

Backup Insurance, Are You Covered?



Abstract

Hardware strategies for performing backups and restores have far reaching effects on the nature and extent of application and data protection that can be achieved. Understanding the ways in which decisions about backup hardware affect the levels of protection available is an important part of determining the correct application and data protection strategy for an organization.

The concept of insurance can be useful when evaluating various backup strategies to understand the consequences of each. To support this process, GST has prepared this paper to clarify how the hardware decisions in backup strategies relate to the levels of insurance that the organization can deploy to protect its applications and data.

A dedicated manufacturer of tape storage solutions, GST, Inc. is providing this GST Research Report as part of its commitment to provide information leading to the better management of data and application protection within the IT industry.

www.gstinc.com/white/insurance.html



GST Research Report

Backup Insurance

Table of Contents

1. Backup: basic protection for applications and data	3
2. How backup strategies relate to insurance	4
3. Exposed insurance level: no backup hardware	5
4. Limited insurance level: single tape drive	6
5. Secure insurance level: dual tape drives with mirroring	6
6. GST Opinion	7
About the author and feedback	8
About GST, Inc.	8
Trademarks	8



GST Research Report

Backup Insurance

Backup Insurance, Are You Covered?

The increasing need to safeguard the organization's critical data and applications dictates the need to understand the affect that backup strategies have on the levels of protection. Insurance is a useful metaphor for evaluating available strategies.

The structural integrity, or vulnerability, of an organization today can be measured in part by the levels of protection that surround its critical data files and applications. Without current and working software that drives the inventories, receivables, operations, customer interface and the like, organizations cannot stay in business. This is also true for the data used by these applications.

The backup strategies that can be deployed each offer a degree of insurance protection that is vital to the organization's continued viability.

1. Backup: basic protection for applications and data.

The backup and restore functions still form the foundation for a host of activities that are necessary for the protection, resiliency and recovery capabilities of IT shops today. At the same time that organizations are becoming more dependent on continuously functioning IT-based systems, the environment for corporate computing is becoming more hostile.

Destabilizing forces that IT organizations face today include:

- Increases in the hurricane season for the US over the next ten years
- Natural disasters like forest fires and earthquakes
- New worldwide terrorism targeting highly visible American business facilities
- Global cyber terrorism targeting computer networks
- Sabotage by disgruntled employees
- Mounting costs from computer downtime
- Increasing customer expectations regarding service and availability
- Global business, causing the need for 24x7 operation
- Building and maintaining integrated databases
- The constant upgrading of servers for new hardware and software



GST Research Report

Backup Insurance

The more secure applications and data are made to be in an organization, the greater resiliency that organization has to withstand the forces that produce planned and unplanned types of server outages described above. The ways that you protect against server outages can be likened to insurance; the more of it you have, the easier it is to weather the troubles ahead.

We now know that organizations that loose access to their computer applications and data for periods as short as one or two weeks run a significant risk of going out of business within one to two years. This is particularly true when applications that demand a great deal of computing resources are lost, such as Data Warehousing, Data Mining, Business Intelligence, Electronic Data Interchange (EDI), Group Computing plus ERP super-applications like Manufacturing Requirements Planning (MRP), Supply Channel Management (SCM), Customer Relations Management (CRM).

The Gartner Group reports the following facts in connection with company disasters:

- 20% of all small to medium businesses suffer a disaster every 5 years.
- Nearly 75% of all U.S. businesses have experienced an interruption.
- 43% of all U.S. companies never re-open after an unexpected business interruption and 29% close within 3 years.
- 93% of companies with a significant data loss are out of business within 5 years.

2. Levels of insurance associated with backup strategies.

There are three basic backup strategies from a hardware standpoint. Each relates to a basic level of backup coverage:

- Exposed – No tape drive and no backup.
- Limited – One tape drive providing one backup cartridge set.
- Secure – Two drives providing duplicate cartridge sets.

In these categories, the tape drive can be in a tape subsystem or a tape library.

Although the first hardware strategy is a non-starter, it is mentioned here because all too often a file or application is not considered important enough to be included in the backup process, resulting in loss of time and information later when the information is needed but no longer available.

The second strategy, a single tape drive in a tape subsystem or tape library, is still the most common today. This basic backup configuration produces a single set of backup cartridges.

The third hardware strategy uses two tape drives in either a dual-drive subsystem or a two-drive tape library to generate identical sets of backup cartridges, called *mirrored backup*.



GST Research Report

Backup Insurance

Each of these three hardware strategies results in different levels of backup and disaster recovery protection that can be related to levels of insurance ... insurance that an organization invests in to protect against unexpected incidents that put the organization's application software and critical data files at risk.

The three levels of risk can be likened to three levels of insurance that we are all familiar with:

	Insurance Coverage		
	Exposed	Limited	Secure
Automobile			X
Dental		X	X
Disability			X
Home		X	X
Life			X
Medical		X	X
Vision			X

If no insurance coverage exists, this is ranked as *Exposed*. Some insurance in the most critical areas is rated as *Limited*. The highest level of insurance coverage can be rated as *Secure*.

This analogy can be useful in evaluating backup strategies. Naturally, the main choice is between *Limited* and *Secure*. Each carries its own levels of costs, protection and benefits.

3. Exposed Insurance Level: No backup hardware.

The failure to back up critical or even non-critical apps and data can be likened to skipping all forms of insurance. There is virtually no cost and no protection associated with this strategy.

Most IT installations recognize that it is mandatory to backup critical apps and data; anything to the contrary would put the organization's very existence in jeopardy.

With this in mind, ask yourself how wise is it to skip a backup on nights when production runs are overextended? Or when failed backup runs make it difficult to complete a tape backup operation successfully? The unintended consequences could be quite serious if such a decision were followed by an unplanned outage (as Murphy's Law would predict) that involved the destruction of some of the prior day's backup tapes; this could take a restore operation from taking a few hours to requiring days to fully restore all applications.



GST Research Report

Backup Insurance

4. Limited Insurance Level: Single backup tape drive.

The most common form of tape backup, and the most common form of backup insurance, is the use of a single tape drive to handle backup for one server. This hardware configuration functions the same from a backup standpoint whether it is one tape drive in a subsystem enclosure or one or more tape drives in a tape library that look and act like one tape unit to the server. The backup can only be written one tape at a time.

This configuration offers a level of insurance from a crippling failure that is deceptive. It appears to be good on the surface, but has serious drawbacks. It is generally adequate for handling planned backups, but can leave the organization exposed when unplanned backups (i.e., unexpected outages) occur.

This backup strategy forces several decisions to be made:

- Should the backup cartridges be kept onsite near the server and ready for restores, or stored offsite for better disaster recovery protection?
- If safely removed to an offsite storage area to facilitate disaster recovery, how do you overcome the delayed return of the backup set to the server if an unplanned restore is necessary?
- Should the backup cartridge set be copied using server cycles to produce a second set to allow both onsite and offsite storage of the backup set?

With only one tape drive in one tape subsystem or tape library generating one backup cartridge set, a failure during the restore process can turn a restore of 3 to 4 hours into a much more complex process lasting a day or more. This is like having an insurance policy that pays off up to \$10,000 in a hospital today, when a single day of hospitalization can run well over that amount....the policy sounds good until you have to depend on it.

5. Secure Insurance Level: Dual tape drives with mirroring.

The other form of tape backup strategy is *mirrored backup*. This type of backup uses dual-drives and a tape controller. This configuration takes the backup data from the server and then the tape controller makes two copies of the data so it can be written simultaneously to both drives. The controller places no extra burden on the server to make an identical set of backup cartridges for the second drive in such mirrored dual-drive hardware configurations. Mirrored backups work the same for stand-alone dual-drive mirrored tape subsystems and for mirrored drives in a tape library.



GST Research Report

Backup Insurance

The advantages of such mirrored backup hardware configurations are:

- An identical set of backup cartridge sets are produced at the same time.
- There is no impact on the server to generate the second backup cartridge set.
- One backup set can be safeguarded offsite for better disaster recovery while the second set is stored onsite for faster restores.
- Mirrored drives provide a fail-safe backup or restore in the case of a single drive or tape failure.

This last advantage above bears explanation. Since mirrored drives are always doing the exact same thing during the backup, if one drive fails or one tape fails, that drive shuts down and the backup operation continues to completion on the other drive. This process is identical for restore operations and can result in the saving of many countless hours if the failure occurs near the end of the restore process.

The mirrored backup function provides an extra level of insurance by generating identical backup sets at no performance cost to the host. It's like getting an extension rider to greatly extend the value of your insurance policy for just a modest additional investment.

6. GST Opinion: New level of mandatory insurance coverage.

A growing number of factors are driving organizations to harden, streamline and accelerate their backup, restore and disaster recovery processes. It has become increasingly apparent that greater margins of safety are needed for the backup process, like insurance that one hopes is never used.

The need to restore quickly from a system crash or other problem has placed great pressure on the backup operation to perform flawlessly. Yet with the huge volumes of transactions and file sizes today, the backup job is harder than ever. This collision of rising backup volumes and the need for less time to be tied up doing backups, has made fault-tolerant operations very critical. This fault tolerance is achieved with a dual-drive mirrored backup system. As a result, a new standard for **Mandatory Redundant Backup** is emerging. Whereas in the past, backups were not considered safe unless they were performed daily with a single tape drive, now the minimum hardware configuration for satisfactorily performing backups and restores is a mirrored pair of drives. We expect to see this trend grow, with the need for both an on-site set and an off-site set of backup cartridges becoming the minimally accepted level of backup to be performed.

With the added insurance of mirrored backups, the organization is better prepared to achieve fault-free backup/restore operations and simultaneously generate the needed backup set for supporting the disaster recovery strategy.



GST Research Report

Backup Insurance

About the author

This GST Research Report was prepared under the leadership of David Breisacher, CEO/Chairman at GST. David is the founder of several successful companies, including GST and BCC Technologies, a manufacturer of eServer disk, tape and memory storage devices. A visionary for the storage industry since the early 90's, David lends his market insight and predictions for the IBM midrange storage marketplace to the research conducted at GST. His experience in sensing shifts in technology and industry directions has made it possible for him to organize and structure successful companies to rapidly meet the evolving needs of storage users.

We value your feedback on this GST Research Report. Please send your comments, suggestions and questions to: research@gstinc.com

About GST, Inc.

GST, Inc. (www.gstinc.com) engineers, manufactures, markets and sells a line of innovative storage products to meet the need for high-performance, continuous reliability and cost-effective data storage. These products include tape solutions available today, and will include storage-related services, software and disk subsystems in the future. A comprehensive array of tape solutions range from single and dual tape subsystems, autoloaders, midrange tape libraries, to modular enterprise-wide tape libraries, with focus on improved backup and disaster recovery solutions. Modular design enables field upgrades, scalability, investment protection for existing GST tape solutions, and lower life-cycle costs. GST's product development is guided by several advisory boards to closely track market needs and fully utilize the latest engineering developments in product design. Complete information about products, support and company background can be found at the company's Website.

###

Trademarks

GST, InternalDR, EntryDR, SafeDR, AutoDR, GrowthDR, ScalableDR, Commander, BridgeLink, SanMatrix and StorMount are trademarks of GST, Inc. in the United States and other countries. AS/400, iSeries, IBM, UNIX, Linux and Windows are the property of their respective owners.