WHITE PAPER:
WHEN GOOD BACKUPS GO BAD

When Good Backups Go Bad: Data Recovery Failures and What to Do About Them

Who should read this paper

A Small or Medium Business Owner or IT Manager

When Good Backups Go Bad: Data Recovery Failures and What to Do About Them

Content

Introduction

It's no news that the world has changed. Business transactions are faster and have a broader reach to more people in more countries than ever before. Businesses of all sizes can cast a global shadow by setting up a website and conducting business over the Internet. The key byproduct of all this change is explosive amounts of data in the form of email, customer information, and business transactions. According to Gartner, data growth is IT's biggest challenge, with data capacity growing at an average of 40 to 60 percent year after year.[1] At the same time the volume of data is growing, so are the threats.

Many people still believe cyber attacks are the main culprit for data loss, however, you don't have to be the target of a virus or a worm to lose data. Natural and man-made disasters wreak havoc on large and small businesses alike. Sixty-five percent of small and midsize businesses (SMBs) of 25 to 500 employees operate in regions susceptible to natural disasters.[2] Add to that power outages, employee errors, and failed system upgrades, and it is estimated that SMBs experienced a median of six outages per company in 2010.[3] With fewer resources on-hand to perform critical business functions, many SMBs cannot recover and ultimately fail in the wake of a disaster.

Successfully backing up critical systems and data is key to disaster recovery and business continuity. Yet, Symantec's 2011 SMB Disaster Preparedness Survey revealed that only half of the respondents have appropriate backup and data recovery plans in place.[4] Why? Some companies just haven't gotten around to it, others are in a state of paralysis trying to figure out what to do, and others have a plethora of solutions in place that work at cross-purposes but fail to consistently back up crucial data. If you've chosen a backup solution, and are now trying to decide which deployment option makes sense, read the white paper, "Software, Cloud, or Appliance? How to Decide Which Backup Option Is Best for You."

What happened to my data?

As you try to restore a critical backup, is there a more unnerving question than, "What happened to my data?" Below are some reasons businesses face more downtime and data loss than is necessary.

The data was never backed up—The easiest data failure to diagnose is the fact that a specific piece of data was not backed up at all. According to Symantec's 2011 SMB Disaster Preparedness Survey, only half back up at least 60 percent of their data, meaning they would lose 40 percent of their data in the event of a disaster. In addition, organizations often fail to back up corporate PCs and other key data, or take an "all or nothing" approach if it can't be all-inclusive. For example, of those surveyed, 31 percent don't back up email, 21 percent don't back up application data, and 17 percent don't back up customer data. It's difficult to quantify the exact value of lost data, but the cost is significant. Think about lost invoices for goods or services, records of funds owed to the company, or lost details on every customer and supplier, and you begin to get the picture. How much would it cost to manually recreate every piece of data lost? How long can your business survive without it? Ultimately, you can't restore what you haven't backed up.[5]

Failing to protect remote offices—Critical corporate data in remote or branch offices require the same protection as data within the data center and is subject to the same compliance regulations. Yet, often IT doesn't know whether remote site backups are performed regularly, are successfully completed, or in the case of tape backups, whether tapes are regularly taken off-site. In addition, limited IT staff at the remote office makes it difficult to manage backups, let alone troubleshoot failed backup and data recovery. As data at the edge of your infrastructure grows, your legacy backup solution becomes less effective, leaving data unprotected, threatening business continuity, and

1-http://www.computerworld.com/s/article/9194283/Data_growth_remains_IT_s_biggest_challenge_Gartner_says
2-http://www.pcmag.com/encyclopedia_term/0,2542,t=SMB&i=51543,00.asp
3-Small Business IT Survival Tips for Dummies, June 2011
4-http://www.symantec.com/content/en/us/about/media/pdfs/symc_2011_SMB_DP_Survey_Report_Global.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Jan_worldwide_dpsurvey
5-Ibid.

increasing the management burden on your remote teams. Remote office backup is a significant risk exposure for businesses today, and many are seeking to consolidate this process.

Inconsistent backup—According to Symantec's 2011 SMB Disaster Preparedness Survey, less than half of the companies surveyed back up their data at least once a week, and only 23 percent back up daily.[6] Regular and automated backup should be an essential IT operation. As outlined above, IT outages and data loss can occur at any time as a result of hardware failure, human error, natural disaster, or improper security processes. Often, the most crucial data to an individual is the project on which they are currently working. As materials age, they tend to be less relevant. Regular and frequent backups are necessary to restore data and resume critical business operations in the event that data is lost, destroyed, or corrupted.

Different solutions from different vendors—Even when you remember to back up your data, include your remote locations, and conduct backups regularly, you can still experience backup failure. According to Enterprise Security Group, even with all the advancements in storage technology, only about 20 percent of backup jobs are successful.[7]The reason for this is "complexity" resulting from a plethora of competing technologies. If companies could start over, they could enjoy solid, stable, and reliable backups using sophisticated new storage solutions and standardizing on one vendor. The problem is that newly created data is accruing at breakneck speed, while emerging regulations continue to mandate changes in how data should be retained. Since it's unrealistic for most companies to start with a new solution from scratch, they tend to add storage in stages, introducing new solutions from different vendors on an ad hoc basis, thereby complicating storage and causing backup problems.

New York City-based Fourth Wall Restaurants manages six upscale restaurants in Manhattan. According to Sumeet Lakhaney, Fourth Wall's IT Director, the company's nightly backups took up to eight hours to complete their run. But, with a Symantec solution that includes deduplication, Fourth Wall is able to reduce the amount of data going to storage and have a time-efficient backup. Using Symantec™ Backup Exec, Fourth Wall trimmed their backup times from up to eight hours down to as little as two hours per night, saving 20 hours per week that they could then devote to the business.

Media failures—Tape and disk-dependent approaches that rely on media with a limited life can introduce risks to businesses. For example, many companies store magnetic tape media improperly, leading to tapes that become damaged and unreadable. Lost or stolen media can expose companies to legal risks, data loss, or damages to the corporate brand if the loss becomes public. Backups are only as good as their ability to recover and restore the information, systems, and applications they contain.

Poor processes—Poor IT practices can lead to backup failures. For example, it is not uncommon for companies to lose track of the software with which backups were created, making the data essentially unretrievable. Or a software environment that formerly supported an application is no longer available, making a successful restore impossible. In another case, companies often change their IT infrastructure but not their backup procedures. So they may be pointing their backup to something that is no longer exists or has changed, therefore not backing up what they think they are backing up. However, one of the main challenges is not testing their recovery plans. It's not enough to *think* you're protected—have you tested the plan? Does it meet your recovery objectives?

6-http://www.symantec.com/content/en/us/about/media/pdfs/symc_2011_SMB_DP_Survey_Report_Global.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Jan_worldwide_dpsurvey
7-http://www.krollontrack.com/data-recovery/complexity-storage-systems/

Repercussions of poor or failed backups

Aside from the very real costs of having to redo work and the negative impact on employee morale resulting from unavailable systems, backup and data recovery failures can result in:

Financial impact—In today's regulatory climate, all companies doing business are affected by government and industry regulations concerning data security and privacy. In addition to hundreds of regulations mandating information security and data protection standards, local, state, federal, country, and even regional (for example, the European Union) requirements must also be met. Losing customer data is treated as a serious transgression. 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 possibly loss of your credit card processing authorization.[8]

Damage to reputation—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 customers' personal information risk public embarrassment that can permanently damage their reputation and cost them customers. According to the Symantec study, outages lead to an average of 54 percent of customers switching vendors because of "unreliable computing systems."[9] For many businesses, a disaster could put them out of business permanently.

Loss of business continuity—The most significant problem is loss of business continuity, or not being able to conduct business at all. Businesses today are heavily reliant upon smoothly operating IT systems. Therefore, protecting data is paramount. It is critical to ensure the continued operation of your systems or the rapid recovery of those systems and data. How long can you afford to have your systems down? How important is your data? Can your business function if it loses its IT infrastructure and data? On February 27, 2011, a software bug on Gmail™ caused 120,000 users to lose all of their emails. Fortunately, the messages were successfully restored from tape backups just hours after the event.[10]

Back up with confidence

The good news is that leading vendors are transforming the backup market with comprehensive and flexible recovery management solutions that significantly alleviate data protection challenges. Symantec offers fast, easy, and modern backup solutions that can be consumed as software, as a cloud service or as an appliance, that offers protection for physical and virtual environments without sacrificing choice. These new tools help control rampant data growth and simplify virtual protection, allowing companies to deploy a modern infrastructure that best suits their needs and that can grow with them. When looking at backup solutions, we recommend you look for those that:

HVAC, plumbing, and electrical services provider, Service Today differentiates itself from competitors by giving employees access to information they need to optimally serve their customers. Monnen Technology, which provides outsourced IT services for Service Today, uses data protection, disaster recovery, and endpoint and messaging security solutions from Symantec to safeguard employees' access to business-critical data. Results include a recovery point objective of 20 minutes and 99 percent of spam filtered at the mail server. Since first deploying Backup Exec, Service Today has upgraded to new versions of the product as they were released. Today, the company uses Symantec™ Backup Exec 2010 to back up 277 GB of data across six servers, including its Microsoft® Exchange-based server. It performs a full backup to tape on a nightly basis and runs a full backup to disk every 20 minutes.

8-http://www.krollontrack.com/data-recovery/complexity-storage-systems/
9-Symantec Disaster Preparedness Study, January 2011
10-http://www.eweek.com/c/a/Messaging-and-Collaboration/Google-Suffers-First-Gmail-Outage-of-2011-850632/

Modernize your infrastructure—As you invest in server refresh or data center expansion, you have an opportunity to update your data protection infrastructure. Modernization includes better protection of virtual machines (VM), more use of disk and cloud as backup targets, and the use of innovative data reduction technologies such as data deduplication and archiving. Ultimately, you can shorten backup windows and reduce risks with new features that modernize backup.

Simplify backup—Reduce the time-consuming, manual process of implementing a custom backup infrastructure, and obtain "all-in-one" versatility with one vendor, one license, and one support contract. Today's backup vendors offer an integrated form factor and wizard to simplify configuration and initial setup. Web-based administration allows status and management to take place from any location. Look for solutions that offer deduplication, virtualization, and archiving, as these features all simplify backup.

Backup versatility—Whether you choose a backup appliance, backup to the cloud, or software-based backup, a modern solution likely exists that fits your needs. For more on how to decide which option is right for you, read the white paper, "Software, Cloud, or Appliance? How to Decide Which Backup Option Is Best for You." Purpose-built backup appliances pre-loaded with powerful software are secure and easy to manage. The appliance form factor assures a consistent technology deployed across an organization, allowing administrators to manage their information from a data center, by a channel partner, or from other remote locations for reliable off-site recovery. As an added plus, appliances and cloud options are often quite cost-effective. Many SMBs are considering an online backup service to either supplement or replace their current process. These solutions have traditionally been called backup Software-as-a-Service (SaaS), but they're increasingly known as online backup or cloud backup. Since cloud-based services are off-site at all times, they reduce hardware and maintenance while providing additional protection in case your place of business is affected. Software offers sophisticated backup and recovery for companies that have already made investments in hardware and infrastructure on which to run the software.

Allow you to virtualize confidently—As you move to the virtual environment, you need assurance that you can recover virtual applications and data when necessary, while still protecting your existing physical systems. Solutions on the market today offer visibility into backups to help you remove duplicate data and control storage costs. Modern backup solutions protect virtual servers by providing granular object recovery from a single-pass backup of an application or VM, dynamic inclusion of new VMs, and deduplication across physical and virtual environments, allowing businesses to fully realize the benefits of virtualization.

Manage storage—As your data grows, backup windows are at risk of not being completed, and management costs climb. Your backup vendor can help you identify locations to reduce unnecessary data, thereby saving time and money. By implementing data deduplication broadly in conjunction with integrated archiving for better storage management, you can successfully manage your data to help you reduce your storage costs and more effectively search and recover older data while you establish proper data retention policies for your business.

Conclusion

Backup is more crucial than ever. Whether you want to manage your own backup policy or outsource it to an reseller or technical consultant, there are new backup solutions that are flexible, easy to manage, and available on the market today. Symantec's award-winning backup and recovery products deliver reliable data protection for growing businesses in both physical and virtual environments. There is no reason to let your business fall victim to downtime because of a computer or system failure. Keep your systems and data safe and retrievable with a tested recovery solution in the event of a natural or man-made disaster.

Symantec helps SMBs protect more, store less, and save money with data protection solutions designed for growing businesses. To learn more, visit us at www.symantec.com.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

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

Symantec helps organizations secure and manage their information-driven world with **data backup and recovery software**.

10/2011 21205744