

# Evidence Management Solutions for Mitigating E-Records Risks

Bringing together IT, legal, RIM, and compliance officers through integrated information risk management (IIRM) is a smart move that can help a company mitigate regulatory and legal risks.

**Rob Peglar**

Reports about various organizations' struggles to comply with recordkeeping regulations are regularly in the news, reinforcing the need for organizations of all sizes and in all types of industries to be more vigilant than ever about their information management practices. Managing e-mail, which is perhaps the least understood and managed set of records in any organization – and is potentially the “smoking gun” used by plaintiffs in litigation against an organization – is particularly problematic for many organizations.

The optimal way to mitigate information technology (IT), legal, records and information management (RIM), and compliance risks associated with managing information is to take an integrated approach, which brings together a coalition of stakeholders in those areas to implement a comprehensive plan, as opposed to piecemeal “point” solutions. This approach is

known as integrated information risk management (IIRM).

An organization must determine such things as:

- Does it have a sustainable records (including e-mail) retention policy?
- Can it efficiently and effectively execute a hold order on electronic information in the event of a lawsuit?
- Are its RIM, IT, legal, and compliance practices integrated into a

comprehensive set of processes and implementations?

If not, they may be faced with above-average corporate risk and cost of litigation. According to the 2005 Fulbright & Jaworski Litigation Trends Survey of corporate counsel, U.S. corporations with \$1.5 billion in annual gross revenue average more than \$8 million in corporate litigation costs and more than 140 cases pending at any given time.

## U.S. Regulatory Requirements

All organizations must be careful to ensure compliance with federal legislation regulating the dissemination of nonpublic information. Three primary U.S. laws – the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and the Sarbanes-Oxley (SOX) Act of 2002 – affect virtually every aspect of an organization's information-sharing practices. While these acts are similar in their intent, they differ in the types of records they target.

### At the Core

This article

- ▶ Explains how using integrated information risk management (IIRM) can help mitigate legal and other risks
- ▶ Examines management solutions for e-mail and other electronically stored information
- ▶ Discusses the elements of a proactive evidence management solution

For example, HIPAA and GLBA are similar in that each mandates how particular healthcare and financial consumer records must be protected by organizations in order to ensure privacy. However, SOX is concerned with the integrity of financial reporting records. It mandates that senior executives must vouch for the financial data reported by

burden on IT's ability to ingest, process, and store the text and attachments.

One challenge is that e-mail is being used by many people as a *de facto* file repository – storing attachments, files, documents, and other electronic media within their personal e-mail space – which e-mail systems are not designed to be. This adds exponentially to the stor-

tems *must* re-examine them, ensuring that they have implemented best practices around this important aspect of information risk. Otherwise, they may find themselves quickly unable to comply or unable to respond to a litigation incident or internal investigation.

Search, index, categorization, access, permissions, chain of custody, metada-

Given the mandates of regulatory and discovery requirements, there is a need to manage ESI as potential evidence for its designated lifetime. One solution ... is to implement a proactive evidence management system that incorporates automated, policy-based retention of ESI.

their organizations.

But all three regulations require that certain material be protected from exposure to unauthorized parties, either to avoid a violation of privacy or to ensure that data has not been manipulated without authorization and authentication.

### E-mail in an IIRM Approach

An organizational practice that spawns multiple areas of risk – legal, IT, RIM, and compliance – is the use of e-mail. And – industry analysts agree – e-mail use is expected to grow significantly in the near term. According to a March 2007 study, “Worldwide Email Usage 2007-2011 Forecast: Resurgence of Spam Takes Its Toll” from analyst firm IDC, “The size of business email volumes sent annually worldwide in 2007 will approach 5 exabytes, nearly doubling the amount over the past two years.” [Editor's note: 1 exabyte = 1 billion gigabytes.]

Furthermore, IDC predicts in the same study, nearly 97 billion e-mails will be sent daily this year – and more than 40 billion of those messages will be spam. For organizations large and small, this explosion in e-mail creates a significant

age space required and is leading many organizations to curb usage or restrict e-mail space via quotas or other mechanisms.

Not only does IT have the challenge of allocating sufficient storage, there is the logical and managerial challenge of determining which e-mails are business-related and should even be retained. As society is becoming increasingly comfortable with e-mail as a communication medium, there is no doubt that a substantial portion of e-mails received by any given organization is not business-related.

Another challenge is ensuring that business-related e-mail is properly categorized, retained, and disposed of according to the organization's retention policy and to comply with the new Federal Rules of Civil Procedure established in December 2006. For public companies of 75 employees or more, there is the additional regulatory burden of retaining certain business-related e-mail for periods as mandated by Sarbanes-Oxley.

Ironically, many organizations do not have any e-mail management system whatsoever, which means, in other words, complete e-mail chaos. Those who do have e-mail management sys-

ta, and many other aspects of e-mail management are now being placed front and center in every organization, mandating a coalition of IT, compliance officers, risk managers, and corporate counsel be formed to determine how to meet these challenges.

### IIRM E-mail Practices

For mid-sized organizations under SOX, the requirement is clear: organizations must save every record that informs their audit processes, e-mails included, for seven years. This calls for an IT environment that implements a proactive evidence management system, one that handles all e-mail as potential evidence for a future SOX audit.

An organization cannot afford – in the operational sense – to hold all its old e-mail on traditional tape cartridges held offsite because of the requirement for rapid discovery and search. Tape is ill-suited in this regard. According to IDC, the average litigation discovery of electronically stored information (ESI) is 72 hours – and shrinking. Many organizations' offsite tape repositories cannot meet that challenge.

In addition, organizations must be careful to select IT systems that use data

availability best practices, such as clustered storage and storage area networking, as well as virtualization to make the movement of e-mail between tiers transparent to the user. Remember, records must first be accessible and available in order to be searched and indexed, especially in a time-critical discovery. The keys to complying with regulations are to store records wisely and use common sense.

**Proactive Evidence Management Solutions**

Given the mandates of regulatory and discovery requirements, there is a need to manage ESI as potential evidence for its designated lifetime. One solution for e-mail retention and other regulatory requirements is to implement a proactive evidence management system that incorporates automated, policy-based retention of ESI.

For e-mail, most vendors have focused on content filtering and encryption technology as a contributor to proactive evidence management. While both of these technologies are needed for proactive evidence management, relying only on these tools will not provide a complete solution. A complete solution must combine multiple records security components into a single, comprehensive package that will:

**Proactive Evidence Management System Capabilities**

**To be effective, a proactive evidence management solution should offer capabilities for all aspects of the organization’s compliance needs:**

**Messages**

The system should protect e-mail messages from snooping and unauthorized alteration by using automated, policy-driven encryption technologies to ensure privacy for customer data and integrity of financial data when in transit. Technology should be able to dynamically select the most appropriate encryption level based on the recipient’s capabilities, including secure delivery to end users with completely unknown encryption capabilities, as is often the case in using e-mail to communicate with clients in healthcare and financial services.

**Users**

The system should protect users by monitoring e-mail for specific words and phrases and notifying the compliance management team to take corrective action. End users who send noncompliant information via e-mail through unprotected gateways face the very real threat of job termination and even prosecution, should their messages end up in the wrong hands. Regardless of whether the user’s intention is malicious or a simple mistake, the solution must ensure that a control environment is in place to proactively monitor for compliance.

**Systems Intrusion**

The system should contain e-mail-specific firewalls and intrusion-prevention systems. An effective solution must be able to detect and block hacker attacks directed at the appliance itself, as well as at the mail servers and other systems sitting “behind” it. Without this level of protection, vouching for the integrity of information sent via e-mail is impossible.

**Monitoring & Reporting**

The system should communicate compliance status and report suspected violations and give administrators easy access to data so they can:

- Analyze and improve the organization’s proactive evidence management
- Automatically deliver decision-making information to compliance officers in a timely manner
- Easily generate instant reports for executives

**Configuration Options**

The system should be readily customizable to meet the needs of any organization. Compliance officers and senders alike should be given multiple options designed to ensure that all outgoing mail is handled according to the organization’s specific policies.

- Accurately detect regulated material
- Dynamically act to prevent compliance violations in real time
- Protect not only messages but also systems and users
- Verify and demonstrate proactive evidence management through reporting and integrity checks

In addition, the solution should minimize the administrative burden associated with deploying and administering proactive evidence management systems without sacrificing the accurate, effective detection and control of regulated content. A seamless integration of corporate policy and e-mail security, along with dedicated reporting and auditing tools for compliance officers, will result in a comprehensive solution that protects every message, user, and system within an organization.

As e-mail has become the most widely used communication tool in nearly all organizations, special care must be taken to ensure that all messages sent or received are within the realm of legally appropriate interaction.

Content scanning technologies are designed to identify protected information. Effective proactive evidence management solutions should contain regulation-specific, predefined dictionaries (also known as lexicons) for HIPAA, GLBA, and SOX. These dictionaries should be capable of being easily supplemented with additional terms supplied by compliance officers or e-mail administrators. Items that are normally expressed in a predetermined format, such as Social Security, credit card, and phone numbers, should be automatically flagged for review by an organization's compliance officer. Furthermore, custom scanning and analysis rules for detecting information in a format specific to an organization, such as patient identification data and account numbers, should be easy for administrators or compliance officers to manage.

The text contained within an e-mail message is just one aspect of the communication that must be thoroughly scanned. Attached files present a significantly greater additional risk, as they can contain libraries of information that must also be handled in accordance with regulatory guidelines. To neutralize the threat of file attachments, a proactive evidence management solution must perform binary checking of attached files, verifying the actual file type based on the file's encoding, not just its extension. Archives such as .zip files must also be scanned, with the proactive evidence management solution evaluating everything contained in the archive.

A proactive evidence management solution provides defense for multiple levels of an organization's communication network, from individual messages to the users who send and receive them, to the very systems that transfer and store critical information. (See sidebar: "Proactive Evidence Management System Capabilities.")

### Compliance Officers Features

At the heart of any good proactive evidence management solution is its ability to provide compliance officers with multiple options for handling noncompliant messages. Notifications of each noncompliant message, as well

as a real-time list of messages, should be considered mandatory for any effective solution. Allowing compliance officers instant access to this information gives them the opportunity to further analyze messages suspected of containing controlled materials.

In addition to receiving real-time alerts of potential compliance violations, compliance officers should have the option of accessing, sequestering, and producing an archive of all messages that have been sent to properly execute a hold order and respond to a discovery motion for electronic information.

The potential impact of litigation and federal regulations like HIPAA, GLBA, and SOX affect communications within nearly every organization. To meet the risk-reduction needs of corporations, universities, government agencies, and other entities that understand the consequences of noncompliance, proactive evidence management solutions must contain multiple, best-of-breed, policy-enforcement capabilities, giving compliance officers and executives the peace of mind that comes with staying on the right side of the law. The implementation of such systems is the end result of bringing together the IIRM team of IT, legal, RIM, and compliance officers/staffers to develop a comprehensive methodology for mitigating risks. ■

**Rob Peglar** is Vice President of Technology for Xiotech Corporation. A 30-year industry veteran and published author, he has global responsibility for shaping strategic vision, emerging technologies, defining future offering portfolios, marketing direction, planning, execution, technology futures, and industry/customer liaison. He is co-chair of the Storage Networking Industry Association (SNIA) Tutorials and co-author of the SNIA Virtualization Tutorial. He may be contacted at robert\_peglar@xiotech.com.

### References

- Fulbright & Jaworski, LLP. "Second Annual Litigation Trends Survey Findings." October 2005.
- IDC. "Worldwide Email Usage 2007-2011 Forecast: Resurgence of Spam Takes Its Toll." March 2007.