What physical disasters are covered? What forms or filings need to be complete after a disaster strikes?

Communicating with employees – If you're a small business with a few dedicated employees, they will be looking to you for direct guidance and encouragement during disaster. They also need to know ahead of time what to do in the event of emergency. For SMBs that don't have HR resources, internal communications around the disaster should come from the business owners, as well as any guidance you wish to communicate in advance of any potential disasters.

DISASTER PREPAREDNESS

Communicating with external audiences – In addition to providing employees with guidance, you'll also need to communicate with your external audiences, who likely will be expecting to hear from you. Make a list of all potential audiences that could be impacted by a disaster to have on-hand if and when the time comes to communicate. For instance, do you have suppliers or vendors who may be planning deliveries? What about people expecting payments or deliveries/services from your business? What do customers and clients need to know about how the disaster impacted your business? If a data breach of sensitive customer information occurred, planning an alert ahead of time can prevent customers from hearing about it through third parties and not directly from you.

Communication methods – Determine the method of internal and external communications. Will you individually notify people via email, phone or the mail? Or will you post information on your website, social network sites or corporate blog?

Money management – Even during a disaster, businesses need to pay their bills, make payroll and pay suppliers. Be sure you know what all of these accounts are and have contact info for all of these parties, in addition to ensuring your financial management system is backed up properly.

disaster readiness quiz

Microsoft

To find out just how prepared you already are, or aren't, for a possible disaster, here's a brief quiz that will help you assess your readiness.

True	False	Don't know	
○	○	○	*My office has an emergency contingency plan in place for physical disasters.*
○	○	○	*IT is the only department responsible for disaster preparedness within my organization.*
○	○	○	*I keep my employees updated on the most current security threats and provide guidance on what to look for.*
○	○	○	*My business operations require a 24/7/365 model that involves constant uptime.*
○	○	○	*My organization houses onsite data that is critical to business operations.*
○	○	○	*My organization and its departments are tightly organized and can coordinate effectively in the event of a catastrophic system failure or disaster.*
○	○	○	*If my business location were struck by a disaster, it could re-establish operations seamlessly or at a minimum within hours or days.*
○	○	○	*IT systems such as email, document storage, telephone PBX, etc. are essential components of doing business.*
○	○	○	*My datacenter can guarantee a 99.95% uptime.*
○	○	○	*My datacenter has an offsite disaster recovery location established and configured.*
○	○	○	*My organization needs a partner that can integrate my systems to mitigate disaster risk and ensure availability of systems and resources.*
○	○	○	*Critical IT systems and data are backed on an hourly and/or daily basis.*
○	○	○	*In the event of system/server failure or disaster, data can be restored quickly and effectively.*

answers

If you responded "yes" to nine or more questions, you are on the right track to prepare your business in the event of a disaster. New developments in technology described in this eGuide offer you additional tactics to consider.

If you had more familiarity with the first half of the questions, you may have a solid business continuity plan in place, but should investigate the types of technology implementation that can make those current plans more effective and efficient. Conversely, if the second half of the questions were easier to answer, you've set in place technology preparations to mitigate disaster consequences, but may also want to consider some business initiatives to explore.

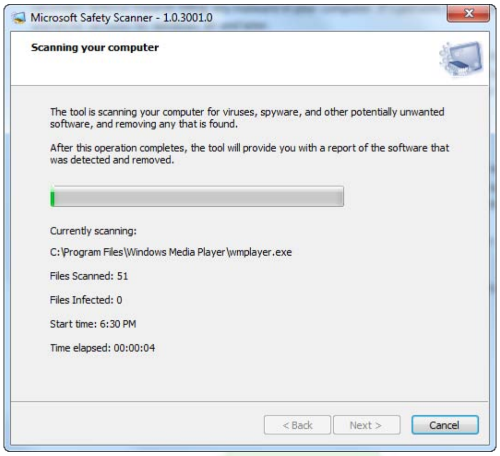
If a majority of your answers were "I don't know," do not panic. This eGuide will provide advice and steps to arm your business in the face of disasters.

Technology tools useful for disaster preparedness and recovery

As mentioned earlier, having the right technology in place can help prepare your business to avoid disaster and/or recover more swiftly from any catastrophes that might occur. The following is a list of technology tools to consider implementing, keeping in mind that many of these tools have significant business benefits that extend even beyond the area of disaster preparedness and recovery:

Free PC Scan from Microsoft

The Microsoft Safety Scanner is a free, downloadable security tool that provides on-demand scanning and helps remove viruses, spyware, and other malicious software from your PCs. It works with your existing antivirus software.



Microsoft Safety Scanner - 1.0.3001.0

Scanning your computer

The tool is scanning your computer for viruses, spyware, and other potentially unwanted software, and removing any that is found.

After this operation completes, the tool will provide you with a report of the software that was detected and removed.

Currently scanning:

C:\Program Files\Windows Media Player\wmplayer.exe

Files Scanned: 51

Files Infected: 0

Start time: 6:30 PM

Time elapsed: 00:00:04

Why is this important?

Your computers could be at risk and you may not even realize it. Many computer users unwittingly download or open files or emails that contain harmful viruses or spyware.

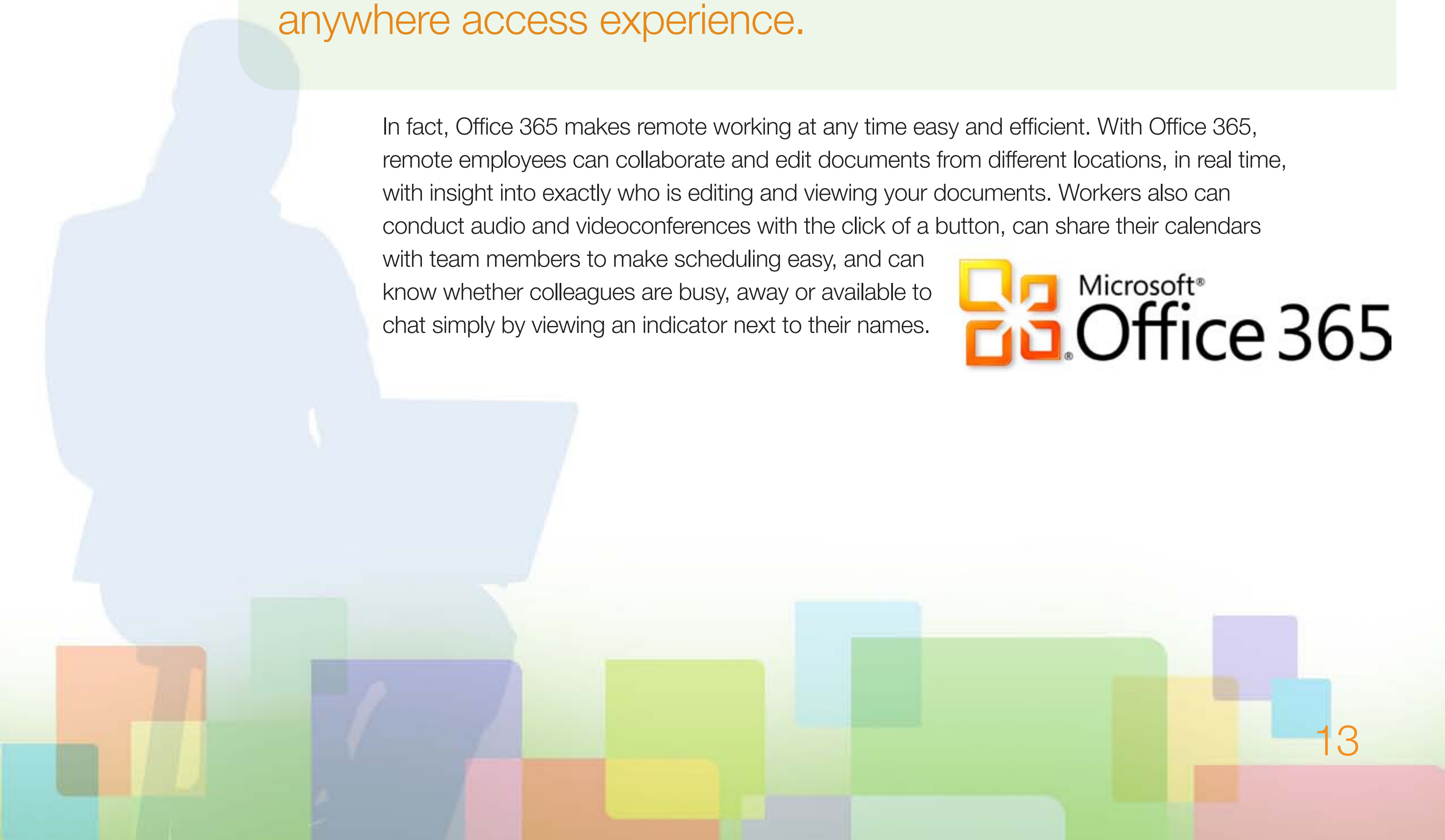
Office 365

Microsoft Office 365 for professionals and small businesses is a cloud-based subscription service that lets users access email, important documents, contacts and calendars from virtually anywhere on almost any device.

Why is this important?

Priced affordably for SMBs, Microsoft Office 365 provides business benefits beyond preparing your business for a disaster. With Office 365, your email, documents, contacts and more are accessible virtually anytime, anywhere from any device. If a natural disaster impacts your physical office location, you will be able to continue conducting many aspects of your business operations from any location, since Office 365 enables employees to be productive and collaborate with the most consistent and secure anywhere access experience.

In fact, Office 365 makes remote working at any time easy and efficient. With Office 365, remote employees can collaborate and edit documents from different locations, in real time, with insight into exactly who is editing and viewing your documents. Workers also can conduct audio and videoconferences with the click of a button, can share their calendars with team members to make scheduling easy, and can know whether colleagues are busy, away or available to chat simply by viewing an indicator next to their names.



Virtualization

Virtualization consolidates physical server hardware onto virtual machines that live in the cloud, helping businesses cut costs, operate more efficiently and recover more swiftly from disaster.

Why is this important?

If a physical disaster ruins your datacenter, it will ruin your virtual environment as well, damaging or destroying critical business data. However, virtualization allows a business to replicate its virtual environment and host it in an offsite or disaster recovery (DR) location. That way, if physical disaster strikes, in most cases business can migrate to the DR datacenter within minutes to prevent downtime.

Furthermore, the complex virtualization layers can sometimes help to protect against virtual disasters. They can act as shared storage in storage area networks (SANs) that allows data to be replicated to other virtual environments.

solutions

Microsoft Security Essentials

Microsoft Security Essentials provides real-time protection for your home or small-business PC that guards against viruses, spyware, and other malicious software. Microsoft Security Essentials is a free download from Microsoft that is simple to install and easy to use and that is automatically updated to protect your PC with the latest technology. Microsoft Security Essentials runs quietly and efficiently in the background, so you are free to use your Windows-based PC the way you want—without interruptions or long computer wait times.

Why is this important?

The greater the security of your PCs, the less the chance that a virtual disaster like cybercrime could impact your business.

Windows 7 and BitLocker

Microsoft's most secure operating system to date, Windows 7 helps SMBs operate more efficiently with features that promote greater productivity, mobility and security. Your business and personal information is one of your most important assets. If unprotected, a company's sensitive records are under risk of unauthorized access by threats ranging from spyware to outright theft. BitLocker and BitLocker-To-Go are built into Windows 7. While USB drives are easy to carry, they are also easy to lose. In order to prevent valuable data from being lost or stolen when you use Windows 7 you can encrypt and secure your data using these programs.

Why is this important?

An operating system that supports remote working and security becomes immensely valuable in times of disaster. With Windows 7, employees can set up Remote Desktop Connections for easy, secure access to important business data from locations outside the office.

Additionally, Advanced Backup and Restore lets users save copies of important or sensitive information to other drives, discs or even networks. Using a program like BitLocker-To-Go prevents someone who finds your USB device from accessing your information. This is especially important if you or your employees are working remotely from a coffee shop or other public place where you'll need protection in the event of a theft.

Windows Phone

With software and services uniquely designed for SMB users, Windows Phone makes it easier than ever before to remain productive, keep in touch and protect your information while on the go.

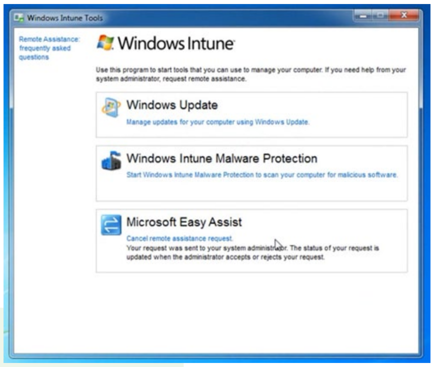
Why is this important?

If disaster occurs, Windows Phone can help keep your employees productive, even if your office is inaccessible, and can safeguard your business information. Windows Phone runs Microsoft Office Mobile, a version of the world's leading productivity software, giving workers the tools they need to accomplish everyday tasks from any location.

Furthermore, Find My Phone, a free PC service that comes with Windows Phone, lets you remotely lock, wipe, or locate your Windows Phone if it is ever lost or stolen. Online backup services provide peace of mind should disaster destroy any data stored on mobile devices.

Windows Intune

Windows Intune simplifies and helps businesses manage and secure PCs using Windows cloud services and Windows 7—so your computers and users can operate at peak performance. With Windows Intune, you can remotely perform a number of security and management tasks including manage updates and endpoint protection to help safeguard PCs from malware threats.



Windows Intune Tools

Remote Assistance: frequently asked questions

Windows Intune

Use this program to start tools that you can use to manage your computer. If you need help from your system administrator, request remote assistance.

Windows Update

Manage updates for your computer using Windows Update.

Windows Intune Malware Protection

Start Windows Intune Malware Protection to scan your computer for malicious software.

Microsoft Easy Assist

Cancel remote assistance request.

Your request was sent to your system administrator. The status of your request is updated when the administrator accepts or rejects your request.

Why is this important?

Windows Intune provides endpoint protection, update management, hardware and software inventory, remote assistance and more through a single Web-based console. This means that your employees can remain productive from virtually anywhere—all that's required is an Internet connection.

where to turn

Need more help?

Proper technology implementation ensures your business gains complete protection from disaster. For the person who becomes the “accidental techie” at an SMB, this task often proves difficult, especially with an overwhelming number of options and solutions to choose from. If your business needs assistance with its technology implementation, check out Microsoft’s Pinpoint, which helps you locate Microsoft partners in your area and also matches your needs to an IT solution provider local to your area.

Now that you've got a background in preparing your business for potential disasters, it's time to put your plan in action. Consider the following worksheet as the framework for your business' GO bag. Much like you started your venture with a business plan, develop your disaster preparedness plan from the ground up.

Business Continuity Basics:

1. Who? Determine who needs to be alerted to a disaster, whether virtual or physical. Focus first on internal communications. For physical disasters, think of employees that may be traveling to the office. With a virtual disaster, don't forget those employees who work remotely and are accessing your network.

How will you communicate? Do you have an internal message board online?

____

____

2. What Happens Next? Your vendors and clients, who are not affected by the disaster, will expect business to continue as usual.

Will you have access to your business data? Does your team know how to access backed up data? Do you have automatic payments in place? If it's a physical disaster that's causing service issues, can you work remotely to continue delivering your product? Do you know what your insurance will really cover in the event of a disaster? Stay current on your insurance policy and new options to protect your business and team.

____

____

3. **Educate Employees.** How often do you alert your employees to potential online threats and how to avoid potential issues? Have you reviewed disaster preparedness plans with your team?

Establish a rhythm of information about your preparedness plans and everyone's role. Discuss new threats, including social phishing scams or malware/scareware attempts, and provide insight on how to avoid being a target.

____

____

Technology Protection

1. **Where is your Intellectual Property?** Your business plans, customer notes and contact information, fee structure or secret recipes are unique to your business. If you store this information on an external hard drive or USB, you could face a catastrophic disaster if those were stolen, damaged or lost.

Do you have an online storage drive or online back up to save your data in the event of a theft or if there is a physical disaster? Who on your team knows how to access the back up?

____

____

2. **What's your security system?** Hackers, now more than ever, are targeting SMBs because of the low-risk of infiltrating their systems. A very simple and free way to increase your protection is to keep your technology updated. Updates are developed to address the latest security threats.

How many machines need updating? Have you set updates to be installed automatically? Don't forget mobile phones used for accessing business information.

____

3. Is travel prevented by a disaster? If a physical disaster is preventing employees from going in to the office or visiting clients, business can still be conducted from remote locations.

Have you transitioned to a cloud service? If employees can access work documents they need from their home machines, you may be able to prevent disruption to your daily deliverables.

____

4. Understand what you own. If you store business information or access it via the cloud, your data is being housed in a data center by your provider.

Review your service level agreement (SLA), which will identify their promised uptime. This will indicate how quickly you can expect outages to be addressed. (Industry standard is around 99%)

____

____

Use the space below to list other areas that you might need to address in the event of a disaster.

____

____

____

____