The business implications of not having a backup strategy: where businesses get it wrong

A business that fails to maintain a copy of its data is asking for trouble. It is extremely easy to lose data and all but impossible to rebuild that data if backups don't exist. Are you backing up your data regularly? This white paper outlines the risks of not having a backup strategy.

GFI®

Contents

Introduction

A business without a backup and recovery strategy is asking for trouble and taking an unnecessary risk. IT staff should never allow this to happen. There are no excuses; backups should be given as much importance as the overall protection of the organization's network.

Hyperbole? Imagine for a moment that one day you go to work to find that all your company data – meaning your email, your Word and Excel documents, PDFs, databases, contact lists, accounting data, billing information, etc. – has simply vanished, permanently. Gone is everything that makes your company what it is and that has allowed it to operate and grow as a business since its inception.

How will your company recover? Are you going to recreate years worth of data in a few months, all the while trying to support and manage your current business obligations? For most businesses, small, medium or large, this will probably be too much to bear – 90% of all companies that suffer a major data loss go out of business within two years (London Chamber of Commerce).

Permanently losing data is a completely preventable disaster, all it takes is a backup and recovery strategy.

The irony is that most businesses recognize the importance of having backups. A recent survey of small and medium-sized enterprises (SMEs) by Rubicon Consulting rated backup as their second-highest computing priority, after defense against viruses and other malware; and ahead of issues like reducing costs and deploying new computers. Yet nearly one-third of SMEs surveyed do nothing to back up their data.

At the same time, while they are struggling with explosive data growth, the backup processes SMEs have put in place often create a false sense of security that puts data and the company, at risk. The Rubicon survey found that 92% of companies have deployed some form of data backup technology, yet 50% of them have lost data. Of the companies that lost data, approximately one-third lost sales, 20% lost customers, and one-quarter claimed the data loss caused severe disruptions to the company.

Criminal negligence or incompetency? When your company shutters its doors for good because it can't service customers, bill or conduct essential business, does it really make a difference?

Getting it wrong

There are any number of ways a business can set itself up for crippling data loss.

Pollyannaesque attitude: Call it complacency, misdirected optimism or simply a firm, if misguided belief that data loss can't happen here. Either way a prime reason that SMEs and some large companies don't have backup strategies is that they can't bring themselves to believe that they can suffer a data loss. It hasn't happened yet, they reason, so it won't happen here. These are the same companies that can't believe they might be affected by a virus or malware.

Not conducting regular backups: Roughly one-third of SMEs do not have a backup strategy in place. For many that do, the words "thorough" and "complete" do not define their data backup strategy. Some backup their hard drives once a week, if they remember. 20% of SMEs do not even backup their servers.

Relying on employees: In a growing number of businesses, critical data are often stored on individual employees' desktops or laptops. These data, which can range from proprietary information to project plans to critical correspondence are typically not tied into the enterprise's backup system. Instead businesses rely on employees to backup their own data, usually without direction or advice. The result, given the uneven IT skills and awareness in any enterprise, is, more often than not, that backups don't take place in which case a single failed hard drive or stolen laptop can spell utter disaster to a business.

Keeping backups onsite: A backup plan is only as good as your ability to recover the data, and one of the commonest mistakes is to store the backup at the same locale as the original data. If the business is struck by fire, natural disaster or a malicious employee, not only is the data lost but the backup as well.

Adhering to a foolish frugality: Some businesses, too many as it turns out, while happy to pay lip service to the idea that a good backup strategy is essential, fall down when it comes to providing the necessary resources. Sometimes the rationale is cost, sometimes it's the small number or lack of expertise of the existing IT staff,

especially when there are other, misperceived "more pressing" tasks to attend to. One common error is to reduce costs by providing inadequate storage media. Another is to fail to utilize technologies that allow for rapid backing up of data.

Not confirming backups: One more oversight that can lead to a permanent data loss is not testing the ability of the organization to recover data. Backups are only as good as the ability to recover data from them. Unless an organization routinely confirms its backups, and its ability to recover lost data with a rigorous testing program, the backup strategy, if one exists may be for nothing. Yet despite this logic, 34% of companies NEVER test their backups and 77% of those who have tested their backups have discovered failed backups before they were needed (US Department of Trade & Industry).

Getting it right

So what makes an effective data backup strategy? The first step is knowing what needs to be backed up, including regulations such as Sarbanes-Oxley and the Health Insurance Portability and Accountability Act (HIPPA), which have specific backup requirements. Businesses should also determine whether data should be backed up or archived. Most businesses do both. Backups are copies of active data for short-term use and are frequently overwritten with updated versions. Archives, on the other hand, contain static data, such as inactive document files and old emails.

An effective data backup plan consists of five parts:

Plan for data backup

» Decide what data needs to be backed up

» Decide where to keep the backup

» Store a full backup at another location or online to protect against fire, theft or other disaster

» If the data are critical it may be a good idea to have a quarterly and yearly backup as well so that you can recover files that may have been deleted, but not discovered until months later.

Begin a backup routine

» Make backing up a part of the normal scheduled daily tasks

» Don't rely on anyone else to back data

» Wherever possible automate the backup process.

Tailor the backup strategy to business needs

» To determine the best schedule for data backup, it is important to know how often the data changes. If data changes weekly, a daily backup might be overkill. If there is critical data that updates every hour, it may be necessary to back up several times a day.

» Full backups can be supplemented by incremental backups. An incremental backup will only back up files that have changed since the last full backup and is normally much quicker than a full backup.

Test the backup periodically

» To ensure that backups are protecting you, periodically test the backup jobs by attempting to restore them to an alternate location. This will bring out any flaws or corrupt data before it is too late.

» Most backup applications also have a "backup log" or generate a "backup report" that can quickly identify any problems or skipped files in the backup job. Be sure to review these logs every time backups are complete, for anything suspicious.

Have at least three different backups of data

» A backup is more than simply moving email, financial documents or other important files off to an external hard drive or removable disk. Simply moving data from one location to another isn't giving you any extra protection in case disaster strikes. If there aren't at least two separate copies of your data, it isn't a backup at all.

» While a single backup may be a good start (two copies of irreplaceable files), there is still some risk for data loss, especially if both copies are kept in the same location.

» The best protection against data loss, especially from catastrophic events, is having at least three copies of your data (the original files, an easily-accessible backup and a protected copy of your backup). While some large companies may use dedicated off-site data storage services for this, a business doesn't have to be big to have three copies of your data. Even something as simple as using an inexpensive online backup service to keep a third copy of the data is sufficient.

Summary

Any business that cares about the security of its data needs to have an effective backup strategy to guard against inevitable data loss. Given the overall negative impact permanent data loss can have on a company, up to and including its bankruptcy, a data backup and recovery strategy that is effective is essential.

About GFI

GFI Software provides web and mail security, archiving, backup and fax, networking and security software and hosted IT solutions for small to medium-sized enterprises (SMEs) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy and a strong focus on the unique requirements of SMEs, GFI satisfies the IT needs of organizations on a global scale. The company has offices in the United States (North Carolina, California and Florida), UK (London and Dundee), Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold Certified Partner.

More information about GFI can be found at http://www.gfi.com.

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

GFI®