GFI White Paper

Understanding data backups: why SMEs need them

Data is the lifeblood of every organization, yet many either fail to back up their data or they are not doing so properly. Losing data can be catastrophic for a business. This white paper explains why backups are important and the challenges they face.

GFI®

Contents

Introduction

If people are a business's most valuable resource, then data is the fuel that drives and sustains it.

Data, in all its forms, is the key to a successful business. Data helps establish strategy, assures appropriate billing, keeps records and myriad other essential tasks. Without data, a business can fail, making the preserving of data nothing less than a strategic priority. This applies to businesses of all sizes, but especially to small and medium-sized enterprises (SMEs).

How important is guarding against data loss? Is survival a good enough reason? Of the companies that lose their data, 90% are out of business within two years and nearly 50% are unable to ever reopen their doors (London Chamber of Commerce) .

While small and medium-sized enterprises don't typically generate the same amount of data that larger enterprises do, they still need the same kind of protection to ensure the timely recovery of essential business data.

The state of SME data backup and recovery

Data has a great disadvantage compared to PC hardware in that it can be lost, and once lost, never easily replaced. You can get a hard disk replaced under warranty, but the new one will come to you totally empty. However, data has a great advantage that compensates for this weakness: it can be readily and easily duplicated.

Given the above, and with so much on the line, you would expect that SME owners and managers have the situation well in hand. Unfortunately, it appears that they don't.

A recent survey by Rubicon Consulting found that while SMEs are grappling with explosive data growth, the backup processes they have in place often put that data at risk.

The survey also 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.

Concerns about potential data loss run high among SMEs. Respondents 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.

In many instances, when they do, these SMEs do not fully back up the data stored on company computers. About a quarter of SMEs conduct no backup of desktops, and another 13% do only informal backups where employees decide the frequency and which files are protected without any guidance. The situation is similar for servers; about 20% of SMEs conduct no server backup.

When backups do occur, most backup files are not stored remotely. More than half of all backup files on desktops and servers are stored in the same location as the originals, a foolish decision which leaves the company vulnerable to permanent data loss. According to survey results, causes of data loss are diverse. Although natural disasters are often cited as a risk, onsite disasters are the primary contributing factors of data loss. 63% of respondents cited hardware failure as a cause of data loss incidents, 27% from deliberate sabotage by employees and 27% from theft.

Challenges facing SMEs

A foolish frugality seems to govern the approach many SMEs have to safeguarding data properly. There is an inherent misconception that with money and staff time at a premium, there's always something more pressing to do than manage backups. As shown above, that sort of reasoning, attractive as it might seem to some, jeopardizes a company's assets as surely as deciding to leave the company cars in an unlocked parking lot, with the keys in the ignition, because it's too expensive and resource intensive to collect the keys. No one would accept that solution.

Given their smaller budgets and lack of in-house IT expertise vis-à-vis larger enterprises, SMEs require solutions that are both cost-effective and easy to use, meaning the top challenges SMEs face with regard to data protection include:

- **Implementing comprehensive protection with minimal impact on business operations:** It is estimated that data volumes are increasing by as much as 50% per year. At the same time, the demand for higher system availability is shrinking backup windows. Together, these trends are placing greater pressure on small to medium-sized enterprises to improve backup efficiencies and deliver prompt recovery. Gone are the days when critical systems could be shut down to perform backup operations.
- **Meeting increasingly stringent backup and recovery requirements:** The requirements to recover lost or corrupt data to a specific point in time and reduce the overall time to restore data are becoming more stringent and are now often measured in hours instead of days. Increasingly, tape-based backup infrastructures are unable to meet these requirements.
- **Dealing with limited backup administration resources:** This is a key issue particularly with smaller companies that may not have dedicated IT staff or backup administrator. The result is that a large percentage of critical data is generated by distributed clients; and an inability to protect this data can leave SMEs open to data loss that can have a significant impact on the business.
- **Deploying disaster recovery strategies cost-effectively:** As the Rubicon Consulting survey made clear, data protection practices aren't where they should be for most SMEs. Too often SMEs lack the resources, administrative expertise, and off-site storage required to provide true disaster recovery capabilities.
- Maintaining a secure backup and recovery strategy by providing adequate security, including encryption and virus protection, plus centralized management of an entire data protection infrastructure, ensuring backup data is protected and efficiently managed.

Solutions

SMEs may not need the scale provided by enterprise backup and recovery solutions, but they do need the same functionality. That means policy-based backups, automated operations and centralized management should be key design tenets to help lightly staffed SMEs effectively manage system and data protection operations. Integrated disaster recovery capabilities, meanwhile, make it easier to rapidly restore complete systems. Newer technologies such as disk-based backup, snapshot backups, data de-duplication, continuous data protection and cloud-based backup options can help SMEs address shrinking backup windows, increasingly stringent RPOs/RTOs (recovery point objectives/recovery time objectives) and recovery reliability concerns.

The technologies to implement these solutions do exist, but many SME managers and IT staff can feel overwhelmed by the technology and often, the cost of the solution, leaving their business vulnerable to an avoidable disastrous outcome. While there is no one answer that fits all needs all the time, SMEs would benefit from a backup solution that allows for automation and centralized management of their backup practices.

Summary

Far too many SMEs engage in risky backup strategies and methods that are born out of a combination of failing to prioritize backup and recovery strategies properly; misplaced optimism that leads them to think "it can't happen to us", and some uncertainty over what methods to pursue. Many, when they have a backup strategy, fail to implement it fully, leaving them at risk but instilling a false sense of security.

These faulty methods can, when data loss occurs, negatively impact an SME's bottom line, sales and customer relationships, which explains why so many data disasters are followed by bankruptcy.

By developing data backup and recovery strategies and deploying appropriation solutions regarding backups of important data on a timely basis, SMEs can ensure that their data, or most of it at least, will never be truly lost; at worst, some will be lost and they will experience the inconvenience of restoring it in the event of a hard disk failure, for example. That is an infinitely better outcome than going out of business.

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

Disclaimer

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.