The 2007 Introduction to SMB Automated Data Protection

The Simple and Inexpensive Solution to Best Protect Your Data

FEATURES:

- *Introduction to Regulatory Compliance*
- *How to Automate your Backup Process*
- *The Latest Automated Data Protection Technologies and Techniques*

TANDBERG DATA
Securing your Information

Table of Contents

1. Introduction

If your New Year's business resolutions included improving your backups, you're not alone. A 2004 Tandberg Data study revealed that 70% of small to medium sized businesses (SMBs) recognize the need to automate their backup process. The Gartner Group estimates that less than 50% of medium sized businesses and 25% of small businesses have data recovery plans in place. An Imation study[1] confirmed that 50% of SMBs do not have a formal backup procedure, and that the reliability of their data backup systems was their second most "extremely" or "very challenging" issue." Clearly, SMB data protection is often neglected, undiscovered until disaster strikes.

The first step in fulfilling your resolution is the realization of three facts:

Data loss is inevitable

It is critical during the design of your data protection strategy to realize that data loss is inevitable. It is estimated that 6% of all PCs will suffer at least one episode of data loss per year, and 20% of laptops will suffer hardware related data loss in their first three years of use. As a comparison, the chance of your being involved in an automobile accident in any given year is 7%. A CBI/FBI survey[2] revealed that 52% of respondents discovered unauthorized access to their systems, and 47% had experienced laptop theft.

Although data protection strategies generally start with protecting servers, a significant portion of your company's contemporary data resides on individual PCs and laptops. Considering the failure rate of these devices, backup system must be capable of scaling with the growth of client computers, and their ever-larger disk drives.

The cause of your permanent data loss may surprise you

Generally, data loss is anticipated as the result of a disk drive failure. While the mean time between failure (MTBF) for most SMB disk drives predicts that one of your drives may fail within a given year, drive failure is not the primary cause of data loss.

Data loss frequently occurs even with a backup system in place. In a recent research report, the Enterprise Storage Group[3] reports that nearly one out of four SMBs respondents to a recent survey reported that at least 20% of their recovery attempts fail. Human

[1] "2004 Imation Data Protection Study", Imation Corporation
[2] "2006 CSI/FBI Computer Crime and Security Survey", Computer Security Institute / Federal Bureau of Investigation
[3] "The Changing Dynamics of Backup and Recovery in the Small and Medium Business (SMB) Market", John McKnight, The Enterprise Storage Group, June 2004

error in the backup process or in the interchange and handling of tapes is cited as the primary cause for data loss.

In a recent survey[4] over 50% of respondents indicated that their tape failures were sometimes, often or always caused by human error. The Gartner Group reports[5] that 40% to 50% of all backups are not recoverable in full, and that 60% of all backups fail in general. Even in large enterprise data centers, nearly one quarter of respondents report that 20% or more of their tape-based recoveries fail[6].

The impact of data loss is likely greater than you imagine

The loss of critical business records such as accounts receivable, customer details or transaction histories is often a fatal stroke. Studies[7,8] show that companies that experienced a loss of access to their data for more than 10 days never fully recovered financially. Half of those companies closed their doors within five years. In all cases of data loss, 17% of surveyed[9] organizations were never able to recover the data.

Beyond financial risk, losing data places your organization in violation of numerous government regulations, often mandating reporting of the event. Furthermore, your risk escalates in the event of an audit or civil action.

It is estimated that the value of 100 megabytes of data is approximately $1,000,000, or $10,000 per megabyte[10,11]. This conclusion is partly based on the effort to re-enter the data (if available), and the cost of an outside specialist to attempt to recover data from a failed device. The financial losses are much higher.

Reducing the human factor through automation

Reducing the level of human involvement in your backup process improves your data protection, and subsequently reduces your business risk. The experts agree[12] – 76% of data protection specialists recommend automating your backup process to reduce risk and save costs. While automated backup systems were affordable only to large data centers at the start of this millennium,

[4] "Tale of the tape", Storage Magazine, February, 2005
[5] Gartner Group, January 2002, Adam Couture
[6] Enterprise Storage Group, "The Evolution of Enterprise Data Protection", January 2004
[7] University of Texas, Center for Research on Information Systems, 1994 Survey
[8] Jon Toiga, "Disaster Recovery Planning: Managing Risk and Catastrophe in Information Systems," (Yourdon Press, 1989)
[9] Dr. David M. Smith, "The Cost of Lost Data", Pepperdine University, March, 2003
[10] Stuart Hanley, "Keep Those Data Protection and Recovery Options Open", Storage Management Solutions, November 1997
[11] "The Data Recovery Solution", ONTRACK Data International, 1998
[12] Software Initiative Deutschland, October, 2006

new breakthroughs in technology and design have lowered costs to well within SMB budgets.

This paper presents the lowered risk, convenience and financial benefits of automating the backup process.

2. The Lurking Backup Disaster – Government Regulations Effecting Data Retention

The financial scandals that befell U.S. industries in 2002 and 2003 dramatically increased the government's interest in corporate governance. This interest directly translates to new requirements for the reliable retention of records for later examination. Virtually every industry has been or will be affected by new regulations. The Enterprise Storage Group has identified over 10,000 state and federal regulations dealing with the retention of records[13]. These regulations directly translate to backup procedures, raising the definition of data loss to potential 20-year prison terms.

Beyond regulatory requirements, your company may be required to produce data in its original form should you ever be involved in a civil proceeding. The failure to promptly produce records may directly influence the outcome of a lawsuit.

Summary of Government Regulations

Government regulations are generally directed at specific industries and larger organizations. To determine your exposure, the following table summarizes the most common regulations by industry.

[13] "Compliance: The effect on information management and the storage industry", May 2003, Peter A. Gerr, Brian Babineau and Patrick C. Gordon, The Enterprise Storage Group.

Regulation	Summary	Retention Period	For More Information:
Sarbanes-Oxley, Section 802	Applies to all public companies	5-7 years from the end of the financial period or audit.	thecaq.aicpa.org
HIPPA	Medical Providers	6 years after last in effect, two years after patient death, until minors reach the age of 21	www.hhs.gov
DICOM	Formats and standards for medical data storage	Defers to applicable government regulations	medical.nema.org
FDA 21 CFR Part 11.10(c).	Pharmaceuticals	Defers to other regulations	www.fda.org
NASD 3010 & 3100	Brokerages	3 years	www.nasd.com
NARA Part 1234	Federal Government	Varies by agency	www.archives.gov
Department of Transportation	Transportation & shipping	1-5 years	www.nhtsa.dot.gov
USDA	Food & agriculture	3+ years	www.usda.gov
DOD 5015.2	Providers of record management solutions to the DOD	Varies by content	www.dtic.mil
ISO 15489-1	International records management best practices	Defers to government regulations	www.iso.org
EPA 8700	Hazardous Materials	2 years to the life of the facility	www.epa.gov
Federal Rules of Civil Procedure	Federal Law Suits	Generally 6 years	www.law.cornell.edu /rules/frcp
State Regulations	Industry impact varies	Varies by state	Your state Attorney General's Web site

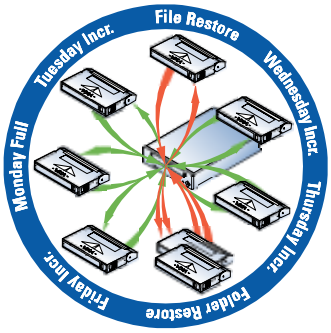


Illustration of 16 tape movements in one week

3. The Manual Backup Process

Continued operation of a manual backup process utilizing a single tape drive requires at least ten tape insertions and removals per week. The number increases when data is restored, a backup exceeds the capacity of a single tape, or a backup fails due to media errors. Over a period of years, the manual backup process is doomed to fail due to:

- The task is generally assigned to the lowest level personnel
- Personnel turnover
- Negligence
- Personnel absence
- Accidental insertion of the wrong tape
- Tape misfiling
- Tape damage or contamination due to frequent handling
- Media failure

The manual backup process generally degrades over time without frequent restore operations. The failure of the manual backup process is often only discovered when data is lost. In most cases, the fact that a backup did not complete successfully will never be known to management.

With the amount of your data growing rapidly year over year, eventually the capacity of a single tape will be insufficient to complete a backup. At that point, backups will become difficult and infrequent, as an employee must be present to insert a second tape after the first has completed.

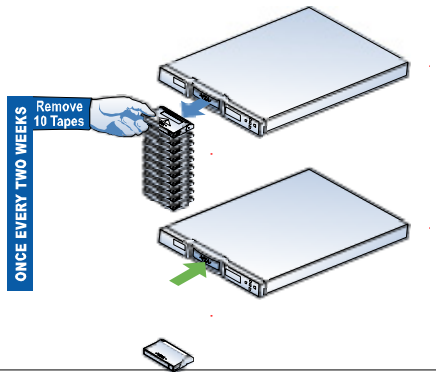
A data center class tape library – the origin of today's tape autoloaders

4. Introduction to Backup Automation

Eliminating the daily insertion and removal of backup tapes by implementing robotic tape automation systems is the key to eliminating the risk of human error from the data backup process. Although standard in large scale IT operations and data centers, tape automation systems are uncommon in small to medium-sized businesses. New innovations in technology and design have created tape automation systems within the budgets of most SMBs.

How an Autoloader Works

A tape autoloader is a compact storage device that contains a tape drive, multiple tape cartridge slots, and a robotic mechanism that moves tapes between the slots and the tape drive. Your backup software controls the autoloader, which instructs the autoloader to insert the correct tape before beginning a backup or restore. Each


ONCE EVERY TWO WEEKS
Remove
10 Tapes

backup operator must be present at the completion of the first tape, to load the next tape, hours after backup initiation.

The Financial Benefit

The daily manual exchange of backup tapes imposes a minimum fifteen-minute interruption of an employee's primary duties, amounting to 65 hours of lost productivity per year. By reducing this workload to only fifteen minutes per week, or 13 hours per year, tape automation annually adds 52 hours of employee time for other tasks. Assuming a total employee compensation cost of $60,000, deploying tape automation realizes $1,500 in annual increased productivity. As such, a solution under $3,000 will pay for itself in less than two years through reduced labor costs. These calculations do not include the labor savings an autoloader deployment achieves by precluding the requirement for after-hours recovery by immediately addressing media and tape loading errors.

The additional reduction of business risk by employing an autoloader presents the greatest return on investment, as the financial ramifications of catastrophic data loss exponentially exceed the cost of the autoloader. Because the autoloader multiplies the reliability of the backup process, any financial justification for an investment in the backup process multiplies proportionately, again increasing the return on investment.

Automating the backup and retrieval processes facilitates increased backup reliability and enhanced operational efficiency. Autoloaders further ensure that processes developed to address regulatory data protection requirements succeed. As such, autoloaders ensure optimal data protection with the added benefit of cost efficiency and investment protection.

5. Advanced Features in Automated Backup Systems

Over the past twenty years, autoloaders have evolved from scaled-down versions of their sibling large-scale tape library systems to simplified and streamlined designs specifically intended for small and medium-sized businesses. Costs have dropped dramatically due to a combination of a new tape technology and elegantly designed advanced robotics, both providing greater reliability at a lower cost. Further designed to reduce service costs, tape drives may be replaced or upgraded, and other common maintenance may be performed in the field by office personnel.

Today's autoloaders offer integrated intelligence, allowing for remote management and capable of responding to critical events. Embedded bar-code readers automatically establish a tape inventory as the tapes are loaded. Bar-coded tapes facilitate on-screen tape load verification by management, and allow backup

software to identify and select specific tapes for backup and restore. With bar-coded tapes, an operator has the ability to instantly verify the autoloader's contents, an operation that otherwise requires ejecting and reloading of all tapes or cartridges.

Where past autoloaders were relatively simplistic devices merely able to respond to commands from backup software with little interaction, today's full featured autoloader is a complete stand-alone system incorporating an Ethernet interface, and Web and email hosts. Incorporating a complete Web host enables remote management and configuration via any Web browser across the Ethernet network, or remotely across the Internet.

The most commonly utilized feature of remote management is the tape inventory display to confirm that the correct tapes are loaded. Further, an advanced feature of remote management allows an IT administrator or technician to remotely access diagnostics and event logs for reactive or proactive maintenance, without being on-site. Should the tape drive begin to report excessive tape read retries, the tape drive can easily be replaced on-site. Even the software utilized to operate and manage the autoloader, called firmware, can be replaced remotely, which uploads new device operations features, supports new devices and accessories, or upgrades the Web based management software application.

The integration of an email server enables the autoloader to automatically notify appropriate personnel of unusual events and device failures. For example, configuring the autoloader to email notifications of excessive tape or loading mechanism retries proactively addresses failing components before they reach the point of unrecoverable failure.

Until recently, features such as bar code labeling and integrated intelligence appeared only on data center class autoloaders costing an order of magnitude more, and thus targeted at large IT operations. The inclusion of this extensive suite of features in devices targeted at small to medium-sized businesses brings greater data protection to those organizations at an easily justified price point.

6. The Tandberg Data Exabyte Autoloader Family

The Tandberg Data Exabyte family includes eight autoloaders and libraries to address the requirements of any organization. Your selection should be based on your current and future capacity requirements. All systems may be upgraded to a larger capacity tape drive by office personnel. Also consider the transfer speed, to ensure that your backups will complete within your backup "window" of time.

	Capacity[14]	Transfer Rate[14]	Drive Technology	Tape Slots	Form Factor	Interface
VXA-2 PacketLoader 1x10 1U	1.6 TB	43.2 GB/hr	VXA-2 Packet Drive	10	1U rackmount	SCSI or FireWire
VXA-2 1x7 PacketLoader Desktop	1.1TB	43.2 GB/hr	VXA-2 Packet Drive	7	Desktop, 8.4"x8.3"x18"	SCSI
VXA-172 PacketLoader 1x10 1U	1.7 TB (upgradeable to 3.2TB)	86.4 GB/hr	VXA-172 Packet Drive	10	1U rackmount	SCSI
VXA-320 PacketLoader 1U	3.2 TB	86.4 GB/hr	VXA-320 Packet Drive	10	1U rackmount	SCSI
StorageLoader LTO-2	3.2 TB	172 GB/hr	LTO-2	8	1U rackmount	SCSI
StorageLoader LTO-3	6.4 TB	576 GB/hr	LTO-3	8	1U rackmount	SCSI
Magnum 224 LTO Autoloader	9.6 TB	346 GB/hr	LTO-2 (1-2)	12 or 24	2U rackmount	SCSI or Fibre Channel
	19.2 TB	576 GB/hr	LTO-3 (1-2)	12 or 24	2U rackmount	SCSI or Fibre Channel
Magnum 448 LTO Library	19.2 TB	691 GB/hr	LTO-2 (1-4)	48	4U rackmount	SCSI or Fibre Channel
	38.4 TB	1152 GB/hr	LTO-3 (1-4)	48	4U rackmount	SCSI or Fibre Channel

[14] All capacities and transfer rates assume a 2:1 compression ratio. Your compression ration may vary based on the types of data stored.

7. Conclusion

Eliminating potential sources of error from the backup process increases backup effectiveness. With the availability of autoloaders, excessive operator intervention in the backup process is an avoidable pitfall. By reducing human involvement by 80-90%, an autoloader greatly increases reliability while eliminating the daily mundane, error prone, and often neglected task of tape swapping. The autoloader's integrated intelligence for emailing notifications of failing components or tapes, and ability to utilize spare tapes for replacement or overload, further ensures that backup reliability remains constant over time.

All organizations, regardless of size, must now value data backup as mission critical. An effective backup strategy must begin with the expectation that the need for data restoration, whether enterprise-wide or isolated, is inevitable. The risk of financial loss due to unrecoverable data is such a compelling reality that optimizing backup reliability as a top priority is necessary to secure business continuity and investment preservation.

The key to comprehensive data restoration is consistent and reliable data backup. The Tandberg Data Exabyte family of autoloaders and libraries offers any sized business an economically attainable solution that reduces the probability of human error, and improves overall backup operations efficiency and reliability.

COPYRIGHT

Copyright 2007, Tandberg Data Corporation. All rights reserved. This item and the information contained herein are the property of Tandberg Data Corporation. No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, without the express written permission of Tandberg Data Corporation, 2108 55th Street, Boulder, Colorado 80301.

TRADEMARK NOTICES

Exabyte, VXA, and VXAtape are registered trademarks of Tandberg Data Corporation. All other product names are trademarks or registered trademarks of their respective owners.

CONTACTING TANDBERG DATA

Tandberg Data Corporation
2108 55th Street
Boulder, Colorado 80301

(303) 442-4333

www.tandbergdata.com/us