

Cryoserver

Email Archiving – Department Benefits

August 2010





Email Archiving – Department benefits

Email Archiving - Taking care of your business

Few would deny that email is the lifeblood of any organisation with as much of 90% of business communication transacted over email, email only has to go down for a few minutes before the phone starts ringing in the IT department. So it is surprising that so many are satisfied with just a corporate email policy document and backing up the mail server as a way of long management of email records. Email archiving should not just be considered “another type of back up” to be turned to by the IT department in the event of a problem, but as a valuable tool for daily use throughout an organisation improving both knowledge management and day to day business efficiency.

HR Department

- **Formal investigation:** HR departments can quickly carry out formal investigations without requiring IT departments to restore back-up tapes, which also means false allegations can be immediately discounted.
- **Ensure greater employee privacy:** Prevents organisation-wide abuse by generating a fully encrypted audit trail every time an authorised search is conducted.
- **Comply with the mandatory retention periods:** for employee records that stretch for many years after an employee may have left the organisation.
- **Settle potential employment tribunal cases before going to court:** By virtue of having a tamper-proof record of email correspondence, the full context of any accusations can be understood and assessed upfront.
- **Monitoring of possible workplace harassment:** Facilitates monitoring for example for, racism, sexism, obscenity, porn, defamation, etc.) with expense of restoring back-up tapes.

IT Department

- **No more email restorations:** Email restorations from back-up tapes take a disproportionate amount of time, are expensive to carry out, and often do not produce the evidence required. You can also import all legacy PSTs and backup tapes
- **Legal Compliance:** It is a breach of Data Protection legislation for IT departments to search through email back-up tapes that may contain personal data and 'sensitive personal data' as defined by the Act. Tapes should only be used for disaster recovery purposes, not for any other purpose.
- **Centralised location for Personal Data:** Users will use Cryoserver to find older email instead of hoarding them on desktops because of mail quotas. It is a breach of Data Protection legislation and security directives such as BS7799 to store sensitive data on PST files dotted around the organisation.
- **Exemption from criminal penalties:** IT personnel have been prosecuted for carrying out orders from management to destroy electronic evidence. Data on Cryoservers in Data Centres cannot be destroyed or altered, thus removing IT personnel from deciding whether to carry out what may be a criminal act.
- **Eliminate restorations of individual email for users:** users access their own email records, and restore the emails they need back to their inbox .
- **Save valuable mail server storage space:** through single instance storage and IT mail server administrators can delete older mail on the servers much earlier.
- **Real-time Replication (RTR):** RTR built in at the application level means messages can be sent to two or more Archives at the same time to provide full mirroring. This removes the danger of depending on a daily back-up which will only be able to restore data stored up to the point that the back-up was made.



Compliance Officer

With : 150+ different regulations and legislation covering records retention Email archiving aids compliance with existing and current regulatory, legal and operational mandates in global jurisdictions through:

- **Capture and storage of email:** That meets both retention AND privacy legislative requirements.
- **Search email records:** In order to comply with for example, SEC regulations Data Protection Act etc.
- **Ensures a complete record of all email correspondence:** By removing the ability to delete or alter email.
- **Set a retention period:** (suggested minimum seven years) to provide assurance that you will be able to produce ANY email records sent or received during this period.
- **Comply with short statutory discovery times:** (for example SEC 36hrs, FSA 24hrs, DPA 40 days, etc.).
- **Validates records:** by digitally fingerprinting the data at the instant of storage, and validated again when retrieved to prove that it is in the same state as when it was

Data Protection Officer

- **Immediate compliance with DPA:** Your legal duty is to
 - Protect and limit access to personal data in email as required by the DPA
 - To audit access to personal data in
- Put full controls around your management of personal data contained within email messages
- Minimise the time and cost of processing Subject Access Requests (SARs) from the general public or disgruntled employees taking the firm to an employment tribunal.
- Minimise the time and cost of processing Freedom of Information Act requests from the general public or media.

Legal Department

By create a forensically compliant record of email (including attachments) an organisations email can be used as admissible evidence in court.

- **Contract management:**
 - Record employees making ad hoc contracts: these may legally obligate the firm or incriminate the employee.
 - Provide the evidence needed to resolve any contract dispute: Contract actions are time-expired after six or more years after the date of breach, so organisations must keep everything - even when it's an ad hoc contract (for example, "We'll get that to you by Friday").
 - Contracts are very often altered, often unknowingly, by email. Again, retention for at least six years of all email is essential to be able to establish the facts.
- **Intellectual Property:**
 - Track and validate your own Intellectual Property: sending an email to yourself containing the firm's latest IP provides an unalterable validated record of when that IP was created.
 - Refute false IP claims for example, claims such as "we emailed that IP to you three years ago and you've stolen it" can be immediately dismissed.
- **Client dispute resolution:** Clients occasionally come back many months after a transaction claiming that email made a particular undertaking or promise



Finance and Accounts Department

- **Cost savings:** The cost of implementing a technical solution like Cryoserver is less than the cumulative costs of legal fees, fines and reputational damage. The savings in HR alone justify purchase; however there is also a very fast ROI in IT,
- **Compliance:**
 - For accounts departments are passing regulated data around in email there is mandatory retention of business and accounting data for varying periods up to twelve years for the average limited firm.
 - Compliance with cross-border and transatlantic financial regulations that now cover electronic data for example the Securities and Exchange Commission (SEC) requires that all financial organisations retain all documents for a minimum of five years.
- **Access to External Auditors:** Save time and money by giving Archive access to External Auditors: This can be as part of your corporate governance programme, or simply as a cost-saving measure.

Employees

- **Increased privacy:**
 - Employee rights, under the Data Protection Act, are protected by ensuring the data is kept physically secure, electronically secure via encryption, cannot be accessed except by named users, and an audit trail is kept.
 - The Data Guardian system provides a dual check on the security of personal data employees are assured that checks and balances are in place to prevent anyone snooping their email without good reason.
- **Comfort against false accusations:** The exhaustive, tamper-evident record of all email provides irrefutable evidence against false claims.
- **Fast searching:** Of every email ever sent or received since the employee joined the firm: Allows the individual employee to retrieve any accidentally deleted email and immediately find knowledge hidden in old email.

Conclusion

Cryoserver is an effective forensically compliant email archiving solution brings benefits to all areas of an organisation ensuring effective control and management of email records leading to improved efficiencies and lower costs.

Goto www.cryoserver.com for further information on the Cryoserver Forensic Email Archiving solution or contact us on info@cryoserver.com or call on 0800 280 0525