WHITE PAPER:
DON'T WAIT UNTIL IT'S TOO LATE: CHOOSE
NEXT-GENERATION BACKUP TO PROTECT

# Don't Wait Until It's Too Late: Choose Next-Generation Backup to Protect Your Business from Disaster

## Who should read this paper

A Symantec.cloud white paper for Small and Medium-Size Business Owners

Confidence in a connected world. Symantec.

# Don't Wait Until It's Too Late: Choose Next-Generation Backup to Protect Your Business from Disaster

**Content**

## The situation

When it comes to disasters, the question isn't *if*, but *when* they will occur. Ranging from minor power outages to catastrophic floods, disasters more often result from malicious tampering, computer failure, hardware theft, computer viruses, or hacking. Even more common is the catastrophe of simply deleting a critical file accidentally. Whatever the cause, if your company's information isn't protected when a serious glitch occurs, the digital assets that drive your business can be permanently lost. Possible consequences including reputation damage, lost revenue, legal liability, even the close of the business are sobering. Companies must be proactive to ensure that when disaster strikes, their data will be protected, so they can get back to work as quickly as possible.

However, rather than being motivated by these risks, many small and medium-sized businesses (SMBs) are not taking disaster preparedness seriously. According to the Symantec 2011 SMB Disaster Preparedness survey[1], half of SMBs don't have a disaster preparedness plan at all, and others say they have no intention to create one. Since these companies aren't backing up their systems, leaving their data unprotected, it appears that many are simply placing their bets against the event of a severe system outage or data loss.

## Why don't SMBs have a plan?

Given what's at risk, the question is, why don't these companies have a plan? Several reasons were offered. Some respondents felt computer systems aren't critical to the business. Others said it never occurred to them to create a plan. Still others claimed disaster preparedness simply isn't a priority, or that they lack the skills needed to identify and implement a plan.

There's no doubt that backup has historically been a hassle. As an organization grows and uses more applications, managing backup becomes increasingly complex and time-consuming. The cost of equipment or solutions can be prohibitive. Many small businesses are simply overwhelmed, with limited resources to manage and maintain backup applications, software, and hardware on an ongoing basis.

## The costs

However, the cost of doing nothing is sizable. From the complete inability to conduct business to loss of customer trust and reputation, system outages and data loss incidents are clearly costing SMBs. Impacts include:

***It's expensive.*** A system outage costs SMBs an average of $12,500 per day. In addition, the act of losing customer data can have financial impacts. For example, the Payment Card Industry's Data Security Standard (PCI DSS) mandates fines of up to $25,000 for minor violations, up to $500,000 for more serious violations, and possible loss of credit card processing authorization.*

***Customers leave.*** Many data protection regulations include disclosure and notification requirements. When sensitive data is lost or stolen, potential victims must be informed so they can take steps to protect themselves from identity theft. Therefore, businesses that lose their customer's personal information risk public embarrassment that can permanently damage their reputation and cost them customers.

***Business continuity is lost***. The most significant problem, however, is not being able to conduct business at all. Businesses today are heavily reliant upon smoothly operating IT systems and, perhaps more importantly, the data they interact with. According to the Symantec study, outages lead to an average of 54 percent of customers switching vendors because of unreliable computing systems. For many businesses, a

1- http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=dpsurvey

disaster could put them out of business permanently. Businesses must do their utmost to ensure the continued operation of their systems and the ability to rapidly recover data in the event of a disaster.*

## SMBs don't act until it's too late

Although 65 percent of SMBs reside in regions that they consider susceptible to natural disasters, they don't have plans to help them keep their computer systems up and running in the face of such a disaster. In fact, these companies experienced an average of six outages in the past year.

Of SMBs that *do* currently have a disaster preparedness plan, half implemented their plan only *after* an outage or loss of data. The top three culprits listed were cyber attacks, power outages, and natural disasters, however, common causes of data loss also include more mundane events such as coffee spilled on a laptop, machines dropped on concrete pavement, and accidental file deletion. It's critical for SMBs to act *before* disaster occurs to protect their data.

## The solution: cloud-based or hybrid backup

It's abundantly clear that SMBs can't afford to wait to figure out what to do. They must begin mapping out a data recovery plan now, before the fact. The good news is, backup doesn't have to be overwhelming and can in fact be rather simple. New hybrid solutions offer the option to back up solely to the cloud, or both on-premise **and** to the cloud depending on the company's needs. Hybrid backup is a compelling alternative to on-premise solutions, allowing a company to replace expensive backup hardware, software, and personnel with a subscription-based service. With no hardware or software to deploy or manage and no need to hire dedicated resources, hybrid backup is quick and easy to set up. Since data is backed up to local servers and then automatically stored to remote computers in the cloud, it is continuously protected in case of a local disaster such as fire or flood. The solution even offers self-service retrieval, enabling employees to restore their own lost data as needed.

Small businesses may prefer solely cloud-based backup initially. As they grow, they may opt for the hybrid option that continuously protects their data by backing up to local servers which then automatically transmit the data to the cloud. This option provides the best of both worlds, with fast backups and retrievals from a local server and the assurance of an offsite copy in the event of a local disaster.

**Backup directly  to the cloud, or via a hybrid solution that backs up both on-premise and in the cloud:**

***Ensures consistent, automated backups.*** Hybrid backup solutions are continuous and automatic. The vendor assumes much of the responsibility for the success of backups and restores. Vendors typically offer 24x7 support and provide a Web-based portal to view completed backups and backup version histories, initiate restores, and run reports.

***Secures and protects the company's data.*** Hybrid data recovery solutions back up data both on-premise, if desired, and electronically over the Internet to the vendor's secure data center. Data is encrypted as it's transmitted to the vendor and encrypted again at the vendor's data center for optimal security.

***Simplifies off-site protection.*** Hybrid backup solutions eliminate the need to physically transport tapes or removable external drives. The result is comprehensive protection with no need for a vaulting service and no interaction with physical media that can fail.

***Protects remote branch offices and mobile workers.*** Many remote and branch offices have limited or no backup in place, or no way to monitor backups to make sure they are occurring. Mobile workers are also often at increased risk for lost or stolen laptops. Hybrid backup solutions allow traveling employees to back up directly to the cloud, after which time the solution automatically synchronizes the changes back to the local storage server, ensuring company data resides both in the cloud and on the server.

***Is fast and easy.*** Cloud-based and hybrid backup is continuous and automatic, reducing the demands for a committed resource to manage them. The hybrid option protects critical data by backing up to local servers providing fast backups and retrievals and automatically transmitting data to the cloud, freeing up the network at high-use times to reduce impact. Vendors that provide block level or incremental backup after the initial backup help to further speed and simplify the process by running the service in the background and copying only items that have changed.

***Predictable costs.*** Flexible subscription-based pricing allows businesses to use only the data protection needed with no per-user licensing fees. Customers have regular, predictable costs and can easily add more storage capacity when needed.

***Increases business focus.*** A common complaint from small business owners is that they have no time to think about how to grow their business or further leverage technology to boost profits, revenue, and productivity. With no need to worry about managing data protection and recovery, business owners are free to focus on the core business. In the event of a failure, downtime is minimized, and users can recover files themselves.

## Conclusion

Small and medium-size businesses are increasingly turning to solutions either fully or partially in the cloud to protect their data in case of a severe computer or network outage. Today, hybrid solutions exist that offer cloud-only backup or a combination of cloud and on-premise backup. Small business owners may choose to back up data solely to the cloud. Medium-sized businesses or those with increasingly reliance on large data files may prefer a hybrid option that backs up data onsite **and** to the cloud, ensuring fast backups and retrievals and an offsite copy. The hybrid option protects critical data by backing up to local servers, providing fast backups and retrievals and automatically transmitting the data to the cloud, ensuring company data resides both in the cloud and on the server. In the event of hardware failure, natural disaster, or accidental file deletion, critical data can be restored locally or from the cloud, as needed.

With the promise of significant cost savings, flexible options designed for agility, and a workforce that is free to focus on the company's core offering, it's no surprise that small and medium-size businesses are leading the charge to leverage the cloud for all or part of their data protection strategy. Symantec Backup Exec.cloud™ provides essential disaster recovery and backup protection for small and medium-size businesses that require comprehensive and dependable backup. Either to the cloud or via the hybrid option onsite **and** to the cloud, business owners will rest assured that critical data can be restored locally or from the cloud, as needed.

*According to the Symantec 2011 Disaster Preparedness Study

**About Symantec**

Symantec protects the world's information, and is a global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com