
WHY ARCHIVE?

It's a matter of Reputation, Integrity, and Control.

The email burden should no longer be thought of as solely a back office or IT matter. It should involve proactive decision-making on the part of senior management to choose a high quality storage and backup solution to efficiently retain, protect, manage, and ensure authenticity of email records, and to implement safeguards and internal supervisory controls against inadequate email management practices. Selecting an email archiving solution should be considered an investment in your organization's future, both in terms of risk reduction and overall firm image.

COMPLIANCE

1. Litigation

Expensive and damaging lawsuits, like the recent Enron-related settlements, demonstrate the importance of having an archiving and monitoring system that ensures information security, availability, and integrity.

Liability - Email and IM correspondence are inherently "public" forms of communication. Your organization is liable for all email distributed via your organization's email system (including personal email and IM). Companies must establish supervisory controls to enforce email usage policies in order to reduce legal risks and improve employee awareness of the related legal exposure. Accordingly, an archiving system should have unified online search, retrieval, monitoring, and audit tools for policy enforcement. Information preserved in the Archive is the property of the company and can be used to protect itself and proactively address discovery issues by taking control of and planning for disclosure.

Preserving Evidence – Email, considered by many lawyers to be the "digital smoking gun" of litigation and often referred to as "evidence mail," can be legally admissible as evidence in a lawsuit and is frequently the principal focus of electronic discovery. Businesses have an affirmative legal obligation to preserve all evidence relating to a dispute as soon as the potential for litigation arises. Problems and consequences associated with inadequate record keeping include:

- Burden of court-ordered sanctions and penalties for failing to preserve emails relevant to anticipated or ongoing litigation. In fact, for pending litigation, it is a criminal act to destruct evidence;
- Possibility that, in order to respond to e-discovery requests, enormous undue burden and expense may be incurred to restore archived data and review vast volumes of electronic data when an unmanaged email system must respond to production requests. This may also result in inadvertent disclosure of privileged or proprietary materials;
- Imposition of discovery sanctions under the Rules of Civil Procedure, including fines, preclusion of testimony, adverse inference instruction to the jury, or even entry of judgment against the party responsible for the improper document destruction or alteration; and
- Damage to reputation as a consequence of non-compliance or poor record management outweighing penalties imposed.

2. Email Archiving Industry Practice Standards

Retention of Email – Retention requirements ensure that records are available for review by regulators and auditors. The requirements apply to companies' business correspondence with the public, tax and employment records, and privacy rights of customer information. Archiving is based on your organization's policies, but litigation consequences often warrant email being archived for up to seven years and beyond. Companies will have to keep the underlying records for an extended period of time and retain them in both auditable and accessible forms that will allow authorities to accurately recreate the company's risk projections.

Rapid Search & Retrieval – Increasing discovery and disclosure requirements and freedom of access, privacy, and litigation matters require a timely and effective response to information and discovery requests. To effectively respond, a fully accessible archiving system providing rapid search and retrieval via full text indexing of all email and attachments is required.

Audit Trail – Archiving provides secure controls to ensure data is processed fairly and lawfully by logging an audit trail that tracks every action against every archived email (e.g. when email is stored, viewed, retrieved, deleted, forwarded), or when any changes are made to the archive system (e.g. retention policies or user access rights). The audit trail cannot be circumvented due to the Digital ID, dual secure encryption, and real-time indexing. Therefore, the audit trail actually protects the company, its users, and trusted staff with authorized access to view personal or confidential email such as systems administrators, compliance personnel, privacy officers, and auditors by eliminating concerns related to abuse of access privileges.

Monitoring - Real time company-wide monitoring capabilities of all email captured by the archive enables the instant detection of inappropriate or misleading email content that violates internal policies or legislation.

3. Legislation

An appropriately designed and implemented email archiving system can dramatically simplify compliance. A variety of federal, provincial, and foreign regulations impose record keeping and monitoring requirements on companies in connection with electronic messages:

Privacy - There are enormous privacy implications for record management disciplines with respect to protection, retention and destruction of customer records and files. To ensure that litigation claims or customer complaints are adequately defended, companies should be very careful about how stored email containing personal customer information protected, as well as how it is accessed and used by its staff with administrative rights.

Various States' legislation and the federal Canadian *Personal Information Protection and Electronic Documents Act* (PIPEDA) provide a right of privacy with respect to customers' and employees' personal information that is collected, used, or disclosed by an organization in the private sector.

Extra-jurisdictional requirements – Companies operating internationally must meet international standards as they are no longer beyond reach of the *US Sarbanes-Oxley Act (SOX)* and/or other foreign mandates, as well as extra-jurisdictional terms in countries' legislation.

SOX and *Keeping the Promise for a Strong Economy Act (Budget Measures), 2002*, in Ontario, Canada, are intended to improve corporate disclosure and financial reporting and increase the accountability of accounting firms for their audits of public companies. While *SOX* is US legislation, it also has an impact on organizations doing business with US companies. In addition to the requirement that an organization must maintain sufficiently detailed audit information for at least seven years, *SOX* also established a new criminal statute relating to the destruction, alteration, or falsification of records in contemplation of, or in a federal investigation, action, or bankruptcy.

SECURITY AND PROTECTION

As a result of increasing interconnectivity, information is now exposed to a growing number and wider variety of threats and vulnerabilities. Information security is essential to maintaining competitive edge, cash flow, profitability, legal compliance, and commercial image. Data must be secured to prevent unauthorized access. Archiving guards against disclosure of non-public customer information, company trade secrets, confidential documents, or intellectual property. The archiving process has secured end-to-end dual encryption using highest standards (NSA level encryption, and a simultaneous secondary Digital ID via an RSA bit key).

Backup Tapes – Conventional tape backups are not a substitute for email archiving. Backup is not designed for compliance reviews or legal discovery. Huge amounts of expense and time are consumed in recovery of email from a tape backup, and often the messages are never found. Long term archive storage ensures there is no loss of corporate intellectual property. Archiving also adds value through collaboration and consolidation of disparate historical and current email in a unified online storage system while reducing storage and backup time.

Email Lifecycle Management - Effective email management solutions must support the complete email lifecycle, including creation, retention, auditing, management retrieval, and timely deletion of email based on internal record policies. If not properly managed, the sheer volume of corporate email generated daily can dramatically impede an organization's growth and even threaten its ongoing viability.

Business Continuity & Disaster Recovery – Geographically isolated offsite backup allows the archive to act as a permanent secondary mail system to send and receive email if the primary mail system is unavailable.



Exchange Archiving - The archiving system seamlessly integrates with hosted Exchange, eliminating concerns over mailbox size limitations and resulting in improved email system performance through operational efficiencies. Archiving also reduces the capital and operation expenditure associated with storage management. Implementation is simple and fast, without need for complex infrastructure, extra hardware, software, or programming.

RISK MANAGEMENT

Whether communicating with clients, business partners, or employees, email has become a principal business communication tool that must be managed as an integral part of an organization's risk management solution. Mismanaging critical customer email information puts your professional reputation in jeopardy and undermines stakeholder confidence. Email archiving technology will play a proactive role in building transparency and ensuring that email is addressed as part of an overall records management program.

Business Record - Email is deemed by the courts and a myriad of legislation to be a "business record." As a business record, email should be preserved in a secure but accessible long-term storage system according to an organization's policies, similar to paper records. Email retention and management are essential to protecting an organization's intellectual capital. As well, by preserving a permanent copy of every incoming, internal and outgoing email and attachment, archiving provides you with an indisputable chronological record to help safeguard your business operations.

Proof of Integrity and Authenticity – In order to preserve authenticity and irrefutability of email in the event of litigation, archiving removes any opportunity for intentional or inadvertent modification or deletion of email with real time capture. WORM back-ups with write-verification, end-to-end security, and audit capabilities ensure message integrity and authenticity, providing quality evidentiary records admissible in court.

ABOUT GLOBAL RELAY

Global Relay is an innovative technology services company, providing managed enterprise-class email and IM archiving and monitoring services worldwide. As the developer and operator of its technology and Data Centres, Global Relay has provided hosted online message archiving solutions for six years without a single incident of data loss.

Global Relay ensures that messages are properly preserved, centrally-managed, and protected on a daily basis, as well as in the event of a disruption or disaster. Global Relay specializes in messaging compliance solutions for public companies, financial, and healthcare industries, and has a significant customer base and reseller network throughout the US, Canada, and Europe.

www.globalrelay.com