

BEST PRACTICE GUIDE TO SMALL BUSINESS PROTECTION: **BACKUP** YOUR SMALL BUSINESS INFORMATION



ENTER ▶

YOUR BUSINESS depends on electronic customer lists, confidential information and business records. Protecting this information—keeping it in the right hands, uncorrupted and available for use—is the foundation of running your business.

Most business owners are confident that their information is safe, and that their customers will tolerate “routine” business interruptions—but the facts tell a different story:¹

- The average small or mid-size business backs up only 60 percent of its company and customer data
- Customers estimate that a vendor’s computer outage costs them \$15,000 per day
- Forty-two percent of small-business customers have dropped vendors because of unreliable computers or systems

The risk of information loss, system failure, external attack and employee error are already significant, and continue to grow along with the volume and value of business information. The time is right for a clear assessment of your risks, and a realistic plan to address them—for your customers, your reputation, and your business future.

Discover best practices for protecting your business data and the solutions available to start now by reading these articles. To learn more about solutions designed to protect your business information visit the [Symantec Small Business Solutions site](#).

¹ Applied Research – West, Inc. SMB Disaster Preparedness: Survey Results (Global Data). (Los Angeles, CA: September, 2009).

CONTENTS

Plan for the Best. Prepare for the Worst.....	3
Do you have a policy to manage your information?	5
How to tackle the backup challenges facing your business.....	7
How to find the right IT partner for your business.....	9

**SYMANTEC IS
BACKUP.**



PLAN FOR THE BEST. **PREPARE FOR THE WORST.**

Here's food for thought:

The average small or midsize business has experienced three technology failures in the past 12 months, with the leading causes being virus or hacker attacks, power outages, and natural disasters. The cost of these outages: an estimated \$15,000 per day.

That's according to [Symantec's 2009 SMB Disaster Preparedness Survey](#). Perhaps more troubling, the survey found a large discrepancy between how small and midsize businesses perceive their disaster readiness and their actual level of preparedness. For example, while 84 percent of the respondents said they feel protected in case a disaster strikes, almost half reported they don't have a plan to deal with such disruptions.

Obviously, no one wants a disaster to occur, but the reality is that they happen. That's why now is the time to ask some hard questions about how well you're protecting your data and systems. For example, even if you consider yourself proactive about backing up your data, how protected are you in reality? Say your company's systems are lost in a flood or a hurricane. How quickly can you recover access to your data and continue business operations? What are your customers' expectations? Can they wait for days or weeks for your business to recover? More importantly, will they?

This article looks at the importance of automating backup and recovery, both for your PCs and servers and for the important data residing on them.

Protect your systems.

Each business has its unique information protection and disaster recovery challenges. However, all businesses face similar issues when it comes to keeping data and systems protected and available. For example, regardless of how many servers you have, you rely on them to keep your employees connected to the applications, printers, and data they share. If your Microsoft® Exchange server goes down, access to those resources is lost until the server can be brought back online. That means you lose collaboration, you lose productivity, and (in most cases) you lose money.

When a server's operating system fails, it can take hours (or even days, in some instances) to rebuild and restore the server. This process includes re-installing the operating system, applications, and patches; configuring settings and application data; and so on. Moreover, there is no guarantee the server will be in the exact same state as before the failure took place.

To hedge against hardware failure and still allow for automated system recovery, some organizations purchase duplicate hardware for their most critical computer systems. But maintaining duplicate hardware is so cost-prohibitive that only a few organizations can justify it. Chances are, a small or midsize business is not in a position to afford the luxury of maintaining extra server hardware in case it needs to replace an existing system.

This introduces the prospect of restoring a system on a new—and dissimilar—piece of hardware. You want to be sure that you can recover from system loss or disasters in minutes, not hours or days—even to dissimilar hardware platforms.

Protect your information.

According to a survey by [Rubicon Consulting](#), half of the small businesses they talked to said they had lost critical data at some time. Unmanaged, hit-or-miss manual backup processes were frequently to blame. That's because manual processes are unreliable and can put information at risk. Automating the backup process ensures that it's not forgotten or overlooked when demands on staff time intensify.

It's also prudent to back up data offsite; otherwise, you risk losing access to both your primary data and the backup in the event of a disruption or natural disaster.

(continued)

PLAN FOR THE BEST. **PREPARE FOR THE WORST.**

While no single set of rules will protect every business, smart businesses follow best practices like these:

- **Schedule backups.** Implement and enforce backup schedules—and automate the process as much as possible. Manual processes are time consuming and prone to error.
- **Back up systems, too.** Backups are only as good as your ability to use the information you recover, so back up systems and applications as well as files.
- **Keep backups offsite.** Fires, floods, vandalism, and sabotage are reality. Be sure files and systems can survive the loss of your primary facility, or even a regional disaster.
- **Test backups.** Don't wait until disaster strikes to discover a resource, process, or technical shortcoming. Regularly test the entire backup and recovery cycle. Can you recover to dissimilar hardware?
- **Get help.** Find a local IT partner who understands and can help with both your business and technical requirements, and whom you trust.

Symantec Backup Exec™ System Recovery

delivers the leading Microsoft Windows® data protection and system recovery solution for small businesses. It enables you to realize shorter backup times, experience faster and more flexible system recoveries, prevent data loss, and minimize system downtime. With Backup Exec System Recovery, you can restore complete Windows systems in minutes, even to dissimilar hardware.

Symantec Backup Exec System Recovery doesn't disrupt data access or application usage. Backups and recovery points can be scheduled periodically throughout the day, helping to ensure that a recent snapshot of the system and open file data is always available.

Conclusion

Today you're using IT more than ever before to stay efficient and competitive. Make certain you stay that way by ensuring that your computers and critical information are protected and available. With [Symantec Backup Exec System Recovery](#), you can be confident that your critical data and systems are continuously protected, allowing you to focus on running your business.

DO YOU HAVE A POLICY TO MANAGE YOUR INFORMATION?

How effective are you at managing your company's information?

It's a question worth asking at any time, but it's particularly urgent today, given that more and more information is becoming digital, new computing devices are proliferating, viruses are flourishing, and issues about privacy and the protection of confidential information continue to evolve. No wonder many small businesses find themselves struggling to keep up.

A solid data management policy is essential to weathering these challenges. If you don't have a policy currently in place, now is the time to get started.

A greater challenge than ever

Whether it's an email message, a Microsoft® Word file, or an instant message, you have to find a way to manage your information responsibly. The same goes for the information that is carried on your laptop computers, cell phones, PDAs, memory cards, flash drives, and even consumer devices such as multimedia players. It all has to be managed.

That means you need to be familiar with all the ways in which your electronic information is captured and stored. The following steps can help you size such a project.

Step 1. Collect the personnel.

Begin by gathering together the people who have the best knowledge of your company's business needs, regulatory and legal obligations (this may involve consulting with an outside legal expert), and email and information use. Get input from a representative of every department to ensure that all needs are considered.

Step 2. Collect the information.

Once you've collected the personnel, identify the types and categories of information that your company generates, where and how that information is maintained, and the people who are responsible for maintaining it. Who has permission to view, modify, and delete information? You must be able to prioritize your information to determine what is critical to securing and protecting your business.

Step 3. Establish a data management policy.

Next, decide how long to preserve your information, beginning with regulatory and other legally established minimum periods. For example, you want to retain patent correspondence indefinitely, but discard spam at once. Specify how data that is no longer needed must be securely purged.

Step 4. Don't forget backup procedures.

Small businesses are vulnerable to various forms of data loss. A 2008 survey of several hundred small and midsize businesses by Rubicon Consulting found that about one-quarter of the companies didn't back up their servers or PCs. In addition, most of those surveyed stored backup files in the same location as the computers backed up. Issues to address in this step include:

- Store backup files remotely. The Rubicon survey found that more than half of all backup files were stored in the same location as the originals. That can leave a company vulnerable to the permanent loss of its data in the event of hardware theft, malicious destruction of the data, or disaster.
- Employ data deduplication. If your company uses a disk-based backup and recovery solution, data deduplication eliminates the need to store multiple copies of the same data over time. Eliminating extra copies reduces the capacity and cost of a disk-based solution.

(continued)

DO YOU HAVE A POLICY TO MANAGE YOUR INFORMATION?

Step 5. Address your company's specific business needs.

You may want to designate retention periods on the basis of specific business needs or on the potential for litigation. For example, you should consider how often access to the information is needed on a regular basis. To what extent is information distributed outside the company? What is the potential for future litigation with respect to the content? You need to establish clear guidelines about how outsourced or temporary staff access your data and how and when to terminate that access.

Step 6. Put it in writing.

The newly established data management policy needs to be written down and distributed to all employees. It shouldn't be elaborate; in fact, the more straightforward it is, the better. But it should include specifics about the various categories of information you identified.

Conclusion

As more and more of your critical information moves from paper to digital format, the pressure is on you to manage that information effectively. The rapidly changing threat landscape and growing compliance and legal discovery requirements are creating additional risks, further complicating the information management challenge. Your task is to ensure that all employees know the proper procedures for protecting critical business information.

Symantec can help you craft a data management policy that focuses on protecting your information from leakage and loss while lowering costs. Such a policy will show you how to automate backups to ensure your information is safe and recoverable in case of hardware failure or disaster, how to stop leakage of sensitive information by preventing its transmission from your computers, and how to minimize downtime caused by lost information or failed computer systems.

Related resources

[Symantec™ Small Business Solutions](#)

HOW TO TACKLE THE BACKUP CHALLENGES FACING YOUR BUSINESS

As a small business owner, you invest a lot of time, money, and energy in making your business a success.

And while you understand the importance of protecting your assets and planning for a disaster, you may not have the time to do all that you need to do to protect your information from malicious threats, human error, or a natural disaster.

How well you are prepared is the key to minimizing the effects of a disaster and getting back to business quickly. Consider: Half of the small businesses that lose customer information go out of business. By implementing the technology tools and best practices to guard against data loss and system downtime, you can ensure that you will be able to recover from any disaster that comes your way.

Let's look at some of the key backup challenges small businesses face today, as well as at a solution that can help backup practices keep pace.

The top challenges

Your business faces significant challenges when it comes to effectively backing up the data that resides on your PCs, laptops, and servers. These challenges have been ranked by the technology analysts at the Taneja Group, as follows:

- Implementing comprehensive protection with minimal impact on business operations. Chances are that your staff is focused on running the company rather than on backing up data.
- Meeting increasingly stringent backup and recovery requirements. The requirements to recover specific data and to reduce the overall time to restore data are becoming more important. Every minute of downtime has an impact on your business.
- Dealing with limited IT administration resources. This is a key issue for smaller companies, which often lack dedicated IT staff or a backup admin. As a result, backups tend to be manual and not continuous.

- Deploying disaster recovery strategies efficiently. The legacy practice of backing up to tape and then shipping the tapes to an outside contractor can be risky. In recent years there has been no shortage of news stories about tapes disappearing during shipment.
- Leveraging new technologies. Because of limited resources, small businesses may be unwilling to evaluate and deploy critical new technologies as they become available.

Manage backups easily.

Keeping your critical data and systems secure should be automatic. That's a guiding principle behind the backup solutions from Symantec: Backup Exec™ System Recovery Desktop Edition and Backup Exec System Recovery Server Edition.

Designed specifically for companies with 10 to 99 employees, Symantec Backup Exec System Recovery protects data and systems from computer failures and other types of disruption by helping businesses do the following:

- Ensure business continuity. With Symantec Backup Exec System Recovery, you can be confident that your business assets—data as well as laptops, PCs, and servers—are protected from computer crashes, power failures, human error, and other disasters.
- Enjoy reliable, automated backup and recovery. You can schedule backups so that protection is automatic. You can also restore entire computer systems to an exact point in time, without the need for tedious manual recovery processes.
- Minimize downtime. You can get your computer systems back up and running in minutes, not hours or days.

(continued)

HOW TO TACKLE THE BACKUP CHALLENGES FACING YOUR BUSINESS

Symantec Backup Exec System Recovery enables you to easily define, schedule, and run backups of your computers. When a backup runs, recovery points are created that can then be used to recover an entire computer or individual drives, files, and folders. Recovery points can be created throughout the day—without interrupting user productivity or application usage.

Conclusion

Small businesses need backup and recovery solutions that are easy to use and automatic. As the data on your computers becomes more critical to your business, the risk of irrevocable harm to your company's bottom line increases if that data isn't protected. [With Symantec Backup Exec System Recovery](#), you can be confident that your critical data and systems are continuously protected, allowing you to focus on running your business.

HOW TO FIND THE RIGHT IT PARTNER FOR YOUR BUSINESS

Do you sometimes have the feeling that there are dozens of things more important to running your business than, say, backing up your electronic information?

You're not alone. A recent study of small businesses by Applied Research West found that 47 percent don't back up business files on desktop hard drives, even though they know it's important.

But protecting this information shouldn't be an afterthought. After all, it's pretty likely that electronic information and communications are at the very foundation of every business relationship you enter these days.

The good news—especially if your employees are already stretched to the limit—is that help is available. According to a recent Yankee Group report, 61 percent of firms with fewer than 100 employees use a contractor or business partner for IT services.

Now we'll look at some of the key steps in enlisting an IT partner and offer some tips on getting the most out of the relationship.

- First, identify your top technology priorities. According to the [2009 Microsoft SMB Insight Report](#), a March 2009 study looking at the challenges facing small businesses, top priorities this year include virtualization, IT consolidation, business intelligence, software as a service, and support for remote workers. Narrow down the list of potential partners by seeking only the ones whose core competencies and areas of specialty mesh with your needs.
- Choose a partner that specializes in small business. A potential partner should be familiar with the challenges facing today's small business and understand that you don't have deep pockets. Find out what percentage of their clientele are small businesses or organizations.
- Check for certification. Consider the potential partner's level of accreditation—check that they're certified in areas of expertise that meet your needs. Major technology solution providers offer certifications, demonstrating that a partner has

the qualifications and knowledge to expertly work with their solutions. While hiring a certified partner may cost a bit more, it may save you money in the end. You could end up spending a lot more in time and implementation costs to get up and running if you hire the wrong partner.

- Make it personal. A good partner is someone who really wants to get to know you, your processes, and your employees. So make sure that time spent in the discovery process is substantial. Also find out if the potential partner will be utilizing its own staff, or if the people working on your account will be subcontracted. Ask the potential partner for references—preferably from companies whose profile is similar to yours.
- Establish best practices. A good small business partner is one who can help you establish best practices so that you get the most out of your information technology investment. But keep in mind that it is up to you, not the partner, to ensure that these practices are implemented by all employees.

Conclusion

According to the [2009 Microsoft SMB Insight Report](#), two-thirds of all small businesses do not have an IT staff, which makes a partner's role in planning and implementing technology for your business absolutely critical. By working closely with a strong IT partner, chances are you'll find a more efficient, comprehensive approach to small business IT solutions that can save you money, generate revenue, and ultimately help your business succeed.

(continued)

HOW TO FIND THE RIGHT IT PARTNER FOR YOUR BUSINESS

A partnership you can count on

Whether you purchase Symantec™ products individually or in convenient suites from a local Symantec partner, you can always count on protection that will not only match your current requirements, but also will help your business grow.

Symantec protects more systems, networks, and business information than any other company. Contact us today for a comprehensive solution for your business.

Select a solution at the [Symantec Small Business Website](#), your online resource for understanding challenges, recommendations, product details, and selection guides.

Find a solution partner at the [Symantec Partner Website](#). With more than 60,000 partners worldwide, you're sure to find one that's right for your business.

Request a call from a [Symantec representative](#).

Symantec Corporation
Worldwide Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934

Copyright © 2010 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and Backup Exec are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other names may be trademarks of their respective owners.
02/10 20996160