

# Proactive Preservation Management

Findings and Best Practices from 2002 - 2004

Author: Jason Velasco, Vice President of Electronic Evidence Services

# Table of Contents

Increased Corporate Risk.....	3
Identified Common Problems.....	5
Changing Perspectives.....	7
Best Practices.....	8
Evidence Preservation System.....	9
Conclusion.....	10
RenewData Services.....	11

## Increased Corporate Risk

### New realities in the era of Sarbanes-Oxley

- C-level executives are now exposed to more severe penalties
- Managing corporate records more important than ever

### Electronic records growth

- Annual growth rate of all electronic records usage approaching 96%
- Estimated annual growth rate of e-mail storage could be as high as 36%

### Residual data risk

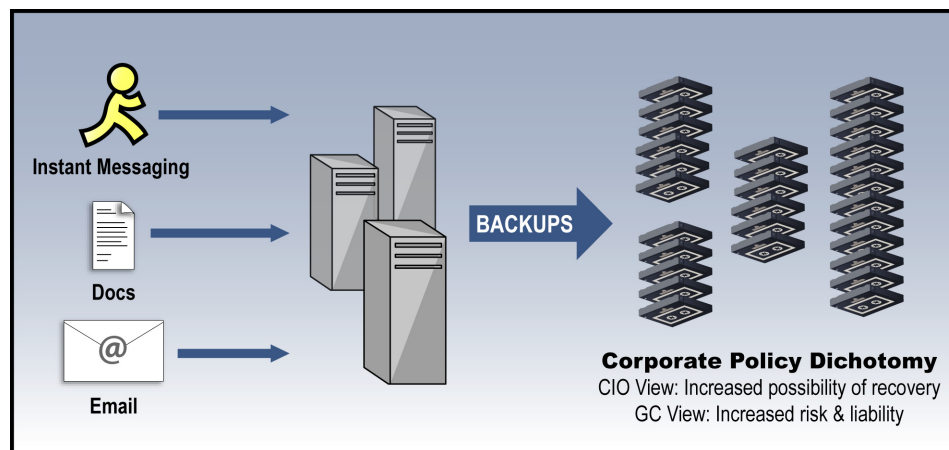
- Corporate IT has been backing up corporate correspondence to tapes for years
- Offsite backup media is discoverable in litigation and therefore may contain information that poses huge and unquantifiable risks and liabilities

### Enterprise User Information (EUI)

- E-mail, User Files and associated metadata.

The changes in the regulatory compliance and civil litigation environment have occurred concurrently with the continuing expansion of electronic records storage. The use of digital information is growing at an annual rate of 96%, while e-mail storage requirements are estimated to have grown by 36% in 2002 and show no signs of slowing. As increasing numbers of both regulatory investigations and civil litigation involve electronic evidence discovery, the need for internal controls of the company's electronic and paper records has become a critical business imperative. *There isn't a large company in America today that knows their complete legal exposure with regard to its e-mails and user files (Enterprise User Information or EUI) when faced with a discovery order or subpoena.*

Corporations have collected legacy email and user files in an uncontrolled manner for years. This buildup has been occurring for the sake of establishing a simple and fool-proof disaster recovery system (diagram below), where tapes used for backups are not always successfully tracked and/or recycled. Organizations and their outside counsel need a new way of managing the full life-cycle of corporate email and user files to decrease *residual data risk* (see side bar).



The recent changes to federal regulations, specifically Securities and Exchange Commission (SEC) and Federal Trade Commission (FTC) regulations, and the implementation of the Sarbanes-Oxley Act have dramatically increased the risk of maintaining the status-quo in responding to subpoenas. Of particular concern is the recent introduction of harsher penalties, including possible incarceration, which board members and C-level executives of public companies now face for infractions.

In the SEC's 2003 Compliance Inspections and Examinations report, the SEC identified its 2004 priorities as continuing "to enhance customer protection and compliance functions" focusing on high priority areas such as "market timing, late trading, sales practices, internal controls/risk management and annuity and mutual fund sales."

## Average number of non-frivolous suits at any one time

- During more than 150 interviews, RenewData found that Fortune 1000 companies are deluged by 50 to 250 non-frivolous suits running concurrently

The increase in investigations has exemplified the new rigor with which the federal government is now enforcing regulations. The SEC has filed an increasing number of enforcement actions relating to financial fraud or reporting violations over the last several years. For example, in fiscal year 2003 the commission filed 199 such actions, up from 103 in fiscal year 2000. Moreover, in the first half of the current fiscal year the Enforcement Division opened approximately 125 new investigations relating to potential financial fraud or reporting violations.

As corporations are being confronted both by government agencies with low tolerance for production delays and liberal civil discovery laws, the General Counsel (“GC”) is facing increasing responsibility to properly manage electronic productions. For every matter, the GC must answer:

- Has relevant data been properly preserved?
- What is the time, difficulty and cost to recover and retrieve relevant data?
- What level of business disruption will there be preserving and recovering data?
- How can irrelevant and privileged data be sorted out prior to legal review?
- How can truly relevant data be identified?
- How can the same preserved data be leveraged across multiple matters?
- How can costs be managed to avoid skyrocketing costs for future requests?

As quoted in a Network World article on August 9, 2003, between 2002 and 2004 RenewData conducted interviews of more than 150 Fortune 1000 corporations and found that on average, the firms deal with an average of 125 non-frivolous suits at any one time. This white paper discusses the common problems identified with reactive responses to subpoenas and discovery requests and best practices to resolve those problems.

# Identified Common Problems

## Identified Common Problems

- Insufficient Planning
- Poor communication between groups
- Lack of trust
- Disruption of IT department initiatives
- IT outsourcing challenges
- Duplication of work for subsequent requests
- Incomplete email retention policies
- Obsolete or incompatible technology
- Poor inventory control and storage
- Difficulty forecasting budgets

## Preservation Anecdote

One interesting anecdote from a major financial corporation was related to preservation. Their corporation was ordered to preserve daily backups for multiple sites effective from the date of the preservation order. As a result, this IT organization was creating hundreds of daily backups, putting a huge strain on the IT organization. This was creating problems locating and buying enough backup tapes to have a two week supply on hand, logistical issues storing the tapes, and the need for increased IT investment in the equipment capable of managing the backup function during their allocated service window.

## Planning

Approximately 70% of the corporations interviewed said they either did not have a litigation preparation strategy or a litigation/investigation response plan. An additional 15% said they were “not fully comfortable” with their existing plans. Of the remaining 15% who had an already implemented litigation preparation strategy or a litigation/investigation response plan, 80% of those companies had been part of a major litigation or government investigation in the past two years.

## Language and Communication Problems

A common frustration by both GC’s and IT executives were around language and communication problems. Corporate legal staffs were frustrated with the inability of the IT organization to communicate in non-technical terms. At the same time, members of the IT organization were frustrated that the legal team had difficulties defining what was really needed.

## Lack of Trust

In general, GC’s are feeling more isolated than they have in the past. Because of public disclosure of lawsuits and items such as Wells Notices, virtually all GC’s noted both they and their staffs were being targeted by an increasing number of vendors. As one GC said, “Every in-house vendor wants to sell us something -- from the copier salesmen to the IT contractors.”

## IT Disruption and Burden

A major complaint voiced by IT executives was the disruption caused by responding to legal business problems. Because their IT organizations are often struggling with tight budgets and lack of bench strength, having to manage locating and preserving potential evidence typically resulted in other initiatives being delayed or cancelled.

## IT Outsourcing

Corporations that outsourced a significant portion of IT sometimes experienced unique problems. Typically these problems were related to gaps in outsourcing contracts that required negotiation or incompatible processes. One GC didn’t learn for over 3 weeks that the reason an IT contract vendor had failed to find the backup tapes that needed to be preserved was because the vendor was waiting for a project code to be added to their time management system in order to bill the work activity. One IT executive was frustrated at a situation where two different vendors were providing backup services at different locations. One vendor did a “great job” following the preservation instructions, where a second vendor failed for weeks to properly catalogue the backup tapes causing additional work locating the right tapes.

## Long Lead Times and Rework

Of those companies that had been part of a major litigation or government investigation in the past two years, the primary problem identified by GC’s relating to lead times was not with the initial production, but with subsequent productions. A common mistake made during federal investigations was the

processing of backup tapes for email and user files for only the initial list of target names. During a two year period, these GC's typically had the backup tapes processed three (3) times in order to respond to subsequent requests.

### **Email Retention Policies**

Of those companies that had been part of a major litigation or government investigation in the past two years and who had an established email retention policy, approximately 65% said their retention policies had not protected them from discovery. The problem they encountered was that their email server backup tape rotation program failed to account for individual user archive files stored on local computers or network drives, resulting in these files being discoverable.

### **Obsolete Technology**

One challenge many of the IT executives identified was backup software and hardware that was more than three years old. The backup tapes from these systems, either internally generated or obtained through a merger or acquisition, was often in a format that was incompatible with the currently deployed backup system.

### **Poor Inventory and Lost & Damaged Media**

Many IT executives were embarrassed when their listed inventory of backup tapes was significantly different than the actual number of tapes. One GC, based on information provided by corporate IT, initially planned on having 700 tapes restored. Because of a combination of an inaccurate inventory and a mistake in a spreadsheet calculation, there actually were double the amounts of tapes -- resulting in increased processing costs and a delivery schedule renegotiation with the federal agency. Also cited by IT executives was a problem with media being lost by their storage vendor or damaged older media.

### **Budget Planning**

In some of the examples cited above, particularly the situation where tapes were being processed multiple times for subsequent requests, those GC's found the process of accurately forecasting a budget difficult to accomplish.

## Changing Perspectives

### Changing Perspectives

- Ignorance no longer a valid defense
- Email retention policies unique compared to paper retention policies
- Sarbanes-Oxley Act compliance requires action
- Burdensome arguments rarely win in court
- Cost shifting strategies inconsistently effective

The interviews identified areas where GC's were changing their perspectives regarding long-standing record management and legal practices. Specifically, the acknowledgement of changes in records management and data retention philosophies showed an increased understanding of the growing responsibility of the GC position.

#### Hear No Evil, See No Evil

Before Sarbanes-Oxley, it was possible for corporate executives to take a "Hear No Evil, See No Evil" approach to electronic records, particularly email. However, now that CEO's and CFO's must attest to the accuracy of financial records, along with increasing board member liability, GC's are seeing the old policy of ignoring email and user files is no longer appropriate.

#### Paper Retention Policies Are Not Good Enough for Email

More GC's are starting to see that paper retention strategies are not robust enough to apply to email and electronic records. Retention policies require that a document be managed, controlled and destroyed as required. It was relatively easy before the wide adoption of email to control and destroy copies of paper documents. With the viral nature of email though, there is no guaranteed way to destroy every copy of an email.

#### Sarbanes-Oxley Act Compliance

The Sarbanes-Oxley Act of 2002 has introduced new dimensions and gray areas to business records handling requirements. Sarbanes-Oxley has far reaching implications that impact the management of all company records relating to externally reported financial results. More importantly, the personal penalties of multimillion dollar fines and long term imprisonment apply to all people responsible for ensuring the integrity, preservation, availability and accessibility of all company records. Legal and IT departments are particularly at risk because of their direct responsibility for the protection of record integrity. The key challenge is that the Sarbanes-Oxley Act is vague and ambiguous regarding financial related records management.

#### Burdensome Arguments & Cost Shifting Strategies

Typically promoted by their outside counsel, GC's have learned that the necessary tactics of pursuing burdensome and cost shifting arguments to have very low success rates. In federal investigations, GC's have found the burdensome argument to fall on deaf ears. In the post-Enron era, federal agencies such as the SEC and FTC have obtained a de facto mandate through public opinion to pursue potential wrong-doing. The cost shifting strategy of the early days of electronic evidence rarely came to fruition. Cost shifting became the exception, not the norm.

# Best Practices

## Identified Best Practices

- Proactively prepare for future litigation
- Know who has access to all critical electronic data and where those systems and backup media are located
- Align Legal and IT
- Disaster recovery strategies must no longer be de facto retention programs
- Create a records retention program that is enforceable
- Eliminate rework by implementing an evidence preservation system.

In order to meet these business requirements, the following best practices were identified by the executives interviewed:

### Initiate a Litigation Preparedness Program

A company should implement a schedule where a full litigation preparedness analysis and implementation is conducted every five years. A full analysis using a third party is necessary every five years to ensure a complete understanding of legal and regulatory changes, trends and updated best practices. Between the five year cycle, companies should implement an annual review and scorecard of their efforts.

### Create & Maintain a Data Topography

A company should have their IT organization create and maintain a data topography showing the location of all active and archived data that may be relevant for future investigations and litigation. This topography should include a list of all email servers, compliance systems, records management systems, financial systems, executive information systems, and the computers of high profile employees.

### Establish a Formal Legal & IT Alignment Counsel

A company should implement a formal legal and IT alignment counsel that meets quarterly. A critical element is to include representations not only from the centralized IT organization, but also from any decentralized IT function as required. It is also suggested that representation be included from the Audit department. The charter of this counsel is to ensure that changes in regulatory and legal requirements that impact IT are properly communicated and managed.

### Disconnect Retention from Disaster Recovery

A company should separate the requirements of electronic records management and retention from IT backup and disaster recovery responsibilities. Backup tapes should not be used for records retention. Data on backup tapes is not directly searchable, not easily accessible, expensive to restore in large volumes and impossible for most systems to delete specific records.

### Create an Enforceable Records Retention Programs

A company should be able to apply targeted retention policies to all of its electronic and paper records, reducing its long-term liability risk as well as minimizing costs associated with storage. Key to this program is the ability to identify records relevant to existing and pending investigations and litigation and ensure those records are not deleted as part of a normal destruction cycle.

### Implement an Evidence Preservation System

Companies must be able to know the legal, non-compliance and business risk embodied in email and user files, both current and historical, before litigation or investigations commence. The general counsel's office should have the ability to immediately search the entire company's e-mail, attachments and user files that are stored in a forensically sound manner in order to assess risk exposure from investigations or litigation.

# Evidence Preservation System

## Benefits of Having an Evidence Preservation System

- Knowing “your hand” early or before litigation
- Eliminate risks of evidence spoliation
- Reduce time and costs spent on subsequent evidence productions

## Evidence Preservation System Best Practices

- Define your methodology prior to selecting technology
- You can start small
- Store native files with chain-of-custody proof of the source

The best practice that seems to hold the most practical promise to resolve the identified common problems is that of an Evidence Preservation System. Under this model, the company would migrate all key records from inaccessible backup tapes to a central, searchable repository while maintaining chain of custody “links” to the original media.

An evidence preservation system can help protect the company from any risk of spoliation. This system also eliminates the need to reprocess the same backup tapes multiple times for new matters or subsequent requests.

Using a proactive evidence preservation approach, when a GC, the head of litigation or an independent third party has the tools to assess the company’s legal exposure early in the litigation process or even before litigation begins, three scenarios are possible:

1. **A “smoking gun” e-mail or user file is found.** The company is guilty – bad news. The good news is that the position is known early. The strategy is typically to settle as soon as possible. The company saves on outside legal costs, executive time and very likely, on settlement costs.
2. **A “white knight” e-mail or user file is found that completely exonerates the corporation.** The evidence can be presented to the other side (perhaps a plaintiff attorney on 100% contingency), resulting in termination of the case. The savings are obvious.
3. **No information is found that proves/disproves innocence.** The company can at least know that it can execute a legal strategy without fear of any negative repercussions resulting from future electronic evidence productions.

The best practices identified for an electronic preservation system are:

### Define the Methodology

The methodology used for electronic evidence preservation must be defined prior to any technology selection. The methodology must be tested against standard scientific principles such as “verifiable and repeatable.” The methodology must also define how chain-of-custody will be managed.

### Start Small with Existing Matters

If the focus of the project is truly electronic evidence preservation and not part of a larger initiative such as compliance and retention, then the company should start the project using evidence from existing matters. As each new matter is initiated, the preservation system can be checked for responsive data. If the matter requires additional electronic evidence, then that data can be added to the preservation system, resulting in a more natural, organic growth that is funded from the budget of each matter.

### Electronic Evidence = Native Files

An effective evidence preservation system needs to focus on managing the original native files. A system that focuses on TIFF renditions of documents may not have all of the meta data or electronic chain-of-custody information. By maintaining native files in the preservation system, companies have more flexible output options.

## Our Conclusion



During the past two years as RenewData conducted these interviews with over 150 legal and IT executives, we gained a significant amount of knowledge about the problems, changing responsibilities and best practices relating to litigation and investigation management in the U.S. corporate environment. This research has allowed our company to define our focus and strategy to be responsive to our client's requirements. We hope you will benefit from some of the information we share in this white paper.

What we found interesting is how electronic discovery has failed in many regards compared to the promise of lower costs. Five years ago, electronic evidence vendors were touting how email and user files can be extracted for .10 to .25 per page as opposed to .75 to 2.00 per page for the scanning and coding of paper documents. Unfortunately, the cost of electronic productions and subsequent reviews skyrocketed due to the pure volume of data. This has led to interesting cost reduction strategies, including keyword negotiation, native file culling and native file review.

However, these are still tactical, reactive strategies. We believe the best promise for companies to reduce production costs are proactive strategies, including litigation preparedness initiatives and specifically the re-use of previously restored email and native files using a native file preservation system.

# RenewData Services



*RenewData's vision is to migrate companies from reactive to proactive data management for litigation and investigations.*

RenewData's unique blend of proprietary technology, as well as legal and technical expertise allows us to provide a complete array of electronic evidence and legal consulting solutions geared toward the needs of all parties including inside counsel, outside counsel and corporate IT departments.

## **Our services include:**

- Litigation response planning
- Evidence collection and preservation
- Forensic and investigative services
- Electronic data extraction
- Litigation production services
- Expert witness consulting
- **Proactive and reactive evidence preservation and archiving**

## **About the Author**

Jason Velasco is the Vice President of Electronic Evidence Services at RenewData. Mr. Velasco has over nine years of experience in electronic evidence and forensic investigations. Mr. Velasco has conducted more than 250 computer forensic examinations for civil litigators and companies; and has emerged as a leading forensic computer specialist providing expert witness services related to electronic evidence topics and data preservation. Mr. Velasco is currently serving on the Litigation Support Task Force for the Standards Development Committee and served as a panelist and speaker at the 2005 US Law Network Client Conference. Mr. Velasco has also conducted over 100 CLE courses on topics such as Electronic Discovery, Document Retention and the Technical aspects of Electronic Evidence. In addition Mr. Velasco often consults for Fortune 500 companies and law firms by designing procedures and protocols related to the technical and legal aspects of electronic evidence productions. Mr. Velasco received a bachelor's degree from Indiana University.

<sup>1</sup> Osterman Research Messaging Archive survey of 146 IT managers



9500 Arboretum Blvd Suite L2-120 | Austin, TX 78759 | [www.renewdata.com](http://www.renewdata.com)  
512.276.5500 Office | 1.888.811.3789 Toll Free | 512.276.5555 Fax

Copyright © 2005 Renew Data Corp. All rights reserved. RenewData and the sphere logo are registered trademarks and ActiveVault is a trademark of Renew Data Corp. All other company and product names may be trademarks of their respective owners.