Data security challenges in a distributed world

Data security was once something only the IT staff cared about. Customer lists, new product designs and financial reports were kept on mainframes in well-protected data centers, and could be seen only by users who were in the office or logged onto a terminal. Nobody had an easy way to download or copy large databases.

Today business-critical information is forever on the move from mainframes to departmental servers to notebook computers to on-site and off-site backup. Today, virtually every business must be able to operate electronically, which includes processing orders, scheduling production, completing transactions and providing customer service. This vast distribution of mission-critical data, while necessary to compete, also creates new challenges: It is much more vulnerable to theft or corruption.

Security failures, such as losing backup tapes that contain personal customer information, causes the culpable company embarrassment, lost sales and falling share prices. At the same time, financial scandals and privacy concerns are driving regulators and consumers to demand bullet-proof protection for sensitive information. With penalties for data breaches so high and so immediate, data security is now a strategic priority not only for IT, but also for business directors up to and including the corporate board.

Whether an organization integrates the necessary technology, people and processes itself or relies on a solution provider, it must meet a new set of basic requirements for data security. These include central management capabilities and automated processes that do not rely on overworked or non-technical users to carry out key security tasks. Security risks must be mitigated through data encryption, the use of processes and procedures validated by recognized third party experts, the ability to secure backup and restore processes, and the ability to monitor and readily prove the effectiveness of data security measures to regulators and stakeholders.

With regulatory compliance, corporate reputation, and even disaster recovery at stake, organizations must continually monitor the security of data in transit and at rest, and do everything possible to mitigate risks.

What's Driving Data Security

Regulatory Requirements

The ever-increasing role digital information plays in the economy has elevated the level of scrutiny over how it is stored and protected, with both government and industry groups placing new security demands on organizations of all types. The Sarbanes-Oxley Act, for example, requires public companies to have appropriate safeguards to maintain the integrity of financial records. The Payment Card Industry Data Security Standard requires, among other things, that any and all cardholder information in storage be protected by encryption or similar technologies. In the modern economy, effective data security is a prerequisite to compete and to avoid regulatory reprimands such as fines, or even jail sentences.

Key Regulatory Data Security Requirements

Section 404 of the Sarbanes-Oxley Act requires business managers and auditors to attest to the business' controls over the gathering and calculation of financial results. Services providers under contract to the business must be SAS 70 Compliant.

The Payment Card Industry Data Security Standard requires that cardholder information stored anywhere be protected by encryption or similar technologies.

The Health Insurance Portability and Accountability Act (HIPAA) requires that healthcare institutions keep patient information confidential and destroy them between two and five years after the patient's death.

SEC 17a 1) defines which records financial institutions must create and maintain; and 2) defines the media requirements and conditions an institution must meet to store electronic records. Retention periods range from three to six years.

Department of Defense 5015 Standard requires efficient creation, retention, archiving, retrieval and disposal of data with security confidentiality.

Business Ramifications

Even where regulations do not require data security, the marketplace does. Over the last several years, a string of high-profile companies and institutions have reported the theft or loss of backup tapes containing millions of consumer records. Such incidents cause and instant and dramatic surge of bad publicity for the organization, a drop in consumer confidence, possible lost sales and even reductions market share and stock price. A survey performed by the Ponemon Institute of 14 companies who had experiences a consumer data breach showed they lost and average of $13,800,000.00 as a result, with almost half of the loss—$6.7 Million—resulting from customer attrition.

Moreover, a 2004 survey of 388 storage professionals conducted by the Enterprise

Storage Group showed that 27 percent had either experienced a data security breach, couldn’t tell if they had suffered such a breach or didn’t know.

The Challenge of Secure Data

Distributed Data

The decentralized, Web-centric nature of today's businesses means that data, and the control over it, becomes more decentralized. That creates a host of new data storage vulnerabilities.

When companies outsource product design, customer service or back-office accounting, critical customer, product and price data gets moved to servers in various departments, remote offices, or at customer and supplier sites. This means that data security is suddenly dependent on a milieu of unknown and uncontrollable factors such as:

1) physical security at the remote site
2) the technical safeguards in place on the site's server
3) storage and network infrastructure, and especially
4) the quality of the security processes and security staff at that site.

Access Control

With data being used and stored remotely, access control becomes more challenging and complicated. A customer service representative in an offshore location may need to see certain customer information such as account number and last product purchase, but not credit card or Social Security numbers. How do you guarantee that one, and not the other, gets revealed?

Creating and enforcing proper access control policies is critical to ensure that only the appropriate users see various types of information, but sometimes more importantly, to prove these policies are being enforced. Without such policies, an unscrupulous user or administrator could easily access, corrupt or steal data.

Backup Vulnerabilities

Many organizations send data here and there across their own networks to implement Information Lifecycle Management (ILM) strategies, in which data is moved to different storage platforms as its value to the organization changes. Trouble is, these networks are very vulnerable to all the viruses and worms constantly circulating on the public Internet. If

administrators fail to apply the latest security patches to their software, update antivirus software or properly configure firewalls, this data is at risk.

Backup software used to move data from production storage systems to the backup target is of particular concern. In the past year, storage experts discovered critical vulnerabilities in popular backup products, including Veritas NetBackup, Backup Exec and Storage Exec, Computer Associates' BrightStor ARCServe, EMC's Legato Networker and Sun's StorEdge Enterprise Backup Software.

Internal Threats

Any organization dealing with sensitive data, but especially those in industries such as financial services, must guard against unauthorized corruption or deletion of information by insiders as well as outsiders. Employees are the second most likely source of security-related events, accounting for 33 percent of security events in 2005, according to the State of Information Security 2005 conducted by *CIO* magazine and PricewaterhouseCoopers.

Nobody's Perfect

Human error is another major threat to data security. In the same ESG survey referenced above, 33 percent of the respondents reported that mistakes are the greatest data security threat.

Human error takes many forms: A storage administrator might give a password to a thief claiming to be a legitimate user who has lost his password, or a storage administrator may not properly configure a switch on a storage-area network, or a busy user at a remote site could fail to do an end-of-day tape backup.

Skilled staff with the time to devote to security is key.

33 percent …

… the percentage of security events caused by employees in 2005, according to the State of Information Security 2005 conducted by *CIO Magazine* and PriceWaterhouseCoopers.

… the percentage of storage provessionals who told the Enterprise Strategy Group that mistakes are their greatest storage security threat.

Solution Requirements

While every organization's needs are unique, there are some common denominators when it comes to the key requirements for mitigating data security risks. These include the ability to centrally manage storage, providing at-once access (as well as protection) to stored data, preventing data corruption, monitoring systems and processes, and proving the effectiveness of data security solutions in real-time.

Centralization

It is impossible to protect what you cannot find, or do not even know is there. But many organizations find themselves in this situation more often than they care to admit because of the widespread use of notebook computers, email and Web commerce sites. Analysts estimate that 60% of company data is created and stored outside of the corporate data center, making it imperative to implement storage solutions that not only centralize this data, but also verify that it is properly categorized and protected according to corporate policies and procedures.

Authentication/Authorization

Authentication in the context of data security means verifying that people are who they say they are; authorization is the process of controlling which information each user can see, and what actions they can take with that information. Data security solutions must support detailed and granular policies to ensure that all users (whether within or outside of the organization) do not receive overly broad access; they must also support audit trails that verify proper security and access policies have been followed.

Encryption

Encryption ensures that even in the event of improper granting of access to information, it cannot be read. Encryption is particularly important for data backed up over public networks such as the Internet. Support for high levels of encryption such as AES is the standard in some industries and for particularly sensitive data.

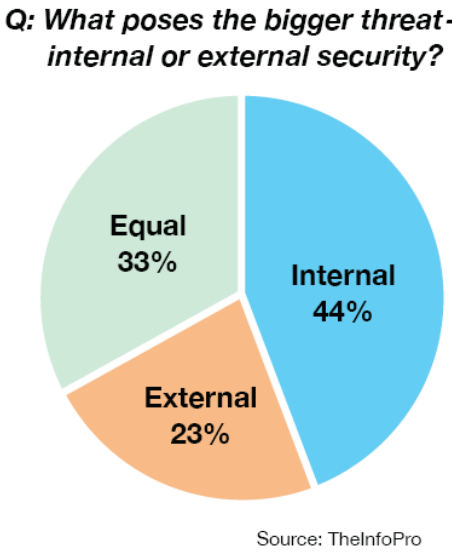
Data Restores

Security is counterproductive at best if it keeps legitimate users from accessing the information necessary to do their jobs, or if it keeps employees from easily recovering files or emails that get

accidentally deleted. Data security solutions should allow users to easily recover backed-up data without expensive help from the IT organization and without interrupting other back-up processes being run for disaster recovery or business continuity.

Eliminating Tape Backups

The theft or loss of data from backup tapes is one of the most common and embarrassing lapses in data security for many large companies. The vulnerability arises not only because the tapes must be moved off-site for storage and archival, but because they often are left unencrypted or even include a tape header utility that describes how to read the tape. Companies should look for disk-based backup systems that transmit encrypted data over networks to eliminate this potential cause of data loss.



Network Security

An organization's storage infrastructure must be tightly protected with technology such as a firewall configured to permit access to only the port required to provide storage services. The firewall and other security systems must be monitored 24x7 to provide real-time response to any threats.

In addition, policies requiring periodic changes to user passwords and the use of encryption to protect passwords are also critical.

Virus Prevention

Viruses are a common cause of data corruption. Yet many common viruses can be blocked with intelligently designed storage systems, as well as the proper application of security patches and updating of antivirus programs. Security solutions should include both the best technology and the best practices in virus detection and mitigation.

Corruption Prevention

More and more companies, particularly those in highly regulated industries, are being required to prove that key data has not been altered since it was first stored, and that they can restore corrupted data to its original state. Storage solutions must be architected to block viruses and worms which can corrupt data, and may also require the use of systems which can prove that data has not been altered since it was first stored.

Monitoring

Security defenses must be monitored to be effective, and staff must be able to pinpoint and fix vulnerabilities when they are discovered. Data security solutions should include real-time monitoring of defenses such as firewalls and intrusion detection systems, and integrate best practices in threat response.

Staff Skill Sets

Security requires constant vigilance from skilled professionals trained in the latest threats, and experienced in handling issues ranging from physical security to database and application access control. Whether within the organization or at a solution provider, security staff cannot work at peak effectiveness if it is overwhelmed with other IT responsibilities.

SAS 70 Certification

SAS 70 (the American Institute of Certified Public Accountants Statement on Auditing Standards) Number 70 documents the findings of an independent review of the controls of an organization which stores data. A SAS 70 report represents an assurance by a trusted, outside observer that an organization’s data security technology and processes meet industry standards. Increasingly rigorous mandates such as Sarbanes-Oxley make SAS 70 audit reports even more important to measure and report on the effectiveness of internal data security controls.

Thinking It Through: Implementing Secure Data Protection

Properly securing data across the value chain and throughout its life cycle can require significant investment in both technology, skilled IT staff, time, and resources to develop, implement, monitor and provide training for multiple policies and procedures.

Businesses can always make these investments themselves, but there are also managed storage services providers that already have infrastructure, policies and skilled staff in place to ensure protection of critical data, wherever it resides. Should a business wish to build from the ground up or seek to partner with a service provider, the following are the factors it ought to consider.

• Centralization: Maintain a secure, remote location at which data from multiple locations can be centrally stored and secured. Pysically protect the facility with best practices and a state of the art network infrastructure.

• Authentication/Authorization: Implement multiple levels of controls to authenticate users and administrators. Control their access to data; define which activities they can perform and which data they can view or act upon.

• Encryption: Look to build SSL, a 128-bit Advanced Encryption Standard (AES) encryption for network communication, into the client and server software. Ideally the system will not need security keys.

• Eliminate tape backups: Tape cartridges holding unencrypted data are a tempting target for thieves, and all too easy to lose while en route to off-site archives. As such, the ideal process is to back up data off-site using encrypted network links. Then, when storing the data at rest, distribute components of each file across multiple disks to make it even harder for unauthorized users to access.

• Data Restores: Unlike tape, disk-based backup allows users to restore their own files without interrupting other backup jobs or reducing overall system performance.

• Network Security: The best protection for a storage platform is a Netscreen firewall configured to permit access only to the port required for the storage services. Tripwire software ensures no unwanted changes get made to the file system. Users must change \ passwords every 45 to 90 days, and passwords are stored in PGP encrypted files.

• Corruption Prevention: Store all data and indices in a content-addressed store (CAS), which uses mathematical hashes to verify that data has not been changed since it was first stored. Ideally, companies ought to verify the integrity of each piece of data every day, and restore to the original, uncorrupted data as needed.

• Virus prevention: Systems should be architected to prevent storage of any infected data, and to eliminate any risk of a virus spreading into other data. Companies should also consider patch management services to ensure the latest and best virus prevention has been applied to their storage systems.

• Monitoring: Whether self monitoring a system or relying on a service provider, the only surefire method is 24x7 real-time monitoring of network firewalls and intrusion detection software protecting storage networks. Companies also ought to monitors all systems for file system changes as well as malicious traffic.

• Staff Skill Sets: Internal IT staff has many responsibilities, so it is important to build a dedicated staff that focuses full-time on maintaining and improving on best practices for data protection. This skilled, experienced staff should have the know-how to handle every mode of challenge, ranging from physical security through access control, ensuring the latest security patches have been applied to critical systems and monitoring vital processes such as backup and data replication.

• SAS-70 Certification: If hiring a service provider, ensure that its processes and procedures are certified by the Statement on Auditing Standards No. 70 Type II (SAS 70). A SAS 70 certificate is widely recognized because it signifies that a service

organization has been through an in-depth audit of its IT and related processes and controls.

SAS-70 simply demonstrates that a service provider's procedures are optimized to host or process data belonging to customers. This is extremely important for customers subject to Section 404 of the Sarbanes-Oxley Act, which stipulates the company must report on effective internal controls of service organizations serving it.

Conclusion

To be sure, today's business climate has created a highly complex data protection custody chain. Companies must replicate more and more sensitive data in order to protect it, but there's a catch. The more data a company replicates, copies and backs up, the more data it must secure and the more vulnerable that data becomes.

When you add to this the fact that most companies create and use mission-critical data on remote servers, desktops and laptops, the security challenge becomes even more pronounced. To meet it, companies must rethink the controls, reporting mechanisms and staff skillsets necessary to manage, monitor and police distributed data.