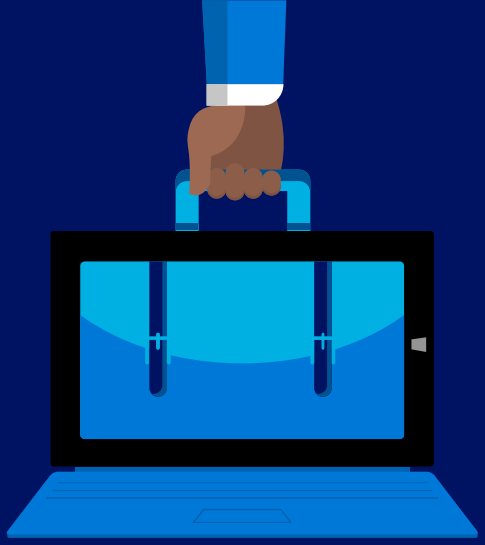
South Bay
Computer Solutions

eGuide: Create the Ideal Disaster Plan for Your SMB

From natural disasters to cyberattacks, small businesses face big threats. We'll help you defend against them.



One solution, designed for your business

- Achieve more together
- Anywhere it matters
- Always-on security
- Simplified for business

Here's what you'll get from this eGuide:

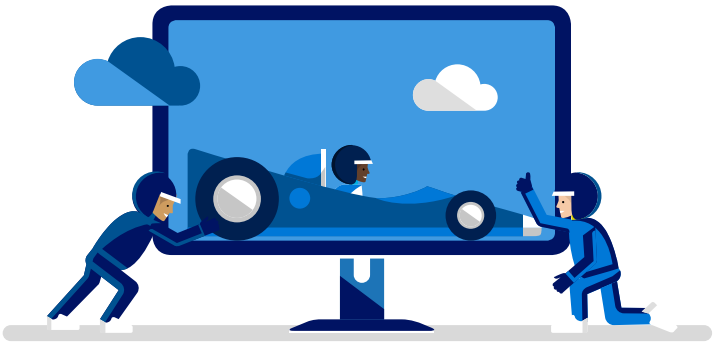
1. Discover why disaster preparedness is a top priority for your business
2. Take our quiz to assess your level of preparedness for cybersecurity threats
3. Learn how to develop a quick start business and technology plan

South Bay Computer Solutions

Disaster preparedness is a business priority

Every business in the world starts small. However, even small companies face huge threats. In this eGuide, we'll explain why a comprehensive cybersecurity and disaster-recovery plan should be a top priority for your company, even if it only has a few employees. To help you devise the perfect strategy, we'll outline some of the biggest threats for small companies, assess where your business currently stands in its cybersecurity approach, and assist you in finding experts to help implement a solid solution.

If you own or work for a small business, you're far from alone. Nearly every business in the U.S. is a small- to medium-sized company: According to 2014 U.S. Census data, nearly 90 percent of businesses in the country have fewer than 20 employees, while a staggering 99.7 percent have fewer than 500. These small and medium-sized businesses (SMBs) represent the backbone of the U.S. economy. As such, it's essential to protect their data, their finances, and their future from a complex variety of threats.



Many of those threats seem difficult – if not impossible – for an SMB to plan for. A natural disaster, for example, can strike when least expected. What's more, SMBs have become a top target for cyberattacks, and for the majority, the effects of a cyberattack will put the company out of business.

An SMB's employees are often required to wear a lot of hats in terms of job responsibilities. It's what helps make these companies nimble, exciting, and rewarding to work for. But it also makes them vulnerable. Fewer resources and employees often equate to the lack of a dedicated IT department, sufficient security practices, or adequate security training for employees.

Natural disasters and coordinated cyberattacks may seem like vastly different challenges, but preparing for each scenario involves a lot of overlap. Both require devising a strong, easy-to-understand, and multifaceted response and recovery plan that involves the entire company. Both also necessitate smart technological planning, such as making business data and applications available in the cloud. Lastly, both call for similar logistical planning on the business end, such as training employees for mission-critical recovery tasks.

Putting off developing a plan puts your business at risk. We're here to help you get started. First, we'll help determine where your company stands in its disaster and cybersecurity preparations. Then, we'll walk through the best practices for devising an effective strategy for your technological infrastructure and your business operations. Don't worry if you don't have the headcount to devote to the task; as a your Trusted IT Advisor. We can help your business on a regular basis with an Remote Service Plan.

South Bay Computer Solutions

Disaster-Preparedness Quiz

An internet outage or inaccessible systems can cost your company thousands of dollars every day, even if your business is small. That's why it's incredibly important to prepare for the worst, whether it's a security threat, a natural disaster, or a power outage. This quiz will help guide your company toward an effective recovery plan.

Are your company's critical systems backed up on an hourly or daily basis?	○ Yes	○ No	○ I don't know
Are your company's critical systems accessible in the cloud?	○ Yes	○ No	○ I don't know
Does your business have an emergency contingency plan in case a disaster strikes?	○ Yes	○ No	○ I don't know
If a disaster struck your office or business location, would your systems keep running, uninterrupted?	○ Yes	○ No	○ I don't know
If your systems were hacked or otherwise compromised, do you have clean data backups that can be implemented swiftly?	○ Yes	○ No	○ I don't know
If there is a system or server failure, can your company's data and website be restored quickly?	○ Yes	○ No	○ I don't know
Are your employees aware of the latest security threats and how to identify them?	○ Yes	○ No	○ I don't know

Are your employees regularly informed about what to do if a system failure, cyberattack, or natural disaster occurs?	○ Yes	○ No	○ I don't know
Is each department in your company aware of what to do and how to collaborate in the event of a system failure, cyberattack, or natural disaster?	○ Yes	○ No	○ I don't know
Are employees outside of your IT department aware of what to do if a disaster strikes and are they trained to perform the basics?	○ Yes	○ No	○ I don't know
Does your business have redundant servers and data centers in various locations?	○ Yes	○ No	○ I don't know
Do each of your employees have an emergency contact list?	○ Yes	○ No	○ I don't know

If you responded "yes" to eight or more questions, your company is on solid footing when it comes to disaster preparedness. If you responded "no" or "I don't know" to some of these, read on. This eGuide provides more advice to help your small- to medium-sized business running smoothly when confronted with calamity.

South Bay Computer Solutions

Disaster Preparedness **Technology Plan**

Use the cloud for anything you can

Many businesses keep critical servers, systems, and data on-site. That may make it easier for your IT team to service and maintain those important systems, but it can spell doom if your office takes on damage from a natural disaster. Cloud storage and web applications ensure that your important data and processes are always available, no matter what happens. They're also incredibly convenient for the mobile workforce.

Eighty percent of Fortune 500 companies use Microsoft Cloud, and with good reason. Web storage and applications ensure important data and processes are always available.

Back everything up, everywhere

Cloud services should also be used to create regular, redundant data backups in case your systems are damaged or compromised by a security threat. Don't limit your backups to just the obvious stuff. If your company uses smartphones and mobile applications as part of its workflow, make sure the data on those devices is also backed up. In addition to using cloud storage, it's wise to create hard-drive backups in case the online service you use is compromised or temporarily inaccessible.

Secure all your backups

You should apply the same security practices to your backups as you do with all your business data. That means encrypting all your files, whether they're online or on a hard drive. Otherwise, one stolen drive or password could put all your company's critical data in the wrong hands. And of course, please don't use passwords that are ridiculously easy to guess.

Azure Security Center protects against many kinds of cloud-based attacks, keeping your data secure.

Disaster Preparedness **Technology Plan**

Ensure your tech is safe

An out-of-date operating system (OS) or unpatched software can be rife with security holes. To avoid exploits, make sure your software and OS are set up to install all the latest updates. They should include all the necessary security patches and other critical updates, and you can configure your PC to install them automatically. In Windows 10, automatic updates are enabled by default.

Each month, Microsoft releases a Windows Update to ensure the operating system is protected against the latest known vulnerabilities.

Don't get burned by IoT

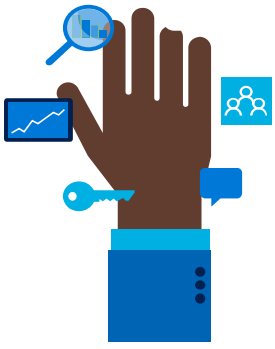
Internet of Things devices such as connected security cameras are useful for your business, but they can also open up security vulnerabilities in your network. The massive Mirai botnet spread across the globe through IoT devices, and they have become primary attack targets for a simple reason: You can't install antivirus software on many IoT devices. Make sure your security solution can detect and eliminate network-wide malware.

Keep important documents offline

Even if you have a well-thought-out plan, a disaster may make it inaccessible if it's stored on a computer. Make sure you have printed-out versions of your emergency contact lists, employee roles, and disaster-response plans and that they're easily accessible for your entire team. At least two people should be trained to do every disaster-recovery task.

When in doubt, ask for help

Even when there isn't a disaster to contend with, running a small- or medium-sized business can be a handful! If you need access to an IT expert that can ensure your disaster-response plan is built for success, the Microsoft Partner program is an invaluable resource. Ensure you have all the bases covered by visiting the Azure disaster-recovery guidance page, the Azure backup and archive website.



If your company needs custom guidance ,as a Microsoft Partner we can help..

South Bay
Computer Solutions

Disaster Preparedness **Business Plan**

Make sure employees know their roles

As a small- or medium-sized business, your company may not have an HR department. That means it's important for business owners to make sure their employees are organized, informed, and prepared for a crisis or security breach. Make sure each employee's role is clearly defined, multiple employees are trained for each task, and that your leadership team will be able to provide guidance and encouragement along the way. You should also create a chain of command when it comes to external communications.

Make sure each employee's role is clearly defined and that several employees are trained for each task.

Plan a diverse communication strategy

In the event of a disaster, your customers, colleagues, and audiences will want to know that you're OK. Everything from phone service to power to internet connectivity may be down during extreme circumstances, so it's wise to create an external communications strategy with several options in mind. That means more than just having a plan for social media, email, and phone communications – although all those things are important. It also means having a list of all your suppliers, vendors, partners, and employees' emergency contacts, complete with information on how to reach them across all those options.

If the power goes out, will you still be able to communicate? Your plan must have several options in mind.

Disaster Preparedness **Business Plan**

Know your coverage

You can't plan for a disaster, but you can plan for the best recovery possible. Make sure you read your company's insurance plans and policies thoroughly to determine which physical disasters and other situations are covered. It's also important to get all your forms and deadlines in order so that the response can be swift after a disaster strikes.

Your company's insurance plans may not cover everything. Read them thoroughly as part of your disaster preparations.

Practice, practice, practice

You shouldn't execute your disaster-response plans for the very first time during a disaster. Just like a fire drill, your team should simulate these scenarios and go through the process of getting your business back on its feet. As part of the preparation, each of your employees should also work one full day from home to determine whether critical systems run smoothly for remote workers.

Don't forget your bills

It may be the last thing on your mind during a disaster, but your company will still have to pay suppliers and make payroll during tough times. That means ensuring you have access to your financial data, key contacts, and contingency payment options even if your power or internet is down for days.

Avoid paying overdue bills during your recovery process. Ensure you have access to financial data, contacts, and payment options.

Insider Tips:
Surprising SMB Security Threats

From mobile to social to the cloud, the past decade has introduced amazing new possibilities for small businesses everywhere. However, many of those groundbreaking capabilities have been accompanied by frightening new threats.

The face of cyber threats is changing every day, and protecting your business against the prevalent threats of years ago isn't enough. You need new layers of defense to mitigate new vulnerabilities, as well as vigilant employees who can identify potential risks as they occur. The nature of those risks can be unexpected, so instinct alone can't be your mainline of defense.

The good news is, you don't have to go it alone. A Microsoft Partner can help you protect your data, your customers and business. In fact, we enlisted the help of two Microsoft Partners in the SMB security consulting industry to create a list of the most surprising security threats right now. Paul Hager, CEO and president of Information Technology Professionals (ITP), and Bruce Ward, vice president of business strategy at Peters & Associates, share their expert insight below.

Mobile threats

Whenever we ask a customer "do you have antivirus on your phone?" they look at us like we're aliens. It's not a crazy question to ask, and it is really critical. There are thousands of mobile viruses, and they are scary. Some download illicit material onto your phone and then report you to the police. Mobile devices have to be part of your security plan, and that must extend beyond simply being able to remotely wipe the device. There has to be antivirus, and there has to be control on where data is going. It's not hard to do. Microsoft Intune and Microsoft 365 in the cloud make it easy to take that security step for mobile devices. – Paul Hager, ITP

Mobile viruses are a big threat to any business, and they use shocking tactics.

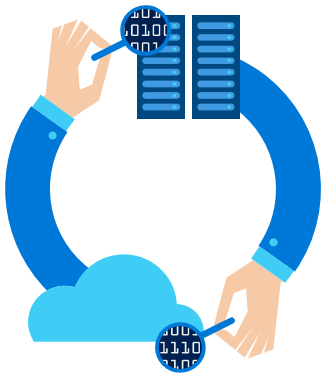
Insider Tips: Surprising SMB Security Threats

Sketchy heists

Fraudulent instruction is on the rise. With some clever maneuvering by a hacker, a businesses' accounting department is coerced into wiring money to a vendor that suddenly shows up in their system. It's particularly prevalent in small and medium-sized businesses. If an email clearly doesn't have the same tone your colleague would typically use, it should raise flags. We had a conversation with a CEO recently whose accounting department sent $35,000 to an unknown vendor based on how closely the request mirrored a legitimate one. He said it was like money coming directly out of his pocket. Amongst other things, you need to make sure that fraudulent instruction is specifically covered in your cybersecurity insurance policy. – Bruce Ward, Peters & Associates

Old-school exploits

Thumb drives are still an interesting one. We've put software on a thumb drive and left it in the parking lot to see how many people pick it up and plug it into a computer. We've done experiments with school districts where we call into a teacher's room and say we're from IT support and we need to verify their password. Fifty percent of teachers will give us that password over the phone. All you need to do is be nice. These are experiments based on what people are actually doing, and they are targeting schools. – Paul Hager, ITP



Schools have become major targets for hacks, cyberattacks, and data thefts.

Doubling down on SMBs

Small and medium-sized businesses are likely more prone to known vulnerabilities as opposed to zero-day threats. Many don't have the resources to stay patched or to even track those things, which can make them one of the biggest threats. Hackers aren't really targeting specific organizations, they're looking for the weakest link. Most times the evil-doers are not differentiating or being scrupulous about who they're hitting. It's just a blanket approach. – Bruce Ward, Peters & Associates

Need Help with your business ? Contact me for Assistance

Delivering technology business solutions, best practices, service and support through proven methods of proactive analysis, implementation, configuration and maintenance. I help create solutions designed to reduce costs, increase your profits and mitigate business risks, working with you as your Virtual Technology Partner. Focusing on your technology, allowing you to focus on your business.