STORAGECRAFT.

Backup Fast, Recover Faster

Building Your Backup and Disaster Recovery Plan

101

Abstract

Small and medium businesses cannot afford to lose access for their data. Research shows that even brief server failures lead most smaller businesses to shut their doors for good. In light of this, any business should develop a workable backup and disaster recovery plan. Until recently, however, this was difficult since most backup and disaster recovery solutions were aimed at large enterprise. Today, the environment is changing. Protecting data is becoming more and more important and new technologies are making backup and recovery strategies more viable to smaller businesses.

Contents

STORAGECRAFT®

Building Your Backup and Disaster Recovery Plan

101

Most businesses today must run 24/7; there's no room for downtime. In the globalized economy, operating in failsafe mode is imperative because, let's be honest: lost data of any kind—email, corporate financials, archived and updated legal proceedings, payroll records, databases and so on—can cost a business not only time and money, but rob it of its future altogether.

A recent study highlights the stakes: "Of companies experiencing a 'major loss' of computer records, 43 percent never reopened, 51 percent closed within two years of the loss, and a mere 6 percent survived over the long-term"[1]

Of course, there's no telling how or when that "major loss" will occur, but when it comes, the small and medium-sized businesses (SMBs) that survive are the ones that are prepared. They have a comprehensive backup and disaster recovery (BDR) solution in place that includes the reliable, efficient and daily backup of essential information, as well as a clear plan for recovering that

1. Cummings, Maeve; Haag, Stephen; and McCubbrey, Donald. 2005. *Management information systems for the information age.* http://highered.mcgraw-hill.com/sites/0072935863/information_center_view0/.

information. IT managers can't afford to be caught with their pants down. Now is the time to create an effective BDR plan or review one already in place before disaster strikes.

Determine your need

Backup and disaster recovery is essential for SMB survival, but without a solid and realistic BDR plan, it can be a time-consuming, frustrating and damaging process. Unfortunately, there's little or no direction available for small businesses, a fact which often leads to additional problems. For example, small businesses frequently don't realize that they may be violating the law when they fail to put a BDR plan in place.[2] Most don't know or understand the regulations and requirements of their own industries.

Of course, in order to understand the true necessity of a solid BDR plan, IT managers should recognize all the implications of data loss for their business. There's more to it than simply saying data loss equals business death and without a comprehensive view of what's at stake, business owners and operators will struggle to be as prepared as they should be.

Not all these issues are addressed directly in this white paper, but IT managers and business owners who are not convinced of the need for a stable BDR plan or who are unsure of the

2. The Sarbannes-Oxley Act of 2002, for example.

STORAGECRAFT.

effectiveness of the plan they have in place should consider the following questions:

- If you lose data, can you recover it and if so, how easy will it be to access?

- How long can you operate without access to your data or systems?

- How reliable are your current data backup procedures (if any)?

- How much time and money will it take to recover your data without a BDR plan in place (or with your current plan)?

- What data are you legally required to back up (health records, court records, etc.) and what are the legal ramifications of losing that data?

- What are the potential hazards to your data, such as floods, earthquakes, malicious attack, operator error and so on?

- What operating procedures put your data at risk and how can you reduce them?

- Is your data secure and encrypted, especially if you are backing up over a network or to the cloud?

- Do you know the best available technologies for executing an effective BDR plan?

- What resources do you have available for a BDR plan (i.e. budget, servers, network resources, personnel, etc.)?

- What available solutions meet your resource constraints?

- In the case of a recovery, does your BDR plan account for deploying data and backup files across multiple devices?

- Are you prepared to aggregate and integrate both recent and historical data?

The answers to these questions can help establish the need for a new (or improved) BDR plan and as they demonstrate, knowledge about available BDR technologies is crucial. The rest of this paper, then, will focus on the core of any solid BDR plan: the backup and recovery of data.

Know the facts

In the past, IT specialists and BDR service providers focused mainly on backup and recovery options for large enterprises. Today, however, the real need for similar solutions for SMBs, along with innovative new technologies, has inspired a revolution.

The SMB BDR Environment

A recent study conducted by the Enterprise Storage Group (ESG) and examining the unique BDR needs of small businesses paints a good picture of the current SMB environment. The respondents

STORAGECRAFT.

(who were storage and IT professionals and who are outlined in figure 1) cover a wide variety of industries and business sizes, allowing for an analysis of the field that is both deep and broad.

Target respondents	Storage and IT professionals from SMB organizations. For this survey, SMB is defined as those organizations with less than $500m in annual revenue.
Sample size	N=186
Respondents by company revenue	61% with revenue of less than $50m 25% with revenue between $50m and $249m 14% with revenue between $250m and $499m
Industry distribution	More than 20 different industries represented including , Banking, Biotech/Life Sciences, Construction & Engineering, Consulting/Business Services, Consumer Goods, Education, Electronics, Financial Services, Government, Healthcare, Hospitality & Travel, Information Technology, Insurance, Manufacturing, Media & Entertainment, Pharmaceuticals, Retail/Wholesale, Telecommunications, Transportation & Logistics, and Utilities

Figure 1: Demographics of the ESG study (see note 3).

In reviewing the data, author John McKnight identifies a three-fold pattern that defines the BDR requirements of SMBs:[3]

1. Data is growing 25 percent annually, due in part to the replacement of paper systems with digital processes.

2. Fifty-two percent of respondents indicated that their business could only handle a maximum of four hours of downtime before feeling a significant impact, powerfully underscoring the need for reliable backup and recovery (see figure 2 on page 10).

3. McKnight, John; 2004. "New Requirements and Systemic Challenges Open the Door for On-line Backup Service Providers." http://www.keysolution.com/ESGResearch.pdf
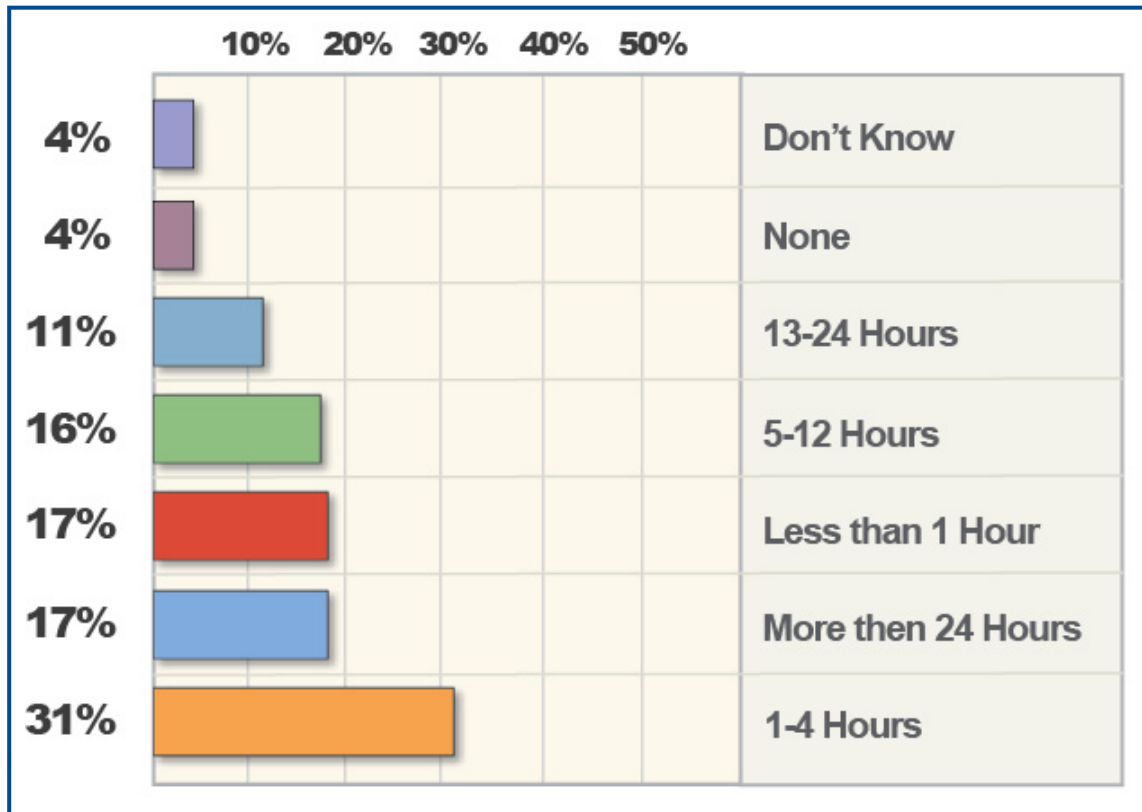
STORAGECRAFT.

Figure 2: SMB ability to tolerate downtime before loss, adapted from the ESG paper (see note 4).

3. Eighty percent of SMBs run backups nightly; 84 percent backup once per week. Even so, 38 percent of these businesses don't think their solution is complete or even "adequate." They continue these practices, however, largely because they fear the perceived complexity and cost of new technologies and thus the expertise and resources needed to upgrade.[4]

These fears, however, are unfounded. In fact, many new technologies and virtual processes currently available make it possible for SMBs to migrate their data into more secure systems quickly,

4. Ibid.

easily and in some cases, automatically. In addition, these technologies allow businesses to recover their data faster and with greater accuracy. There is no excuse in today's environment for businesses to rely on antiquated processes. Again, knowledge is the watchword.

Backup, Storage and Recovery Media

Data is valuable and so it's no wonder that the evolution of storage media has been stubborn. No one wants his or her business-critical data stored on a new, untried medium. In the end, however, technological development has allowed IT professionals to adopt the media that best meets their needs.

Initially, tapes were the media of choice. Even today, many businesses rely on this old workhorse of storage. Tapes, however, are unwieldy in a recovery scenario and ultimately unreliable. With a failure rate exceeding 70 percent for data restorations from delicate tape systems, the standard BDR media gradually became disk arrays.

More recently, however, flexible cloud storage and responsive virtual servers have emerged as the new, high-speed contenders in the BDR space. This option brings significant advantages such as scalability and restoration speed to a BDR plan.

Tape backup. High failure rates, high degradation and resistance to encryption limit the usefulness of tapes. Even with the

STORAGECRAFT.

evolution of virtual tape libraries, they are a slow method of disaster recovery, which makes them difficult to retrieve information from and unreliable over time. Tapes are really only suitable for off-site vaulting, long-term data archiving and other related uses.

Disk arrays. The current standard backup choice, disk arrays offer a reliable solution that tapes cannot match. Backup techniques like disk-to-disk snapshots, storage tiers, replication and RAID-6/DP shorten backup times, enable more optimal recovery point objectives (RPO) and help businesses realize their ideal recovery time objective (RTO). Additional technologies can make disk arrays even more effective, such as using ultra-reliable fiber-channel style drives for the array.[5]

Cloud backup. The emerging backup method of choice is the "virtual cloud," where data is stored offsite, frequently with services that provide BDR features not normally available to businesses using traditional disk arrays. The development of cloud backup, which itself has been made possible by increasing transfer speeds and faster, better disk arrays, has also paved the way for a number of other useful technologies. Cloud backup allows for automated recovery and verification and even the use of virtual servers or machines (VMs) operating on demand. These VMs (sometimes called cloud servers) are dynamically scaled in real-time and are available in multiple OS configurations. Consequently, these virtual machines can act as storage, integrate with

5. SearchDataBackup.com, 2011. "Enterprise-class disk array purchase considerations." http://searchdatabackup.techtarget.com/tutorial/Enterprise-class-disk-array-purchase-considerations

STORAGECRAFT.

other backup options—such as hard disk arrays as when using network attached storage (NAS)—or operate wholly on their own as a remote server. Overall, these virtual servers offer superior response times to traditional disk-based solutions when retrieving assets and data.

Backup, Storage and Restore Strategies

Of course, BDR technology (such as the media options described above) is at the foundation of any good plan and as technology evolves, the options for backup, storage and restoration continually improve. The following backup, storage, and recovery strategies take advantage of the current technological milieu. They often overlap in their execution and can certainly be used in conjunction with each other.

Disk imaging.   Imaging allows a business (or individual) to back up complex and large amounts of server data. Initially, the backup software creates a baseline image of the hard drive. The image is then continually updated using block-level imaging— that is, the software takes continuous "snapshots" of the drive. The software then compares the snapshots and updates the differences. Events are "folded" into only the real-time data to conserve space. Maintaining the image using block-level imaging means that the most recent version of the server is always available—even instantly if need be.

STORAGECRAFT

The result is that administrators can restore their server, or even individual files, to a state at any point in time. Disk imaging also offers significant management overhead and disk space cost savings.

Bare-metal restore. This type of data BDR allows an IT manager to restore a system from the "bare metal," or, in other words, without the need for anything like an operating system or drivers.

Backed-up data includes not only the content, but the applications, the OS, and all the drivers and system data required to enable a new device as well. Some bare-metal recoveries require identical hardware, but virtualization can support hardware-agnostic, bare-metal restores by retrieving drivers and other hardware-specific elements on the fly.

Bare-metal restores are usually pulled from disk images and can be executed from network or virtual machines.

Virtualization. Virtualization is quickly becoming the BDR method of choice in the current, booming information age. When used in conjunction with strategies like disk imagining and bare-metal restoration, virtualization offers an extremely flexible and robust BDR solution. Disk images are digitally transferred to cloud storage or to an enabled virtual server, both of which are usually managed by third party providers. Bare-metal recovery of those files allows complete access to a server in almost any

environment. The allure, then, of virtualized backup and recovery is the ability to recover an entire machine or system—or even run the duped server on a VM from the cloud—in mere minutes following a disaster or failure. This ability to continuously back up your data to a virtual machine and run it from the cloud has made recovery from zero-to-functional a reality and the baseline standard in many business environments.

Build your BDR plan

Knowing the technology and strategies is only part of the game, however. A successful BDR plan requires forethought, planning and careful execution. The following procedure describes the development of a solid, reliable BDR plan. Visualize the backup, storage and recovery process with a flowchart or other diagram and consider again the questions on pages 7–8. Consider as well creating a cross-functional team that brings to bear a wider array of perspectives and expectations to the development of the plan.

Identify risks. Use a process workflow diagram to carefully identify the risks leading to data loss and the impact of those risks. It's important to examine each process carefully to properly identify all possible risks. Consider process-independent risks as well, such as natural disasters, employee error and malicious intent. Now is the time to assess an ideal RPO and RTO.

STORAGECRAFT.

Determine threat levels. After surveying all possible risks and identifying an RPO and RTO, prioritize the list by identifying the likelihood and severity of each threat. Those risks that have a direct impact on business continuity should be assigned the highest priority.

Develop a flexible BDR strategy. Starting with the highest-priority threats, determine the best, most practical response to each. Be sure to define the infrastructure, technology, legal issues and personnel necessary to implement this response. The sidebar "Developing responses to threats" on page 17 offers two examples.

Document recovery approach. Based on the response plans developed previously, document the necessary steps and dependencies for each response so in the pressure of a disaster, each step of a response is clearly laid out.

Implement BDR plan. Using your plan, assign team members to set the plan in motion, developing the necessary infrastructure, ensuring proper and efficient backups, training personnel on recovery procedures and so on.

The most important part of a BDR plan is preparation. Take the time to consider all potential risks and develop responses so that in the event of a disaster, recovery can be as smooth and painless as possible.

Developing responses to threats

These examples demonstrate how to develop responses to specific risks. These examples are really outlines. A serious BDR plan will include significantly greater depth.

Example 1

RISK: Onsite network and server damaged (multiple potential causes).

IMPACT: Disruption causes a loss of $10,000/hr.; potential violation of contractual obligations to protect data; legal action possible.

THREAT LEVEL: Critical.

RESPONSE: Employ BDR software, pulling data from offsite or virtual storage, cloud retrieval and real-time operation as necessary.

DEPENDENCIES: BDR software and offsite storage network must be in place; IT personnel must be trained in recovery processes.

Example 2

RISK: Workstations offline due to power loss (multiple potential causes).

IMPACT: Orders cannot be fulfilled; shipping slowed.

THREAT LEVEL: Moderate.

RESPONSE: Use backup power supply in call center until main power is restored.

DEPENDENCIES: Functional backup supply; necessary hardware to maintain connection to backup.

Conclusion

As SMBs become more complex in a competitive global environment, data becomes critical to customer service and ultimately, survival. Gone are the days when BDR solutions are only available to big corporations, and IT managers and executives of SMBs need to consider the best ways of protecting their data and their businesses. A crucial part of this consideration is a solid BDR plan that makes use of the best technology available. With data backed up and a plan in place to recover it, businesses can operate in confidence, knowing that they're prepared.

About Us

StorageCraft Technology Corporation provides innovative disaster recovery, system migration, data protection and security solutions for servers, desktops and laptops. StorageCraft delivers software products that reduce downtime, improve security and stability for systems and data and lower the total cost of ownership for servers, desktops and laptops.

Interested in learning more about how StorageCraft and our award-winning backup and disaster recovery software can contribute to your BDR plan? Please contact us:

StorageCraft Technology Corporation

11850 South Election Road, Suite 100
Draper, Utah 84020
U.S.A.
www.storagecraft.com

Email us:
contactus@storagecraft.com
sales@storagecraft.com

STORAGECRAFT.