Microsoft

Disasters happen.
Is your business ready?

Guidance for preparing your business to withstand the unexpected

Microsoft

Table of Contents

executive summary

44%

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

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.

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

Microsoft

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.

Microsoft

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.

50%

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

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.

technology strategy

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

Microsoft

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.

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.

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.

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.

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.

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.

DISASTER PREPAREDNESS

Microsoft

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.

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.

DISASTER PREPAREDNESS

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.

9

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.
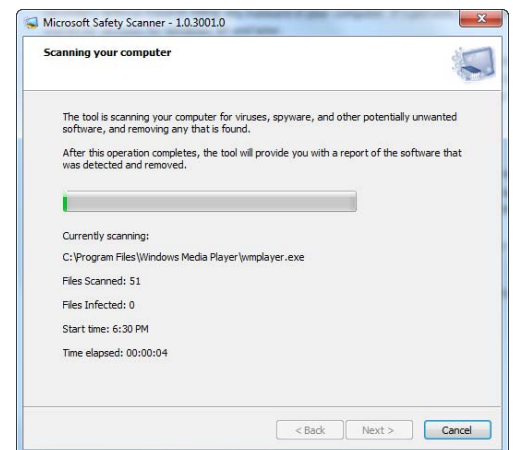
solutions

Microsoft

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

< Back   Next >   Cancel

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.

solutions

Microsoft

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.

Microsoft® Office 365

13

solutions

Windows Server 2012

Having a virtual machine or virtualizing your computer is a key component to disaster preparedness, as it helps businesses recover when on-premise servers are struck by a physical disaster. Windows Server 2012 makes desktop virtualization more accessible and affordable for small businesses. Traditionally, only large companies could afford a virtualization solution, but now small businesses have access to the same disaster preparedness capabilities through Windows Server 2012.

Why is this important?

The threat of losing important business data can be daunting and knowing how to protect that data may be unclear. Imagine a worst-case scenario, which could be anything ranging from a fire to a flood, and your business could lose critical data. With virtualization, SMB customers are able to replace traditional workstations with low-cost virtual desktops, personalized PC profiles and applications that employees can access over a local area network or the Internet from a variety of devices. Windows Server 2012 offers customers of all sizes, enterprise-level capabilities to keep their businesses running, help them make the most of their IT budgets, and identify ways to scale their technology to meet fluctuating needs at an affordable price. With Windows Server 2012, small businesses can continue work uninterrupted even during a disaster, giving you the comfort of knowing that your data is safe and will not be compromised.

By consolidating physical servers onto virtual machines, you can be up and running even within moments of a disaster occurring. With Windows Server 2012 and they can get Remote Web Access which provides a streamlined, touch-friendly browser experience to access applications and data from virtually anywhere. Additionally, now a small business can connect to, search across, and access files and folders on their server through a Windows Phone app. The Windows Server 2012 edition also contains Hyper-V Replica, which provides a complete copy of your data between your on-premise and off-premise server, using a standard broadband data line. Hyper-V Replica continually makes copies of changes to your data every five minutes, so if a failure disables the primary server onsite, the organization never loses more than five minutes of data which promotes business continuity should a disaster strike.

 Windows Server 2012 Essentials is another of Microsoft's server offerings, also made specifically with small businesses in mind. Storms and fires aren't the only disasters to prepare for and with this version, if an employee of a small business happens to misplace their laptop, the business has a line of defense to protect business information on the machine. A small business with 25 employees or less can back up all of their computers and servers in the office and in the cloud with Windows Server 2012 Essentials. Additionally, Storage Spaces are also available on this version to enhance the process of increasing data backup capabilities to be more affordable, easier and quicker.

solutions

Microsoft

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.

solutions

Microsoft

Windows 8

Microsoft's newest operating system, Windows 8 Professional was designed with SMBs in mind to deliver an experience with new levels of mobility, productivity and security, without sacrificing performance or choice. The features that promote greater productivity, mobility and security in Windows 8 will help to defend your business against potential virtual or physical disasters.

Why is this important?

An operating system that supports remote working productivity and security becomes immensely valuable in times of disaster. Productivity is a major factor in keeping businesses running after a disaster affects your business. The Remote Desktop feature allows users to connect to their desktop back at work and have full access to their files, so it's as if they are sitting at work in front of their computer.

Windows 8 Professional includes built-in mobile broadband support for 3G and 4G telecommunication, enabling businesses on-the-go to connect to the Internet immediately and also identify Wi-Fi hotspots when available. With increased mobility, comes additional security considerations and BitLocker, a feature in Windows 8, can help protect your business from security disasters. BitLocker helps protect business data on PCs with faster hard drive encryption, helping to keep data safe without interrupting worker productivity. In addition to BitLocker, Windows 8 Pro also has BitLocker To Go, which takes the same technology and applies it to USB sticks and external drives so that file information there can be completely locked down and become virtually impossible for hackers to compromise. This is important for any of your remote employees who may be conducting business on the road, at a local coffee shop or on a plane who could be at risk for data theft.

One of the biggest virtual disaster threats doesn't have to do with hackers or thefts, but with phishing attacks, where people are tricked into disclosing their passwords. With Windows 8 Pro, SMBs can now browse more confidently with features like Windows Defender and Windows SmartScreen, along with more security built into Internet Explorer 10, which helps identify and warn against phishing attacks.

While most SMBs will opt for the Windows 8 Professional version, the technology in Windows 8 adapts to meet the needs of a growing business. In the Windows 8 Enterprise edition, available to volume licensing customers, the Windows To Go feature can give you a complete installation of your Windows 8 corporate desktop on a high performance USB flash drive. It has to be provisioned by an IT professional within the enterprise organization, and will turn any computer into your business computer after the proper installation done by an IT professional.

solutions

Microsoft

Windows Phone

With software and services uniquely designed for SMBs users, Windows Phone makes it easier than ever before to remain productive, keep in touch and protect your information while on the go. If a disaster prevents you or your employees from returning to a physical office location, having a Windows Phone allows you to work no matter where you are.

Windows® Phone

Why is this important?

Windows Phone can help keep your employees productive, even if your office is inaccessible, and can safeguard your business information. Windows Phone offers familiar Office Mobile apps like Outlook and Lync that are already built-in. It also runs Microsoft Office Hub, which provides access to Office applications like Word and syncs documents, files, videos and photos to SkyDrive for secure backup. Furthermore, SharePoint, Office 365, Exchange and other favorites are accessible, giving you and your employees the tools needed to accomplish everyday tasks from any location. Additionally, Windows Phone offers robust security features to protect your business information, guard against malware and even lock, wipe or locate your phone if it's lost or stolen from a remote location.

solutions

Microsoft

Windows Intune

Windows Intune™

Windows Intune is a cloud-based device management system that helps small businesses avoid upfront maintenance costs while being able to check for updates and install software as needed across Windows and non-Windows machines and devices. Small businesses can use it to make sure computers and mobile devices are up to date and delivering top performance to remote workers, while protecting business data from virtual disasters such as breaches and corruption.

Why is this important?

Windows Intune offers small businesses a comprehensive package of PC security and management solutions and Windows upgrade licensing in a single subscription. You can remotely perform a number of security and management tasks to protect your business data and technology, including management of updates, remote assistance to offsite users, PC monitoring, endpoint protection to help safeguard PCs from malware threats, and inventory management so IT and end-users can remain productive from virtually anywhere. With Exchange ActiveSync (EAS) capabilities you can manage the software and hardware used by mobile phones connected to your network, while also enforcing encryption and password requirements that you determine. Windows Intune makes it simple to manage updates and enforce device access policies – the only thing you need is an internet connection.

where to turn

Microsoft

Want to learn more?

A little research and some expert guidance can help ensure your business is protected from potential disasters. For more information, visit www.microsoftbusinesshub.com, where you'll find technology best practices and business advice for small businesses, learn more about Microsoft products for SMBs, find technology support resources, and find a Microsoft Partner with small business technology expertise to assist you.

worksheet

Microsoft

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.

_____

_____

worksheet

Microsoft

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.

_____

Microsoft

---

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.