

The Paradox in Data Storage

Disaster Recovery vs. Record Retention

White Paper



Table of Contents

| | |
|---|----------|
| Introduction | 3 |
| The data you store can be used against you. | 3 |
| Who's Responsible | 3 |
| Paradox: Backup vs. Record Retention | 3 |
| Legislation and Litigation | 4 |
| Legislation | 4 |
| Litigation. | 5 |
| In The Court Room | 6 |
| Summary of Issues | 7 |
| Meeting Compliance Requirements..... | 7 |
| Applying Information Life Cycle Management best practices | 8 |
| How Can LXI Help | 8 |
| About LXI | 9 |

Introduction

The data you store can be used against you.

Can you imagine having a backup that will cost your company millions of dollars? Could it be possible that your backup tapes (whose only purpose is for disaster recovery) are the source of evidence used for a criminal proceeding against your company? Alarmingly, not only are these scenarios possible, but, today, more and more often both scenarios have become common place. The fact is that your well intentioned disaster recovery plan, with all its built-in redundancy for data protection and conservative retention practices, can provide data that can be used against you in a court of law.

Who's Responsible?

With the introduction of Section 404 of the Sarbanes-Oxley Act, all publicly traded companies must include in their annual report a statement signed by both the CEO and the CFO attesting that the information contained in any SEC filing is accurate, and the company is willing to submit to an audit to prove that accuracy. If the audit proves the reports to be incorrect the individuals that signed will be held personally liable. This sobering requirement will no doubt be transferred to IT management. The CIO, IT Directors and managers will all be held to a higher level of accountability by those individuals that sign their names and trust in the accuracy of the systems that produce the information. Private firms, although not governed by these rules, should also abide by the spirit, intent and letter of the law, because someday, through IPO or acquisition, these rules may apply.

The CIO, IT Directors and managers will all be held to a higher level of accountability by those individuals that sign their names and trust in the accuracy of the systems that produce the information.

The Internal Revenue Service provides, in Rev. Proc 91-25, additional liability to consider. Any individual that willfully fails to supply requested information to the IRS can be subject to jail and fines up to \$25,000 if convicted. Companies can also be fined in excess of \$100,000 for failure to comply with IRS requests for information.

With just these two examples, it is clear that regardless of what legislative body or regulatory agency set the requirements for your industry, IT professionals must understand that they are not insulated from liability and can be held personally accountable.

Paradox: Backup vs. Record Retention

Traditionally, data stored on backup tapes is thought to be valuable only if it is needed for recovery purposes. The goal of a backup is to create a temporary copy of the data on a less-expensive media that can be accessed and restored in the event the primary data is destroyed, lost or corrupted and only accessible by a limited number of IT personnel. A second type of data storage is becoming more and more important: Record retention (sometimes referred to as archiving) has a primary goal of moving active information to durable, less-expensive, long-term accessible storage media that is made available to many authorized personnel.

Paradoxically, the objectives of disaster recovery and record retention are completely different. Disaster recovery strategies tend to protect as much data for as long as possible and once expired, little attention is given to the old data's retention. On the other hand, record retention practices are designed to store data for only as long as absolutely necessary with specific actions to dispose of that data once it is expired. In short, disaster recovery stresses that more is good, while record retention emphasizes that less is better. IT managers must take a new look at how, why and for how long data is stored as backups and begin initiating record retention policies along with disaster recovery practices or face the consequences uncontrolled data life cycle management now presents.

Disaster recovery stresses that more is good, while record retention emphasizes that less is better.

By calling for regular backups to be stored apart from the originating host system, IT organizations have strived to ensure that their company not only survive disasters but also be able to recover an up-to-the-minute image of the failed system. Many managers, however, mistakenly assume that by doing regular backups they are also satisfying their record retention and regulatory requirements simultaneously. Procedurally, the old bias to keep backups longer than absolutely necessary and once expired, give little concern to the disposal or destruction of the data is a risk that many IT professionals don't clearly understand.

Legislation and Litigation

Legislation, litigation and renewed focus on corporate governance has forever changed the importance of knowing the value of data throughout its life cycle. Managers that depend upon their backup strategies to provide both recovery and compliance are exposing not just their company but themselves to extensive liability. Two distinct motivations are emerging for IT organizations to re-address the way they store data; Legislation and Litigation.

Legislation

Legislation such as the Sarbanes-Oxley Act and HIPAA (Health Insurance Portability and Accountability Act of 1996) has been introduced to protect the individual while reinforcing accountability and corporate governance. This renewed emphasis on process controls leads directly to the IT department as HealthSouth's CIO, Kenneth Livesay, demonstrated when he pleaded guilty to charges of falsifying financial information. In most instances, the legislation enacted is not specifically targeted at IT, however, the fundamental intent is to ensure that adequate, appropriate and auditable controls are in place and, more importantly, being followed. Therefore, since IT is responsible for the systems that generate, change, house and transport data, CIO's have inherited the responsibility to implement controls that ensure the information systems stand up to audit scrutiny. In short, the government is attempting to legislate good business practices.

The interpretations of legislation are always challenging and most times confusing. The following attempts to present a high level examination of several of the most notable enactments and rules facing corporations:

Since IT is responsible for the systems that generate, change, house and transport data, CIO's have inherited the responsibility to implement controls that ensure the information systems stand up to audit scrutiny.

HIPAA – Health Insurance Portability and Accountability Act of 1996

- Limits the use and disclosure of individually identifiable health care information
- Requires health care entities to establish administrative, physical and technical safeguards

Sarbanes-Oxley Act of 2002

- Changes securities regulations, corporate governance, and auditor regulations
- Response to Enron, WorldCom, ...
- Introduces accountability for fraudulent accounting practices

Gramm-Leach-Bliley Act

- Requires financial institutions to take steps to ensure security and confidentiality of customer's non-public, personal information
- Privacy notice must be "clear and conspicuous"
- Must provide opt-out process

IRS Revenue Procedure 98-25

- Computer records must be retained in retrievable format, made available to the IRS when requested, along with documentation and audit trails that provide evidence of authenticity and integrity. Must also convert old formats to current, accessible by IRS representatives, sequential file version relational database systems and detailed transactions involved in EDI commerce.

IRS Revenue Procedure 91-59

- Records must be maintained and be available regardless of the existence of the original software or hardware, and no exceptions are made for deteriorated media.

Federal Rules of Civil Procedures; V. Dispositions and Discovery:

- Rule 26: Quick identification and reproduction of requested information
- Rule 34: Sets the rules for requesting data under Rule 26; firmly establishing how electronic evidence is to be handled in lawsuits
- Rule 37: Failure to make disclosures or cooperate in discovery sanctions

Litigation

While compliance enforcement has caught the attention of the press and senior management, stored data presents a second exposure. Litigation has become every bit as threatening as failing to meet all compliance requirements. The risk that data on backup tapes will be subpoenaed for discovery purposes under the Federal Rule 26 and used in civil actions against your corporation presents an even bigger challenge. Steve Davidson, Chairman of the Intellectual Property and Information Technology law department of law firm Leonard, Street, and Deinard in Minneapolis describes three reasons for the increased use of stored data in litigation. "First, more companies and more attorneys are aware of the existence of electronic evidence. Second, the courts now recognize how important this kind of evidence can be. And third, the sheer volume of electronic records – all of it evidence or potential evidence – is increasing every minute of every day."

In the Court Room

Stored data can be used against you in several ways. IT managers must understand the implications of the four example rulings and implement controls that ensure timely compliance to discovery requests:

1. In an action brought against Crown Life Insurance Company the judge did not accept Crown's argument that "backups don't count." The court's ruling found that if data is stored on media, regardless of its purpose, that data must be produced when requested.
2. Wyeth Corp. contested that the cost to recover data from the backup tapes would be too expensive and therefore be an unreasonable request. The court ruled that the cost to produce the requested information did not exclude the defendant from complying with the discovery request. One conservative estimate places a \$2,000 price tag on each backup tape that must be searched. In some instances, a company may want to settle out of court rather than fight, because the cost to identify, restore and produce the requested information will be significantly more than the cost to settle.
3. In a well publicized ruling, Prudential Insurance Co. was ordered to pay a \$1 million penalty for having what the court described as a "haphazard" data retention policy. Prudential's inability to enforce a reasonable and consistent data retention policy was serious enough to warrant a seven-figure fine.
4. Sprint Communications and Arthur Anderson provide two examples of inappropriate use of data retention (and destruction) practices that caused significant problems. Both companies were found to have destroyed data relevant to pending legal actions. The argument that the data was destroyed under normal retention policies was rejected by the court. The ruling stated that companies have "an affirmative duty" to preserve data that could be relevant to a pending case.

The risk that data on backup tapes will be subpoenaed for discovery purposes under the Federal Rule 26 and used in civil actions against your corporation presents an even bigger challenge.

Each case highlights the significant exposure that IT managers and their companies now face, especially since "ignorance of the law is not a defense."

It is imperative that expired data be removed from any backup tape - that includes those used for archiving, or record retention, and those used for regular backup.

Summary of Issues

Good record retention practices are not achieved through regular backup processes.

- There are significant penalties for failure to implement good record retention strategies.
- Government and regulatory agencies are introducing more stringent requirements regarding record retention.
- Data on backup tapes can be used against you in a court of law.
- IT management must understand the risks and implement controls to reduce the risks.

Meeting Compliance Requirements

In general, regulatory agencies do not advocate specific compulsory technologies. There are exceptions, of course, such as the SEC's requirement in Rule 17a-4 that investment brokers-dealers must use "write once, read many," or WORM technology to archive transaction data along with email, but even that is up for debate. More often, legislation attempts to follow the recommendation best defined by the Centers for Medicare and Medicaid Services on its HIPAA Fact Sheet on Security Standards Final Rule. Standards are "...Technology neutral – The standards do not specify any particular technology. They outline what must be done, not how to do it."

By keeping the compliance wording vague, legislators have attempted, in regulations such as HIPAA and Sarbanes-Oxley, to take into account that a company's size, business complexity, capabilities, and cost to comply, directly effect how well and how quickly a business can become compliant. In the same way, the courts have not established exacting standards for complying with discovery requests. Compliance as John Hagerty writes "is a process, not an event." The best defense against exposure to legislation, litigation or disaster is found in the implementation of existing "best practices" with a focus on process.

The importance of developing procedures, practices and policies that ensure compliance must be a boardroom initiative. Without buy-in from senior management, compliance programs are destined to fail or at best fall short of fully meeting all requirements. CEO's must see that the requirements are more than financial burdens and must understand that IT plays a significant role in providing the infrastructure for the covered information. Budget must be approved to evaluate how data is used, where it resides and what safeguards are already in place. Then, once the budget is in place, objectives must be defined that address the high level requirements of disaster recovery and record retention.

The common objectives of information life cycle management that address the majority of legislative, litigation and disaster recovery requirements are:

- **Information Security:** Establish procedures and mechanisms that protect the confidentiality, integrity and availability of electronic information
- **Information Administration:** Ensure that all stored electronic records are true, complete, authentic, and accessible
- **Media Management:** Protections are in place that will reasonably protect against loss, alteration or destruction of the stored electronic information
- **Data Integrity:** Implement processes, procedures and technologies that will ensure the ability to identify, locate, recall and restore any required data quickly and accurately from individual data elements to entire system platforms.

Without buy-in from senior management, compliance programs are destined to fail or at best fall short of fully meeting all requirements.

The most important part of establishing any control process is to clearly communicate the process, and its purpose, to everyone in the company. Failure to educate the individuals that perform the tasks will severely limit the control process if not condemn it to stop working. All individuals must know not only what must be done but also why it must be done and the consequences of not getting it done. Along with the education process, the control process must be documented. Flow charts showing each stage of a workflow with specific control points simplify the training and auditing.

Applying Information Life Cycle Management Best Practices

Adopting solid process controls can generate several additional benefits. In the early 1990's, the buzzwords were "re-engineering" and "continuous process improvement" both focused on examining the workflow of a business or department and introducing changes that improve that flow. The technique to implement process controls for improved business operations can be applied to information life cycle flow. A company can develop comprehensive recovery plans along with compliant retention strategies by identifying how information flows through the organization and understanding the critical control points and processes that ensure the security, integrity and availability of data.

A well constructed information life cycle control plan has other benefits. By understanding the difference between data storage for recovery purposes and retention requirements, media storage strategies can be altered to provide maximum recoverability and suitable compliance with a minimum number of tapes, saving time and money. In addition to reducing costs and streamlining operations, establishing a strong control oriented information life cycle minimizes the risks and exposures to legal and legislative actions.

All individuals must know not only what must be done but also why it must be done and the consequences of not getting it done.

How Can LXI Help

LXI is dedicated to helping customers effectively build and manage their information infrastructure by providing quality products, customer support, and professional services. The company's storage management software solutions for open systems and the IBM iSeries provide comprehensive backup, recovery, tape protection and management, device control, and on-site / off-site location and vault management.

Working closely with customers over the years, LXI has a solid understanding of the retention and disaster recovery challenges faced in day to day operations. LXI products and services are designed to enable compliance and facilitate control while automating the procedures of not only regular backup processes, but also that of record retention. Essential to providing both retention and recovery capabilities are the abilities to protect against inappropriate or misuse of media across multi-platform environments. LXI technology protects and consolidates active data through its life cycle.

One of the common challenges companies have when required to deliver information is to quickly and easily locate the requested data. LXI products are designed to deliver fast and accurate location by providing index (catalogs) of all data being written to tape and tracking the location of the tapes.

Uniquely designed, LXI vaulting solutions provides the best of breed vault management. Midrange vaulting solutions are typically limited in their flexibility, forcing consumers to adapt their processes and procedures to the software. This inflexibility limits those products' ability to manage the compliance requirements. The LXI vision is significantly different. Allowing multiple location move schedules, LXI vaulting can be configured to automate any scenario and implement thorough compliance control processes.

LXI products and services are designed to enable compliance and facilitate control while automating the procedures of not only regular backup processes, but also that of record retention.

For more than a decade LXI has been supplying products and services to the iSeries and open systems market place. Founded on the principles of strong audit compliance, LXI provides the technologies to meet both your disaster recovery and record retention requirements.

About LXI

LXI Enterprise Storage (LXI) helps businesses manage their enterprise storage needs in heterogeneous environments, simplifying cross platform storage policy administration, integrating disparate platforms and network backup products, and consolidating media information for centralized management. End-to-end data protection solutions help ensure that data is saved, archived and tracked, giving organizations data assurance across the enterprise for recoverability and regulatory compliance.

With LXI, customers gain the benefit of industry-leading storage management software, hardware and services. LXI and its partners bring together the experience, the products and the integration necessary to provide complete data protection for data retention, business continuity and compliance.

To learn more about LXI, visit us at www.lxi.com or call 214.260.9002.



391 E. Las Colinas Blvd
Suite 130-440
Irving, Texas 75039 USA

Phone: 214.260.9002
Fax: 866.898.5753

www.lxi.com