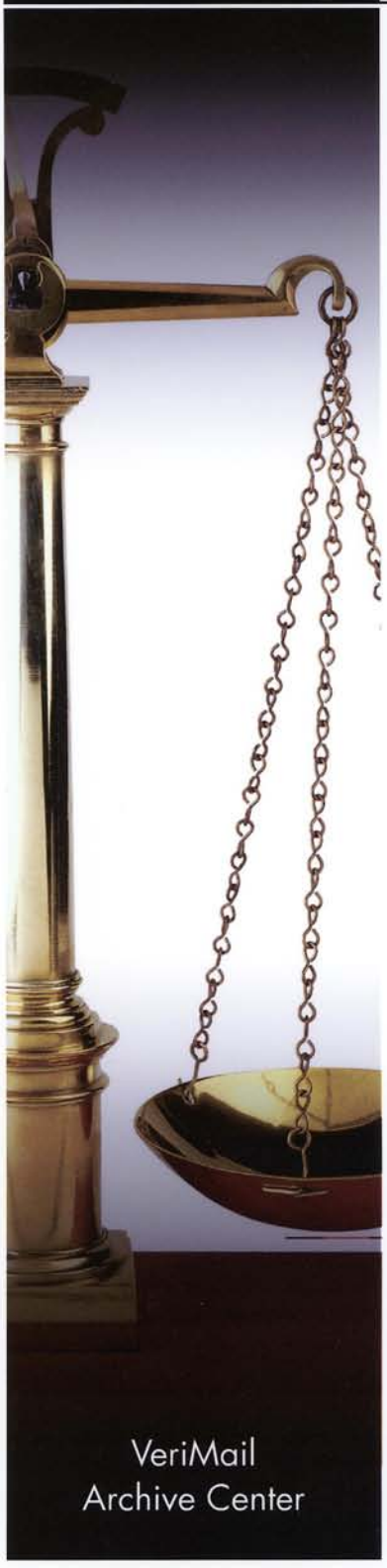
Litigation: An Ever-Present Threat

IWITNESS



"Unmanaged electronic data is the biggest unfunded liability that companies face today."

John Jessen
CIO Magazine, June 1999

Every major corporation faces litigation that can damage its reputation, disrupt its operations, and deplete its financial resources. The Microsoft antitrust case, in which 70% of the government's evidence came from email, has made it common knowledge that email is a treasure trove of potentially damaging information.

According to a PricewaterhouseCoopers/American Bar Association survey, email is now the form of digital information most requested by opposing counsel in corporate litigation. Nevertheless, an astounding 83% of the survey respondents also said that their clients or employers lacked an established protocol for responding to opposing counsel's requests for digital information.

Most civil litigation is settled out of court, resolved on the basis of review and production of documents –called "discovery" in the legal vernacular. The largest direct costs of this pre-trial process are fees paid to counsel for the review of documents—a task that occurs repeatedly as the litigants move toward trial—and associated out-of-pocket expenses. The hidden cost, often disregarded by the courts and exploited by opposing counsel, is business disruption.

Be Prepared

Typically, the party who controls the pace of discovery wins the case. It pays to be prepared. The ability to quickly determine the strengths and weaknesses of the case is critical. Whether there's a "smoking gun" lurking in email messages opposing counsel might demand to see—or strong support for the defense—it's better to know sooner rather than later.

Courts consistently reject the plea that digital information is too costly to recover and produce for discovery. CIBA-Geigy, the predecessor of pharmaceuticals manufacturer Novartis, was required to produce at its own expense related items from 40 million pages of email.

Moreover, a lawyer who assures the court that all relevant email messages have been produced in response to a discovery order had better be right. The price of error can go far beyond damage to credibility. The court may allow an "adverse inference"—the presumption that the respondent was deliberately withholding evidence. In extreme cases, executives may face jail time for improperly managing digital records.

A corporation without a legally defensible system for managing email records may find itself in this awkward situation. While opposing counsel can introduce as evidence email that creates a negative inference, the defendant may be unable to introduce its own email on its behalf.

The solution comprises four major components:

- Iwitness VeriMail" automatically captures email messages.
- Iwitness Archive Center indexes messages, applies retention and security settings, and writes the messages to secure storage. It also initiates and maintains a Digital Audit Trail for each record.
- Iwitness Archive Navigator allows in-house and outside counsel to retrieve and review messages from online and off-line storage systems—any time from anywhere—and to forward them for further review or action.
- Iwitness System Manager allows system administrators to configure and manage the application.

Iwitness VeriMail System

Automatically and verifiably captures email messages of employees based on the rules set by the organization.

Iwitness Archive Navigator

- Provides an interface for in-house and outside counsel via the Internet.
- Allows users to search corporate records for litigation needs.
- Enables hold orders to be placed on specific records.
- Provides searchable field for annotation of records.
- Allows users to view the historical audit trail of the record.

Iwitness Archive Center

- Indexes entire messages upon capture which enables key-word search and retrieval of archived messages.
- Initiates a digital audit trail upon capture, which generates time stamping and history throughout the life of the record.
- Provides integrity checking throughout the life of the record.
- Applies retention schedules to each specific record based on type.
- Applies appropriate security to maintain authorized accessibility.

Iwitness System Manager

- Provides a complete, simple-to-use interface for system administration.
- Enables scheduling of VeriMail capture processes.
- Allows management of users and groups.
- Provides for importation of users from LDAP.
- Enables creation of site-wide and user-specific rules for archiving.
- Allows configuration of hierarchical storage and lexicon management.

Why the Iwitness Solution?

The Iwitness system can be configured to capture messages based on site- or user-specific rules. A comprehensive automatic capture setting is available to ensure compliance with court instructions to preserve email during the course of a dispute.

An evidence-quality Digital Audit Trail shows the complete history of the records and maintains them in an auditable, accessible form. This provides integrity checking of the records throughout their retention periods. The Iwitness system provides a complete picture of who knew what and when: it automatically captures the entire message, including attachments, and the blind carbon-copy (BCC) field; it also automatically expands the distribution list in real time.

Disposing of messages that are no longer required for business or legal purposes is as important as keeping what's needed. Organizations can choose disposition processes that fit their security needs.

Laws, business practices, and technologies evolve. The Iwitness solution is designed to accommodate changes and to handle enterprise-scale volumes of digital information, providing a cost-effective, long-term solution.

More information:

Iwitness is available via phone, fax, or email.

Email: info@iwitness.com
www.iwitness.com

Iwitness, Inc.
2995 Wilderness Place,
Suite 2N
Boulder CO 80301
(303) 545-9000, x 143
(303) 545-9155