LiveVault
a j2 Global Company

Whitepaper

Is Your Critical Business Data Safe?

Table of Contents

Overview

Data loss is inevitable. In 2014, 64 percent of businesses suffered from data loss or unplanned downtime.[1] Anything from accidentally overwritten data to a natural disaster can negatively impact your data. However, a consistent, reliable and comprehensive backup process can mitigate the most severe results of data loss, including financial calamity. Data loss and downtime combined cost businesses worldwide $1.7 trillion in 2014 alone.[2]

Many small-to-midsized businesses (SMB) lack adequate data backup and recovery programs – 74 percent of SMBs reported having no disaster recovery plan at all, and 71 percent are not fully confident that they can restore data from the backups they do have.[3] Does your business have a disaster recovery plan in place to respond to data loss, regulatory mandate or an eDiscovery request?

The LiveVault® eGuide offers best practices for testing your data recovery capabilities and provides guidance on implementing a cost-effective data protection policy that will enable your business to recover quickly in the event of critical data loss.

How Data Loss Occurs

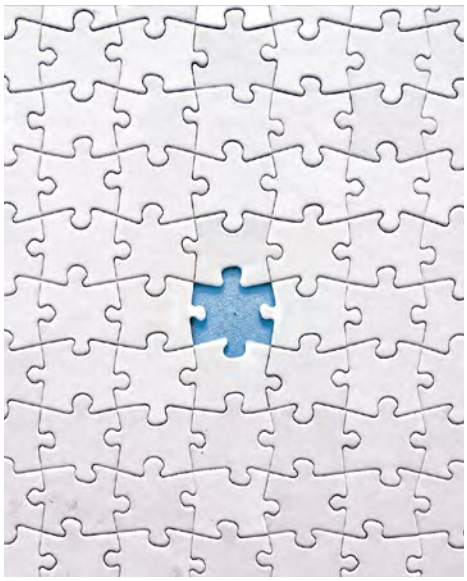
Though many SMBs have cloud-based data storage systems, they fail to identify gaps in their data protection strategies – often leading to permanent data loss. The following are the most common – and often avoidable – reasons for data loss and downtime.

The data was never backed up to begin with

The single biggest driver of permanent data loss is, quite simply, that data was never backed up in the first place. Half of SMBs back up less than 60 percent of their data, leaving the remaining data vulnerable to loss at any time. Sixteen percent of SMBs never backup PCs and laptops and many more fail to execute backups at remote offices or for mobile employees. Some SMBs fail to recognize email and other databases as “critical” and choose not to regularly perform backups. Having a backup system is not enough. Without a backup strategy, data loss will occur.

The data recovery process fails

While most SMBs have a data backup system, those systems – for various reasons – sometimes fail. Without regular testing, it is impossible to determine the effectiveness of your data protection process. All too often, businesses are unaware that their backups are incomplete – or outright failing – until the time comes to attempt a restore operation under pressure. 23 percent of SMBs lack a remote backup strategy, leaving their entire corporate data store vulnerable to disaster. Similarly, 42 percent of SMBs have no automated backup program. Instead, they rely on failure-prone manual backup technologies like tape or disk.



Backup media are damaged, corrupted or missing

Unreliable backup processes and unreliable media are a significant cause of data recovery failures. Outdated hardware media, like tape and disk, have a limited shelf life and can easily fail if improperly stored or dropped. Hardware storage is also vulnerable to misplacement, loss or theft. Recovery from tape backups is notoriously failure-prone, with various sources estimating failure rates from 10 percent to more than 50 percent. While many SMBs have moved backups to the cloud, substantial reliance on outdated hardware remains a driver of data loss.

IT complexities

IT infrastructure continuously changes. Failure to adjust backup strategies to keep pace with these changes can leave data exposed to damage or loss. System-level restores will fail if the server's system data is not also backed up and restorable. In general, complex backup systems that rely on manual methods, legacy technology and/or components from multiple vendors are much more likely to fail than an up-to date, cloud-based system from a single, reputable provider. Businesses with multiple vendors are more likely to suffer data loss (38 percent) than those who used a single vendor (24 percent).[4]

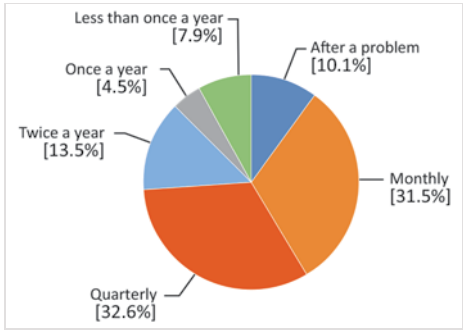


Fig. 1: *How often do SMBs test their backup procedures?*

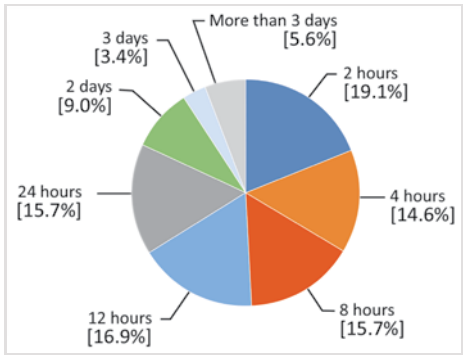


Fig. 2: *How quickly can SMBs restore the "missioncritical" applications and data necessary to run the business after a major loss caused by a disaster?*

Natural and man-made disasters

While natural disasters are the most dramatic and potentially devastating cause of data loss and business system downtime, they represent only 10 percent of severe data loss events. Human error, on the other hand, represents 60 percent of downtime and data loss – more than any other factor. System downtime remains a significant problem worldwide, with 86 percent of organizations experiencing one or more downtime events annually, lasting 2.2 days on average.

Flawed protection strategy and lack of testing

Increasing exposure risks to internal and external data combined with stronger regulatory enforcement have made data security the top priority for IT organizations year after year. Despite the increasing awareness of these risks – 80 percent of US businesses view data protection as critical.[5] Failure to test the viability of backup and recovery processes continues to be a major cause of data recovery failures.

According to research from Storage Strategies NOW, 7.9 percent of SMBs test their backup procedures less than once a year, 4.5 percent test only once annually and 10.1 percent test only "after a problem" (see Fig. 1). Failure to test backup procedures on a consistent basis significantly reduces the effectiveness of backup strategies for SMBs.

This lack of testing procedures is perhaps a contributing factor in the low confidence SMBs have in their data recovery capabilities. Almost 25 percent are only "somewhat confident" (the lowest confidence level in the survey) in their ability to restore lost data and more than 20 percent have no disaster recovery plan at all. In the event of data loss or system downtime, 29 percent of businesses report that it would take them one day or more (see Fig. 2) to restore data and mission critical functionality – causing significant financial impact.

Improving the Odds With Cloud-Based Data Backup

Moving away from legacy systems and hardware backups to Cloud-based backup services is a simple, versatile and cost-effective option for SMBs to significantly reduce the business and financial risks posed by data loss. Cloud backup provides a "second tier" of data protection by storing data offsite, eliminating the risk of natural disaster, theft or misplacement.

The vast majority of SMBs worldwide are already leveraging cloud backup services. Organizations that moved at least part of their data storage to the cloud reported a recovering from downtime rate almost four times faster (2.1 hours versus 8 hours on average) than those without cloud storage.

Many SMBs that utilize cloud backup services continue to protect data locally as well, as locally stored data can be recovered faster – especially in large volume. Cloud backup though, remains key to a best-practice data protection strategy for subsets of applications, files and databases that demand extra protection against deletion or corruption.

Testing Your Data Recovery Capabilities

Performing regular tests on your data recovery capabilities is the only way to identify gaps in your data protection process before they impact your business – and to ensure your data is secure and accessible when needed. Regular testing is essential to a comprehensive data protection policy.

LiveVault recommends testing at least quarterly – especially for the most critical data. Businesses should also define recovery time objectives (RTOs) for each class of critical data, and test to ensure those objectives are met.

Conclusion

Data loss is inevitable – but it doesn't have to derail your business. A well-defined, comprehensive and regularly tested data protection strategy is essential to minimize downtime and financial impacts from data loss.

LiveVault – a leading cloud backup provider focused on the needs of SMBs – will help you identify and address gaps in your data protection policy. LiveVault offers free local onsite backup options, along with leading-edge compression and encryption technology to accelerate the recovery of your data from the cloud if necessary.

For more information, visit www.livevault.com.

Resources

1. EMC Global Data Protection Index, 2014
http://www.emc.com/collateral/presentation/emc-dpi-key-findings-global.pdf
2. Ibid
3. Ibid
4. Ibid
5. Ibid

About LiveVault

LiveVault® is the turnkey, fully managed cloud server backup and disaster recovery service of choice for thousands of enterprise customers worldwide. With more than 16 years of experience in SaaS data protection, LiveVault is a leader in streamlining and reducing the costs and complexities of companies' data security. LiveVault's 24/7 actively monitored, unified solution includes advanced systems for open file backup and offsite data mirroring, flexible long-term retention, legal hold support, and disaster recovery in the cloud. Learn more at www.livevault.com.

Worldwide Headquarters
j2 Global, Inc.
6922 Hollywood Blvd.
Hollywood, CA 90028

Contact US Sales 1-844-LIVE-VLT
email us at: LVsupport@livevault.com

www.livevault.com