



IT Knowledge • Business Results



ESG Report

Data Protection Strategies for SMBs

By Heidi Biggar
Storage Analyst, Data Protection
Enterprise Strategy Group

April, 2007

Table of Contents

- Table of Contents** 1
- Introduction**..... 2
 - Caught in a Catch-22 2
- Data Protection for SMBs** 3
 - Fundamental Realities 3
 - Fundamental Challenges 3
- New Options for SMBs**..... 4
- New Options for SMBs**..... 5
 - Disk Offers New Hope 5
 - The Role of CDP 6
- Conclusion** 8

Introduction

Caught in a Catch-22

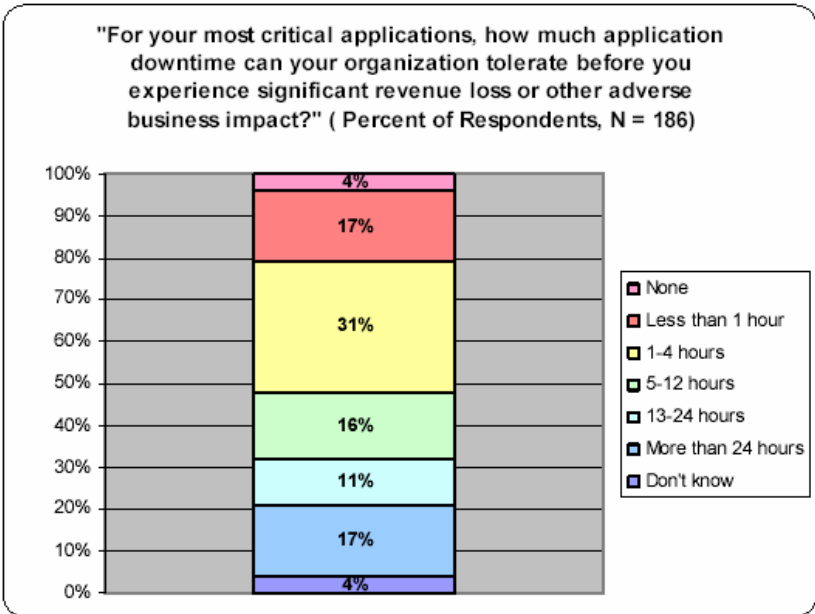
Good things often do come in small packages, but for small and medium-sized businesses (SMBs), this hasn't always been the case for data protection solutions. For years, small organizations – particularly those with limited or no designated IT resources (i.e., people or dollars) – have struggled to find products that enable them to easily and cost-effectively protect their data as well as meet today's new regulatory requirements.

As a result, many SMBs have either ended up implementing data protection solutions over the years that have been too big for their environments, with the hope that they will grow into them, or that have been grossly inadequate, given today's increasingly demanding business climate. And, as unwise as it may seem, still others have had no real data protection strategies in place, putting their critical business applications and data at potentially significant risk in the event of a corruption, virus attack or some type of regulatory or legal inquiry.

According to ESG Research,¹ 79% of SMBs said they could tolerate 24 hours or less of downtime before experiencing significant revenue loss or other adverse business impacts, while 31% said they had a window of tolerance of between one and four hours (see Figure 1). ESG expects this window to continue to decrease as data volumes grow for this class of user, and data becomes an increasingly critical asset of their day-to-day operations.

Bottom line: It's not the size of the organization that determines the value of the data that is generated. Mission-critical data is mission-critical data regardless of who produces it, and deserves appropriate protection. That said, SMBs face a number of different challenges that larger organizations don't (and vice versa), which necessitate some key differences in data protection strategies.

Figure 1



¹ ESG Research, 2004.

Data Protection for SMBs

Fundamental Realities

There are three fundamental realities facing SMBs today: 1) They are generating a lot more data than ever before, and there is no end in sight to this growth, 2) the value of the data they are generating continues to mount and 3) they are becoming more aware of the need to protect their data resources or face significant business risk.

- **Increasing data volumes:** The size of primary and secondary data volumes today rival the data volumes of significantly larger organizations just a few years ago, and these volumes are increasing steadily, year over year. According to ESG Research, more than a third of SMBs report 28% growth per year. ESG expects digital content growth alone to have a 50% or higher CAGR for the next five years.
- **Increasing importance of data:** It's not just the size of the backup volumes that has increased, but the value of the data that is being generated. As the value of data increases, tolerance for application downtime generally also decreases. The opportunity cost associated with a loss of data never diminishes - it only increases. As volume grows, opportunity cost and probability of failure increase.
- **Increasing awareness of need to protect data:** SMBs are getting the message that when it comes to the data that drives their business, what is worth having is worth protecting. However, there are fundamental changes that need to be made to their data protection practices. Doing incremental backups nightly and full backups weekly is often no longer adequate - and it requires people and dollars that SMBs still don't have. New disk-based options provide better data protection from both a backup (i.e., getting backup jobs done in allotted windows) and a recovery (i.e., being able to recover data quick enough in a restore situation to minimize downtime and potential data loss).

Fundamental Challenges

Many SMBs still rely on traditional tape-based products for data protection. The problem is that these products generally fail to address three persistent backup-and-recovery challenges – shrinking backup windows, data protection gaps and long recovery times.

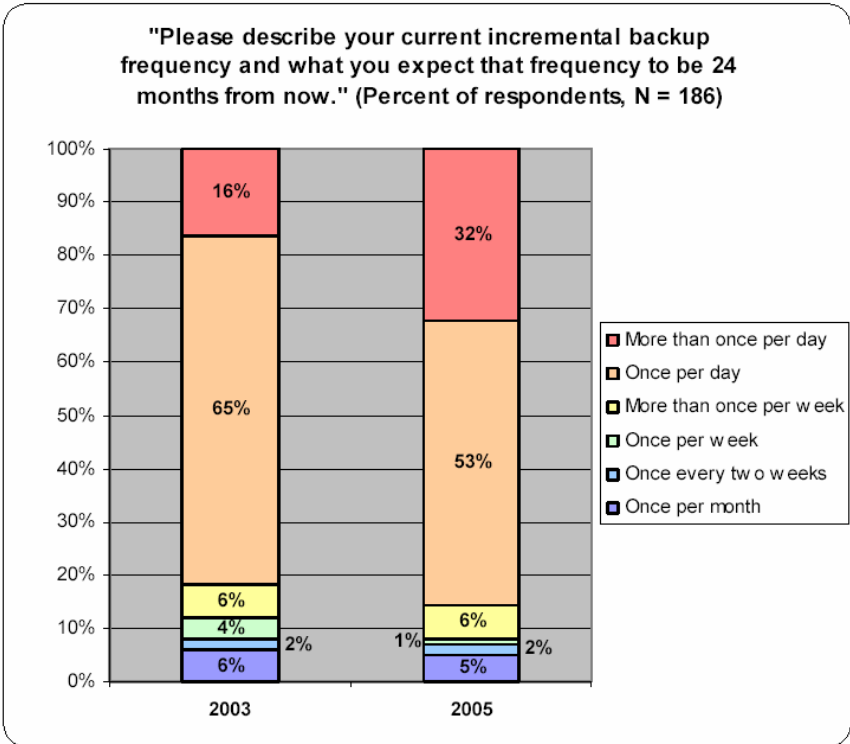
- **Shrinking backup and recovery windows:** Over the past couple of years, ESG survey respondents have spoken loudly and clearly: When it comes to data protection, time is definitely not on their sides, especially as data volumes increase. In fact, the single, greatest data protection challenge among SMBs is getting backup jobs completed in allotted windows. There simply aren't enough hours in a day to back up all data to traditional tape-based data protection targets, especially when SMBs are being asked to keep applications up and running for longer periods of time. SMBs are equally pressed when it comes to recoveries. As illustrated in Figure 1, SMBs' tolerance for downtime is shrinking. Like larger organizations, they are being asked to recover data faster and with less potential data loss.
- **Troubling data protection gaps:** While SMBs recognize the inherent value of their business applications and associated data, for many there's still an apparent disconnect between the perceived value of that data and the frequency with which those SMBs currently back up their systems, though this is changing. ESG Research found that more than one-third of SMBs two years ago either knew or worried that their current backup schedules did not provide an adequate level of protection against loss and as a result were looking to increase the frequency with which they backed up (see Figure 2).

End-User Perspectives: Data Protection Challenges

“Speed of backup is a critical factor in our environment. We’re now running our applications from 7:00 AM to 4:00 AM the following morning, which leaves a very short backup window.”

Other ESG Research² shows that organizations – big and small – are looking for data protection technologies that further speed the backup process and, equally importantly, allow for faster restores. Again, the cost of downtime is driving the need for both faster backup and restore.

Figure 2



- Shortcomings of legacy technology:** As data protection demands on SMBs increase, the shortcomings of legacy traditional tape-based backup and recovery solutions become more apparent. SMBs report problems with both backup and recovery performance, reliability issues (due to media failure, human error, and hardware failure), tape management headaches and high administrative costs. Nearly one of four SMB users in our Research reported that at least 20% of their tape-based backup operations failed, and a slightly higher percentage (26%) said that 20% or more of their recovery attempts failed. Translate these losses into dollars lost, and the impact is potentially financially devastating to the SMB.

End-User Perspectives: Data Protection Challenges

“It sometimes takes us three days to restore a single desktop because the user’s data is scattered across 40 different backup tapes.”

² ESG Research: *Tape Replacement Realities*, March, 2005.

New Options for SMBs

Disk Offers New Hope

The face of data protection is changing for SMBs just as it has for larger organizations. A number of current business realities, including business continuity and disaster recovery concerns, regulatory compliance requirements, information security threats and growing data volumes, are putting increasing pressure on SMBs to change traditional data protection behaviors or mindsets.

The scale of the recovery operation may be different between SMBs and larger organizations, but the need to recover data quickly and efficiently to meet recovery point and recovery time objectives (RTOs and RPOs) is becoming just as critical for SMBs as it is for larger organizations. And as they have in the enterprise world, disk-based data solutions, including virtual tape libraries (VTL), disk-based targets, snapshot, and continuous data protection (CDP), are playing an increasingly important – and prevalent – role in protecting SMB environments.

The problem is that many SMBs still think of data protection in traditional backup (i.e., backup to tape), not recovery, terms and, importantly, most major vendors think of SMBs as an extension of the enterprise and attempt to retrofit enterprise solutions to SMB environments, with marginal success.

SMBs, like larger organizations, are looking to disk-based data protection solutions for data protection because they can significantly help them improve performance, reliability and people utilization (by reducing or ideally eliminating the amount of tape handling that is still required). But SMBs are also looking for solutions that meet a number of other criteria, including:

- **Easy to use:** Is the solution plug-and play? Is it user-friendly? Easy to use? How easy is it to administer, manage and use? ESG has observed that SMB users are significantly more likely than their enterprise counterparts to cite technical (as opposed to business or financial) considerations as reasons for not considering implementing various IT technologies, including disk-based data protection solutions. Also, SMBs share a common trait with their larger counterparts in that they also tend to address the hottest, most visible issue of the day and as such, longer term and more strategic issues such as data protection tend to be put at the end of the list. SMBs, like most of us, fix the problem that is in front of them before looking beyond. They simply don't have the manpower or expertise to handle multiple IT initiatives at the same time - and the perception of the user community is that backup and recovery "fixes" are complex, costly and huge time sinks.
- **Non-disruptive:** Along the same lines as low cost, SMBs are looking for disk-based solutions that can be added to the existing data protection environment or implemented by the first-time data protection customer with little or no fanfare. SMBs want data protection solutions that support existing business applications (e.g., Exchange, Outlook, SQL, etc.) and systems (e.g., both desktops and laptops) that don't require any significant changes in procedures and that have no impact on the existing network or applications. SMBs are all about transparency.
- **Low cost:** SMBs are wary of the capital investment requirement of data protection solutions. Across all disk-to-disk technologies, SMBs state cost as the number-one barrier to deploying new disk-based data protection solutions. In particular, they are wary of the capital investment required to add the new secondary disk capacity necessary for growing data stores.

The Role of CDP

Thanks to the advent of disk-based backup technologies and a number of other underlying factors (e.g., growing data volumes, increased regulatory scrutiny, etc.), data protection isn't just about backup anymore. It's also about recovery. After all, what is the point of backing up data if you can't recover it fully and in an appropriate timeframe when you need to? Disk-based technologies, such as continuous data protection (CDP), make this possible for SMBs.

Continuous data protection (CDP) is one of what ESG describes as a "continuum" of data protection technologies available to SMBs today. ESG views CDP as both an RTO and an RPO enhancer (see Key Definitions for SMBs below).

The beauty of CDP technology is it allows users to restore or recreate data - at very granular levels - to virtually any point in time. Should a file become corrupted or be accidentally deleted, CDP allows the user to roll back to a point in time before the deletion or corruption occurred. CDP means that, instead of waiting to recover last night's - or last week's - information, SMBs can recover from minutes ago. When this technology is applied inside a solution that is "set and forget," the SMB can bring their data protection world to a whole new plane - one that even most of the big shops are not capable of. If an SMB can not only dramatically improve their recovery abilities but also automate those abilities such that they no longer have to spend time and energy on them, at least one major headache and risk goes away. That is a powerful - and necessary - message.

While CDP technology is being integrated into leading vendors' backup and recovery software, it is also available as a storage service and in standalone appliances, which are designed to be plug-and-play additions to SMB environments. Other notable features that SMBs should consider when evaluating products are things such as onboard encryption, open-file backup, incremental backup, versioning (in addition to instant recovery), hands-free offsite backup, network throttling features (for sending data to a co-location facility), user-based recovery and flexible policies. Prioritizing your requirements is a good first step, as you want a product that gives you what you want and not one that forces you to accept what a vendor considers important.

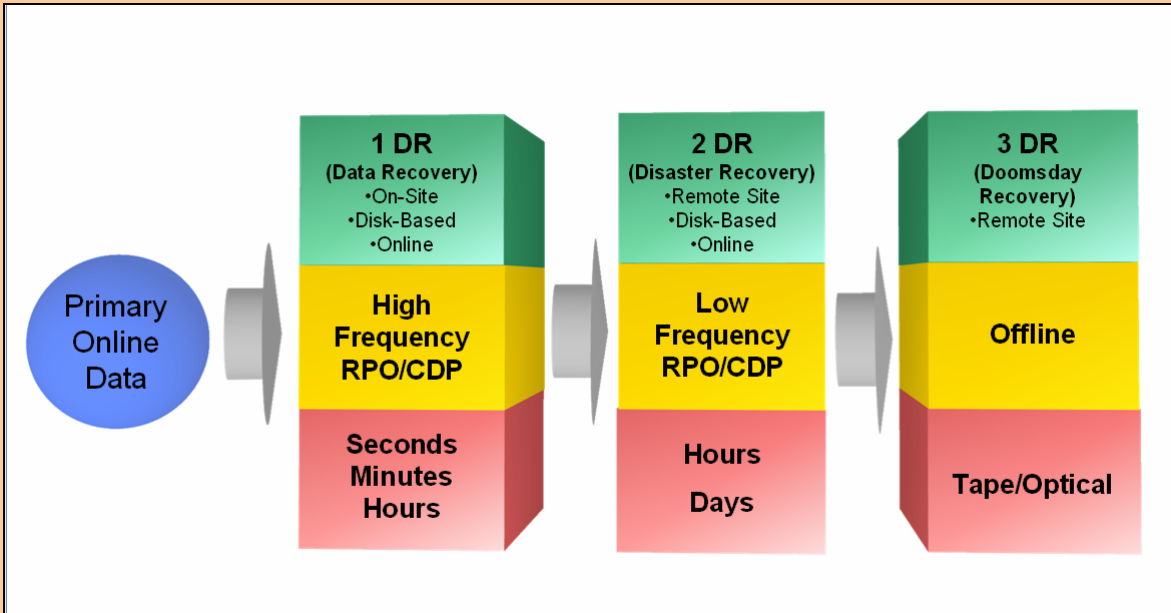
Key Definitions for SMBs

Recovery Time Objective (RTO): A measurement of how quickly data needs to be restored in the event of an outage or some type of disaster. In other words, the amount of the time an organization can be without data (e.g., minutes, hours, days, weeks, etc.).

Recovery Point Objective (RPO): The point in time to which data is restored in the event of an outage or some type of disaster. In other words, the amount of data loss (e.g., 15-minutes' worth, an hours' worth, two days' worth, etc.) an organization can tolerate.

Generally speaking, RTOs and RPOs increase as data ages. However, for SMBs that want to ensure that all data is protected at all times - and want minimal hands-on administration or involvement - CDP can be applied to all points of the 3DR data protection continuum, as shown in Figure 3.

Figure 3: 3DR Continuum



3DR is an ESG construct that describes the ability and efficiency of data recovery within an organization.

1DR, data recovery, assumes that local disk-based devices are used to house data that is statistically most likely to require a recovery operation. In a perfect world, all recovery operations would occur at this stage.

2DR, disaster recovery, implies a second (or third, etc.) set of disk-based devices that house recoverable data outside the main facility. This data may be less granular than 1DR data in terms of RPOs, but access and availability are on-line.

3DR is doomsday recovery or the worst case scenario. This is based on off-line media, typically tape, vaulted somewhere for deep archive.

Conclusion

For years, SMBs have been trying to make enterprise-class backup-and-recovery products work in their environments. But SMBs are a distinct class of users with a distinct set of requirements. Just as no amount of forcing makes a square peg fit into a round hole, no amount of retro-fitting makes enterprise-class products SMB-appropriate.

With the advent of disk-based data technologies, a variety of new technologies have hit the market. For the SMB, this means new choices - ones that can help them meet their specific use requirements without breaking the bank or, importantly, driving IT complexity through the ceiling.

CDP is a technology that will become mainstream within every facet of IT. The proper packaging of the technology, delivered as an appliance, gives SMBs plug-and-play usability and RTOs and RPOs of near-zero. Now, that's proof that good things do come in small packages. If it is priced right and is easy to demonstrate value, vendors will find the SMB a willing and ready market.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. and is intended only for use by Subscribers or by persons who have purchased it directly from ESG. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at (508) 482-0188.