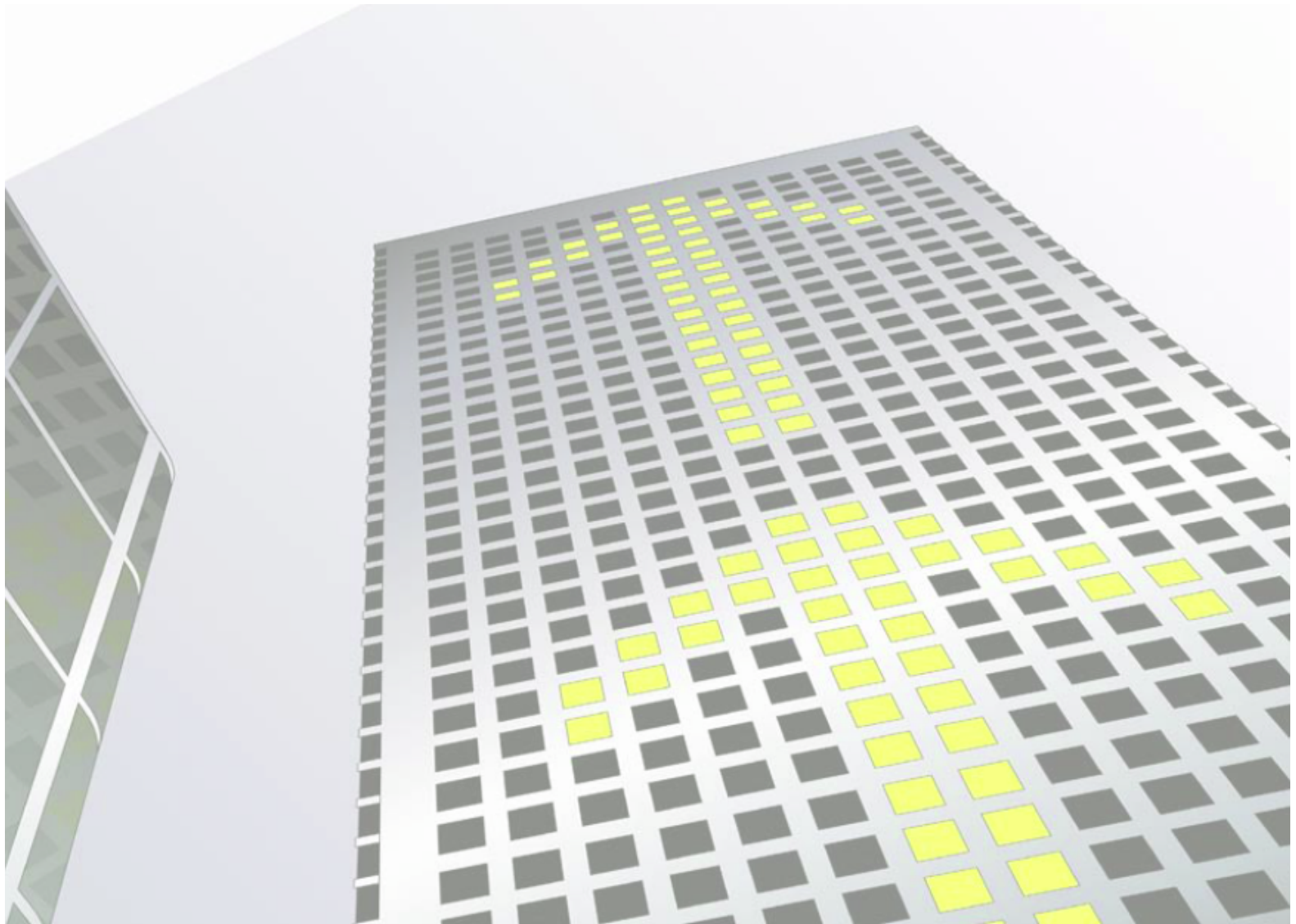


Protecting Critical Data in your Organization:

How to analyze your environment and identify solutions to address current weaknesses.



EXECUTIVE SUMMARY

There are many events that can cause problems – ranging from minor to catastrophic. There are natural disasters such as fire, flood and even regional power outages. Data is subject to hardware failure including servers, disks, disk controllers and so on. Perhaps most obvious is the threat from man-made factors -- data theft, corruption, and simple human error. Whatever the threat, the goal for every company large and small is to ensure that their data is protected.

Micro Strategies' unique consultative services and technology solutions enable a unified information management approach across a company's entire enterprise. Our solutions address business requirements and improve service levels, as well as satisfy data preservation, protection, and discovery obligations for corporate compliance.

DATA LOSS: IT CAN HAPPEN TO YOU

There are many assets that companies put a high value on: trademarks, brand names, human resources, competitive advantages, and the data that is the lifeblood of their organization. Perhaps the most valuable company asset is their customer's data. Protecting customer data is growing in importance for all businesses around the world. But what are we protecting this valuable data from?

Don't think data loss can happen to you? Data loss can occur at any time and is caused by any number of factors, including operating system or application software bugs, hardware failure and power outages and natural disasters such as hurricanes, earthquakes and floods. And you should never discount the human element. Man made disasters such as sabotage, hacking or viruses, and simple human error can use devastating loss of valuable data.

In the unfortunate event of a disaster, hardware and networks can easily be replaced and facilities can be moved to a new location. In fact, with the exception of data, virtually every company asset can be replaced. Therefore, the top priority should be to protect the asset that's most at risk and hardest to replace: your data.

Data pertaining to new and existing customers are the most critical to any business. Marketing departments depend on data to identify and target new customers. Sales departments rely on information to understand customer needs and effectively build relationships. Customer service representatives use these data to deliver the highest levels of service. For businesses today, the loss of customer data can have an incredibly negative impact in real dollars, lost opportunity, customer dissatisfaction, shareholder insecurity and overall corporate image.

DATA LOSS: IT CAN HAPPEN TO YOU

With the realization that any business – including yours - is at risk, comes the question: how can we protect our critical data? The answer is to develop a strategic plan, and the first step before you develop a plan is to ask some critical questions.

- Is your data backed up? Have you restored your backup data to ensure the backups are accurate?
- Is ALL your data backed up? Servers, Clients, Laptops and mobile devices?
- How much downtime can you tolerate? Minutes, hours, days?
- Are you backing up only data? Do you back up your applications?
- Are your tapes protected against data theft?
- What happens if you lose a tape or if a tape gets stolen?
- How long would it take you recover a server, its application and data in the event of a failure?
- Is your sensitive data encrypted? Is your sensitive data used for testing encrypted or masked?
- Is your data on high availability storage? Can you mirror data across different vendor storage arrays?

With these critical questions addressed, it's time to develop a strategic Data Protection Plan. By aligning a well-designed program with an overall data protection strategy, you can gain control of sensitive data, reduce the cost of data breaches, and achieve greater visibility into how data are used throughout your organization. There are three key steps every business should take when developing their unique plan.

Step #1 - Defining DATA

Before you can protect your data, you must define what data is in the environment and what value is assigned to it. Data itself can be diverse. We typically define data in broad terms such as structured, data within a database, unstructured, and everything else. Data can be classified as production, test, archive, and backup.

Data exists in many places within a typical customer environment

- Disk drives
- On servers – mail, database
- On client machines – executives, HR users, Accounting
- External storage – SAN, network storage, flash drives
- PDAs, Smart Phones
- Backup media – tape cartridges, CD/DVD, USB drives
- Network Storage Appliances

A company may put a high price on their customer and order databases, and may assign a lower value to internal documents on a file share. The value is based on how much will down-time cost, how long the company can function in the event of a complete loss of that data, and how critical the recovery time is. System administrators today are typically working under pre-set guidelines that dictate what is acceptable.

For example, guidelines may require that - in the event of catastrophic failure - all major systems must be back up and running within 24 hours. Any longer than that and the company itself may be in danger of going out of business. The National Archives & Record Administration in Washington reports that 60% of companies that lose their data will shut down in 6 months of the disaster. And yet, according to the Global State of Information Security Survey 2007 (GISS) by PricewaterhouseCoopers LLP, CIO Magazine, and CSO Magazine, more than two-thirds of organizations maintain neither an accurate inventory of user data nor a list of locations and jurisdictions where this information is stored.

Step #2 - MAPPING THE CUSTOMER ENVIROMENT

The second step to protecting data is mapping the network environment. Creating a conceptual overview is the foundation to this process and it can be as simple as a basic chart.

All too often we stop here and focus only on the major server elements in the environment. Don't forget about the client systems – 70% to 80% of customer data lives there and less than 8% of companies back this up. Some customers may also have a Storage Area Network (SAN).

Once you have a good idea of what the environment looks like, and have combined it with perceived downtime costs, you can begin the analysis on how data can best be protected.

Step #3 - PROTECTING THE DATA

At the Hardware level

There are several foundational technologies that can be used when protecting key data. The first place data is protected is at the disk drive level. When disk drives are manufactured the vendor typically measures the Mean Time Between Failure (MTBF) or Mean Time To Failure (MTTF) of a disk drive. This is a measure of how long the drive is expected to function based on population data. In a production environment disk drives are typically put into a RAID (Redundant Array Independent Disks) configuration which eliminates the threat of the disk as a single point of failure. Some companies may also have a Storage Area Network (SAN), to help minimize the many 'islands' of data storage. Typically, a storage area network is part of the overall network of computing resources for an organization.

SANs can be difficult to manage in a multi-vendor environment and the Solutions Architect needs to understand that in this type of environment, often with a combination of diverse operating systems and vendor storage devices, some combination of technologies could be required to ensure that the SAN is secure from unauthorized systems and users.

At the Software level

The most important foundation piece from the software perspective is the implementation of backup and archive software such as Tivoli Storage Manager (TSM). TSM helps the customer address storage challenges posed by the emergence of new compliance requirements, the ever-increasing explosion of data, and application performance issues. TSM manages the movement of data from disk to disk or disk to backup media.

This is important because it allows a company to move data to tapes, index all data and move copies of the data off site in the event of a catastrophic failure. TSM extended edition also includes disaster recovery (DR) and reporting features so the customer can keep their DR plan as current as their last backup.

There are four basic concepts to understand when discussing TSM as a solution to protect data:

- **Backup** – The single most important step in protecting your data from loss is to back it up regularly. Backing up your data creates a copy of a file to protect against the operational loss or destruction of that file. Companies control backups by defining the backup frequency and number of versions.
- **Restore** – Places backup copies of files into a designated system or workstation after the loss of a file. By default, the most recent version of each active file requested is replaced.

Step #3 - PROTECTING THE DATA

- **Archive** – Creates a copy of a file or set of files for vital record retention of data, such as patent information, financial information, or customer records. Companies control archive by defining the retention period. This feature enables customers to keep unlimited archive copies of a file.
- **Retrieve** – A function that allows the user to copy an archive file from the storage pool to the workstation. The archive copy in the storage pool is not affected. A descriptive tag can be added to a file for easier file retrieval.

The latest version of TSM has several new features including native data de-duplication, DB2 database, enhanced support for IBM N series and NetApp filers, enhanced support for VMware, item level recovery for Microsoft Windows Exchange, granular support for Windows Active Directory, IBM General Parallel File System Support and enhanced DB and application protection through advances in copy services.

TSM also has a wide variety of agents performing special tasks for applications that are difficult to back up. These applications typically always have open files - forcing companies to schedule outages in order to get a clean backup of the data. (Most backup applications will skip open files since they can't back them up.) TSM has several agents including mail (Domino and Exchange), databases (Oracle and SQL, DB2 is included in the base product), and ERP (SAP databases). There are also agents that perform hierarchical storage management, direct backups over SAN networks, storage archive manager for backing up compliant storage arrays like DR550 and EMC Centera, create portable recovery media, do bare metal restores and integrate with native hardware backup features.

One of the most troublesome backup issues companies contend with is backing up user workstations and laptops. IDC and Gartner studies show that 70% of corporate data resides on desktops and laptops, but fewer than 8% are backed up. Micro Strategies supports two IBM solutions to address this issue - TSM and Tivoli Continuous Data Protection (CDP). TSM may be overkill for many companies when it comes to backing up client systems, because they don't want or need the structure and requirements that TSM imposes. Consideration should then be given to Tivoli CDP, a light-weight client that loads on a company's client systems, and can be used to target specific directories and files.

Step #3 - PROTECTING THE DATA

Once Tivoli CDP is implemented, it will immediately make a copy of a file when it is accessed and keep multiple of versions (customer defined) of that file. Companies will typically define a network file share for the client system and continuously back up the client files to that directory. The IT department will then use TSM to back up the file server with all the client shares on it. If the client system cannot access the file share, CDP will wait until the share becomes available and then write all the files to the target - making it ideal for laptops as well as desktop computers.

Integrating Hardware and Software Solutions

Integrating TSM with other storage hardware and software solutions helps companies access, protect, manage and deliver information more efficiently. For Microsoft applications that require high availability and fast restore you can add Tivoli FastBack. Tivoli FastBack continuously backs up the Microsoft Server and Application by implementing a block level backup of that server. A typical company uses Tivoli FastBack to back up the server and take several snapshots of the server throughout the day - so the server can be restored to a point in time. The benefit of having Tivoli FastBack running at the block versus the file level restoration is speed, allowing applications and entire servers to be backed up in a matter of minutes versus hours or days. If a business interruption occurs, the company has accurate and up-to-date data to quickly restore business data and operations. Tivoli Key License Manager (TKLM) protects customer tapes – ensuring that if a tape cartridge is lost or stolen, the data on it cannot be read.

The best method for protecting sensitive customer data on removable media or within databases is simple: encryption. IBM Database Encryption Expert (DB2) provides high-performance encryption, making it practical to encrypt all sensitive data. DB2 can protect sensitive information in both online and offline environments and has centralized policy and key management to simplify data security management. By adding this solution, customers can restrict data access to only those users, applications and processes that should have it.

All too often IT managers do not know where confidential data is stored or how it is related across disparate systems. An ideal data protection solution must do two things: discover sensitive data across related data stores, and mask it effectively. IBM Optim Data Protection provides comprehensive capabilities for masking sensitive data effectively across non-production environments.

Step #3 - PROTECTING THE DATA

For companies looking to reduce both the complexity and cost of managing their SAN-based storage, there is IBM SAN Volume Controller (SVC). SVC enables protection by allowing data to be mirrored on different vendor hardware. For example, customers can mirror a disk volume that is on an IBM SAN with a disk volume that is on an HP SAN.

Having the right information-protection strategy can provide you with a competitive advantage and minimize financial and reputational risks. Importantly, having confidence in your information protection allows you the greater freedom to “push the envelope” in your business.

About Micro Strategies: Established in 1983, Micro Strategies has distinguished itself as one of the most innovative technology solution providers on the East Coast. An industry leader, Micro Strategies is at the forefront of architecting and implementing quality solutions with a commitment to responsive, client-first service. Micro Strategies provides Business and Infrastructure Solutions for companies of all sizes. Our comprehensive solutions are centered in the following practices:

Advanced Infrastructure - Complex software, storage, and server solutions including Platform and Application Services. Innovative backup and disaster recovery solutions. IBM Smarter Planet / Dynamic Infrastructure solutions.

Business Information Management and Protection – A consultancy that focuses on the management, archival, retrieval and preservation of information to meet regulatory compliance and corporate governance.

Business Systems Integration - Design, implementation, support and training for networking, infrastructure, and business applications. Together with our core partners, we provide industry leading technology solutions, and deliver our custom solutions to meet our clients’ specific needs.

Enterprise Content Management - Design and deliver solutions that help organizations manage all unstructured information (documents, emails, faxes, PDFs, voice messages, etc.) and provide the associated business processes of creating, routing and disposition.

Innovation Center - A showcase for our technical, creative design, and problem solving skills in support of our leading edge technologies. The lab environment is comprised of \$2.5M+ of technology that is available to our clients for demonstrations, Proof of Concept, benchmarking, and training.

Contact Rosary De Filippis, rdefilippis@microstrat.com or (973) 625-7721, or visit microstrat.com.