Acronis

3 Reasons Why Backup is Strategic

This white paper describes the three reasons why backup is a strategic element of your IT plan and why it is critical to your business that you plan and execute a strategy to protect 100 percent of your data.

Table of Contents

Introduction

You are a member of a small IT team working for a medium-size business and a fire destroys your facility including your data center. Unfortunately, you did not have the time and resources to develop and execute a disaster recovery plan. In fact, you had not yet developed and executed a backup strategy to protect most of your systems.

You are not alone. Many SMB organizations do not have effective backup and disaster recovery operations in place. According to the Acronis Disaster Recovery Survey, IDC, May 2014, 70 percent of respondents were not fully confident on the statement, “Our backup and disaster recovery operations are well managed and planned.”

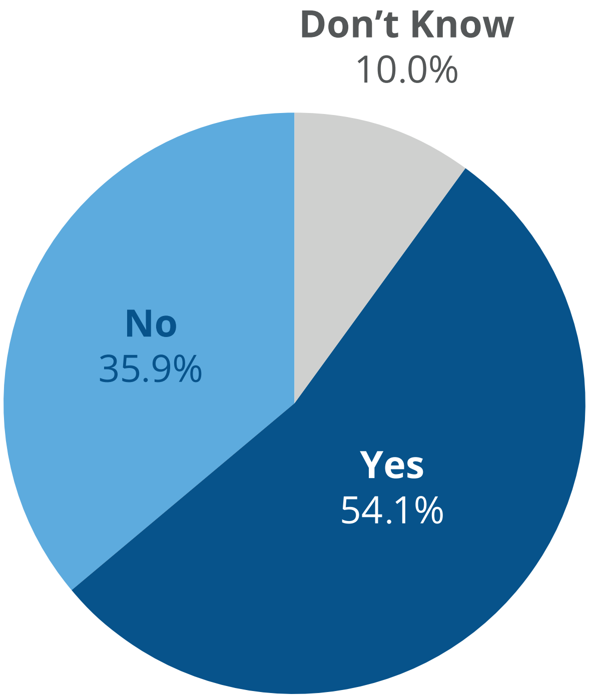
Backup is **strategic** to your **business** because your **data is strategic** to your **business**

However, now that your data center is destroyed, you feel very alone as you contemplate how to tell your management team that much of the organization’s financial records, billing data, orders in process, customer data, and contracts are lost - permanently.

Considering your organization’s existence is dependent on your backup strategy, why is backup an after-thought in the planning process? You carefully plan, design, and implement your systems and network, but delay the “backup discussion” and implementation:

- Gartner estimates that only 35 percent of small / medium businesses (SMBs) have a comprehensive disaster recovery plan in place.
- Only 2 percent of respondent companies back up 100 percent of their data. (Acronis Disaster Recovery Survey, IDC, May 2014).
- 36 percent of respondent companies admit that they do not back up virtual servers as often as they backup their physical servers. (Acronis Disaster Recovery Survey, IDC, May 2014).

Does your organization back up virtual servers as often as it backs up physical servers?



Source: Acronis Disaster Recovery Survey, IDC, May 2014

Backup is strategic to your business because your data is strategic to your business. Without backup, your business will fail. Backup is your insurance policy and nothing - no other technology or manual process - replaces a backup. Losing it is akin to a retailer or manufacturer losing an inventory that the business did not have time to insure!

This white paper introduces the three reasons why backup is a strategic element of your IT plan and why it is important for you to design and immediately execute a backup strategy to ensure that you protect 100 percent of your data.

#1: Backup is the Only Way to Protect Your Business Data

Life is full of uncertainties and your business is not exempt. A natural disaster such as an earthquake or flood, a man-made incident such as a virus or security breach, even a software or hardware glitch can result in lost data. Data loss occurs more often than people realize or are willing to admit. In fact, it is NOT a question of IF you will experience a data loss but rather WHEN it will happen given the variety of internal and external factors that can affect your systems and data.

The number one reason why backup is strategic is that backup is the only way to protect your critical data. Consider the implications to your business if you lose the data held in your POS, CRM, manufacturing, R&D, and financial systems. At a minimum, loss of irreplaceable data results in lost sales and revenue, contract penalties, potential litigation, non-compliance, and loss of stock value. In the worst cases, loss of data results in bankruptcy.

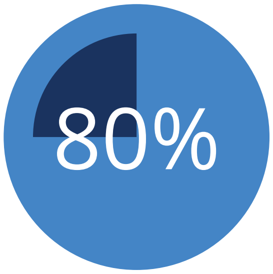
According to the Institute for Business and Home Safety, an estimated 25 percent of businesses do not reopen following a major disaster. Short of a disaster, here are some additional ways data can be lost:

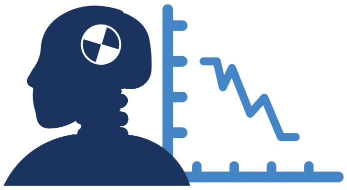
- Every week 140,000 hard drives crash in the United States. (National Archives & Records Administration in Washington)
- 6 percent of all PCs will suffer an episode of data loss in any given year. (The Cost of Lost Data, David. M. Smith)
- 31 percent of PC users have lost all of their files due to events beyond their control.

In order to determine the best backup approach for your organization, you need to understand the value and availability needs of your various data assets and incorporate the results of that analysis into your IT plan.

Not all data is equal in your environment. Some data changes rapidly and is very important to your business. For this data, you should perform frequent backups to make sure you limit the amount of data that you lose. Because this data is more valuable to your business, you should spend more money, devote more resources, and ensure that you can protect and quickly recover 100 percent of this data, or close to it. You should consider implementing a complex backup plan, perhaps performing backups every few hours and prepare those backups so you can recover your systems as a virtual machine (VM) in your primary location or in a remote location.

Other data, while important, does not change as frequently and your organization does not need access to this data immediately. For this data, consider implementing a simpler backup plan; make a copy once a day and store the copy on lower-cost media such as tape or a low-cost, long-term cloud storage option.





Nearly 80% of companies estimate downtime costs them **at least $20,000** per hour or more

Source: Acronis Disaster Recovery Survey, IDC, May 2014

This is a key reason why it is necessary to incorporate backup as a strategic element of your IT plan. By doing so, you can better align your IT architecture and systems to ensure you optimize backup requirements based on the value of the data, the rate at which it changes, and the required time for the business to recover the data.

#2: No Disaster Recovery Plan Works without Backup

Disaster recovery provides business continuity in the event of a disaster or other unforeseen event and consists of a primary and secondary site, either continuously maintained or quickly developed as a standby system. Data, operating systems, applications, files, and folders are replicated and backed up between the sites with the objective to restore your systems to an operational state while minimizing data loss and downtime. Backup is the essential element of an effective DR strategy.

Organizations use many approaches to recover from a system failure or disaster and every one of these relies on backup. For example when a server fails without warning, a failover solution changes a server's workload over to a standby server, system, or network without human intervention. With failover, you need to both replicate the data to the second server and backup the data as well.

High availability provides redundancy so you can minimize or eliminate downtime and ensure that critical systems are always available – not instantaneously but typically within a few minutes. High availability is a single system and contains a single set of data. You may or may not replicate data although you must back it up.

When a disaster strikes, you can recover a system by rebuilding a new system. To accomplish this, you need to either reinstall all the software or copy an image of the old system to the new system. In either case, you need a backup of the data at a minimum.

Migration is the process of moving the operating systems, applications, data, files, folders, etc. to a new (and potentially different) system. There are many reasons why you want to migrate a system including the need to perform maintenance on or upgrade your servers, optimize your system resources, move your physical machines to a virtual environment, replicate servers, recover from a disaster, or modify your IT infrastructure because of a merger, acquisition, or explosive company growth.

There are several different types of migration including data migration, application migration, and cloud migration. To migrate a system, you need to have a backup copy of the data and applications at a minimum.

Failover, high availability, fault tolerant systems, system recovery, and migration are potential elements of a disaster recovery plan when very specific events occur and each method relies on a well-thought approach to backup – an approach you need to plan in advance, not after the fact.

Another important component of your disaster recovery plan is to determine the number of backup copies you need and where these copies reside. Acronis tries to simplify this task and recommends a 3-2-1 backup methodology:

- Maintain all data in three (3) locations: options include production systems, backup on NAS, and backup in the cloud.
- Maintain backup copies on two (2) types of media (disk and cloud).
- Maintain one (1) copy of backup data offsite.

Having an onsite backup copy of your data is effective in the event a primary system experiences a hardware or software failure, perhaps even a breach or virus. If these types of events occur, on-site backup is typically the fastest way to get the organization's systems back up and running when compared to the other options.

59%

of organizations **recognize the dangers** of maintaining just one form of backup

Source: Survey conducted by Redmond Magazine

Maintaining backup copies on two different types of media is important in the event of media failure. According to Boston Computing Network, 34 percent of companies fail to test their tape backups, and of those that do, 77 percent have found tape back-up failures.

Maintaining an offsite backup copy is effective when a disaster destroys both your systems and onsite backup copies. When you need to bring up a secondary site, you can use the offsite backup copy. Storing a backup in the cloud is effective for any unforeseen event especially a disaster. Larger organizations store backup copies in either a private or a public cloud whereas SMBs tend to store copies in a public cloud.

If you cannot ensure business continuity without a disaster recovery and backup plan, you cannot afford to postpone DR planning. It must be, along with your backup strategy, a strategic element of your IT plan.

#3: Backup is a Requirement to Maintain Your Compliance Status

Most every regulatory compliance requirement dictates that organizations must protect and secure their data. Here are some examples of the most prevalent compliance regulations that require an organization to backup data in order to remain compliant.

HIPAA (U.S.) – If your organization maintains electronic patient records, the Health Information Portability & Accountability Act (HIPAA) requires that your organization have controls in place to manage data integrity, authentication, security, contingency planning, and access and audit controls. Backing up patient data is an important element in meeting these requirements.

Data Protection Act 1998 (UK) – The Data Protection Act governs the protection of personal data on identifiable living people in the UK. One of the data protection principles dictates organizations must take measures to ensure no accidental loss or destruction of, or damage to, personal data. Only backup can ensure that data is not accidentally lost or destroyed.

SOX (U.S.) – All publicly held organizations in the U.S. are subject to the Sarbanes-Oxley Act of 2002, which has stringent requirements relating to record retention, record alteration, and destruction. Backing up financial and business records is an important element in meeting these requirements.

Basel II and Basel III (Global) – Among other requirements, Basel II and III mandate that financial institutions must have data under control at all times and that the system back-up plans must be in place.

FINRA (U.S.) – The Financial Industry Regulatory Authority is a non-government organization that regulates member brokerage firms and exchange markets on behalf of the SEC. SEC Rule 17a-3 and 17a-4 outline the requirements for record keeping. According to the rules, these organizations must maintain records of numerous types of financial transactions for a period of three or six years, two years in an easily accessible place.

PCI (Global) – The Payment Card Industry's Data Security Standard (PCI 3.0 DSS) 12.10.1 requires retailers to create an incident response plan that will be implemented in the event of a breach. The plan must address a data backup process.

GLBA (U.S.) - The Federal Financial Institutions Examination Council (FFIEC) federal agencies and the Federal Trade Commission (FTC) oversee financial institutions affected by Gramm-Leach-Bliley Act (GLBA). Both organizations require financial institutions to put contingency plans in place to enable them to recover from an emergency or disaster. The regulations require a data backup plan, a disaster recovery plan, and an emergency mode operation plan.

Why Acronis is the Only Strategic Backup Solution for SMBs

There are three major types of backup solutions available on the market today:

- The one-size-fits-all traditional platform that provides a smart backup server, cell, or core and performs and manages full unified data protection for the entire environment, whether physical, virtual, or both.
- Separate products or tools that protect your different data types, operating system platforms, and applications.
- An integrated suite of products that provides unified control, management, and reporting for your entire environment regardless of the size of your organization, the number of data types, the number and types of operating system platforms and applications.

A traditional platform will support large numbers and types of data elements, operating system platforms, and applications. One platform means dealing with only one vendor and eliminating the complexities of dealing and managing multiple vendors. Purchasing a traditional platform is a strategic decision.

Unfortunately, for SMB organizations, a traditional data protection platform is typically too expensive. There are significant upfront costs to procure a traditional platform including the license, dedicated hardware, the networking components to support the central core, and the maintenance costs. A traditional data protection platform also requires one or more full time, trained and certified system administrators – a resource many SMBs cannot afford.

You can make the decision to purchase separate backup products and tools on an as-needed basis, which is a tactical approach to addressing your backup needs - system-by-system, application-by-application. While this may simplify the initial buy decision because each of these applications is less expensive than a traditional platform, you will be dealing with different backup vendors for each OS and application platform you have.

The downside: multiple products and vendors multiply training, management complexity, installation, monitoring, and reporting activities since each product is different. As your organization grows, the costs for additional separate products / tools will start to add up. As the number of operating systems and applications expand in your organization, you will need to hire more IT administrators, increasing your staff and IT training requirements.

37% of companies

simultaneously need to **protect data** in virtual, physical and cloud-based environments

Source: Acronis Disaster Recovery Survey, IDC, May 2014

If you are a SMB, purchasing an integrated suite of products is a strategic decision because you will have one backup solution that addresses each of your OSs and applications and the ability to blend individual point solutions into one integrated solution. An integrated suite of products means your organization is dealing with one vendor and eliminates the complexities and time associated with managing multiple vendors. In addition, since an integrated suite of products uses one installation console and management console for all of its products, you will simplify your IT staff requirements and reduce your IT training costs.

Summary

IT professionals should never delay the backup discussion. In fact, backup and disaster recovery should be a discussion point throughout the IT planning process. Backup is critical – yes, strategic – to your organization because:

Your business is about your data and backup is the only way to protect it.
No backup = no data = out of business

Backup is the most fundamental component of any disaster recovery plan.
No backup = no disaster recovery = out of business

All compliance regulations require businesses to backup data.
No backup = non-compliance = possibility of civil or criminal penalties

Acronis offers SMBs the only affordable, strategic solution to protect any data, across any environment, in any location. Acronis backup products are powered by the Acronis AnyData Engine, a set of unique, deep, and powerful new generation data protection technologies that capture, store, recover, and manage data in virtual, physical, and cloud environments. Depending upon your business needs, you can deploy individual Acronis products or seamlessly blend what you require into a total unified solution that protects any data, across any environment, in any location.

Regardless of your environment, you can use the same unified console to configure, install, and maintain each product. For multiple business systems, Acronis offers the Acronis Management Server (AMS) - a single pane-of-glass that lets you easily manage the backup and recovery of all data across multiple Acronis Backup Advanced products. Developed for organizations requiring a complete, efficient, and easy-to-use solution, Acronis' new generation technology simplifies backup, disaster recovery, and secure access of your critical data, reducing data loss, IT management time and total cost of ownership.

Acronis

About Acronis

Acronis sets the standard for New Generation Data Protection through its backup, disaster recovery, and secure access solutions. Powered by the AnyData Engine and set apart by its image technology, Acronis delivers easy, complete and safe backups of all files, applications and OS across any environment—virtual, physical, cloud and mobile.

Founded in 2002, Acronis protects the data of over 5 million consumers and 300,000 businesses in over 130 countries. With its more than 100 patents, Acronis' products have been named best product of the year by Network Computing, TechTarget and IT Professional and cover a range of features, including migration, cloning and replication.

For additional information, please visit **www.acronis.com**.
Follow Acronis on Twitter: **http://twitter.com/acronis**.