

'Email Compliance' – Does this really mean me?

Introduction

Over the past ten years email has evolved into a recognized communications vehicle. What began as primarily social use is now ubiquitous in the business world. As usage has increased, so has the span and gravity of the information sent – contracts, marketing plans, employment agreements, financial data and product designs. **Email repositories have now become the 'vaults' for over 70% or more of a company's intellectual property (IP).** As email becomes more prominent, so does the oversight required of an organization.

Why is Email Now Being Scrutinized?

The courts are now catching up to the 21st century and acknowledging the weight of digital data in litigation. The Supreme Court ruling on e-discovery and Federal Rules of Civil Procedure (FRCP) in December, 2006 became definitive on email management. **A company/organization will now have the same onus to deliver digital media as it has for paper documents in the past.** What prompted the new interest in digital messaging?

- **Over 90% of data is now created digitally and 75% plus will never touch paper.**
- Email has proven to be a formidable and broad communication tool in the business environment.
- **Email correspondence generally is less formal, more personal and direct.** Let's face it, how many of your emails would you want to be printed on your company's stationary and mailed out? This direct and casual content style is of keen interest to an opposing counsel.
- **Email has a documented event history** showing, everyone who received a copy, forwarding, date/time, and any changes that were applied.

Who is required to comply?

If you think this may not apply to you, look closer to who does need to comply -

- Certain industry groups and/or public companies have regulatory compliance requirements – HIPPA, NASD, SEC, GLBA, Sarbanes Oxley, Federal Rules of Civil Procedure etc.
- Any group regulated by employee related governance – EEOC, Fair Labor Standards, Americans with Disabilities Act.
- If you are involved in a Federal suit (i.e. sexual harassment), or if a suit crosses state lines.
- Finally, many states are now adopting the Fed's FRCP and e-discovery rules for their own.

The best course is to assume you are required to comply. So, how does this affect you as an employer and will it require funding?

What do I Need to Do?

- If you have not already, publish and distribute a documented policy advising all employees that email is a corporate tool to conduct company business. Inappropriate use, language or questionable content is not to be used. There is **no assurance of personal information privacy - all email correspondence belongs to the employer.**
- **Implement a comprehensive email archival program** – not a backup policy. Backups are similar to storing boxes of loose documents in a warehouse. You know it is probably there, but you hope you never have to go find specific items. **Imagine a request for a chronological report showing all the email correspondence and file attachments for three employees for a six month period three years ago.**

An archival system would be able to deliver this type of request in seconds. A backup system of multiple tapes could take months, which you may not have. The ROI on an archival system becomes quickly apparent on your first request.

Will This Become More Overhead I Need To Manage?

There will be costs to implement an archival system, but there are ancillary benefits that can actually give you an ROI with this solution.

- Relief on the mail server storage. Many employees never delete their email or attachments. **As usage and volume increases, the need for additional storage is perpetual.** An archival system could systematically delete emails based on roles/policy and retention parameters you define. The email is never actually lost, as the archival system always maintains a 'read only' copy. Employees can be given access to their specific emails via a browser based tool in the archival system.
- Efficient storage and compression. **Attachments and multiple emails are not stored multiple times.** If an email with a 3 MB attachment is sent to ten recipients in the company, only one copy of the attachment and email is compressed and stored. This is called 'single incident storage'. Retrieval on any of the ten users would show the email and attachment in full content. Additional efficiencies are gained by compression. A 10:1 data compression is becoming common on archival appliances.
- Disaster recovery/ Business Continuity. Email has been proven to be critical to a company's business execution and needs to be restored ASAP in the event of business interruption. **An archival system will quickly restore all history to within the minute of interruption.**

- Compliance reviews/proactive management. The archival system can also filter content and trigger notifications. If for instance, a credit card or social security number is sent out via email and is not allowed, it can be detected as it is stored. Immediate notification to an administrator would occur allowing you to deal with the incident in a proactive mode. Periodic reviews can also be performed to assure your emails policies are being followed.

Hopefully, you can see benefits to implementing an archival system and not only 'regulatory burden'. Visit our website for more info and Case Studies of how simple and quick deployment can be for your company.

Dan Schutte is the owner of [Enclave Data Solutions](#), specializing in messaging security, content filtering, anti-spam software, data archival and compliance systems. Visit our website to read actual Case Studies of how companies have successfully protected their data networks and met compliance requirements. Free trials and downloads are available on all of our products.

Does your company have a formal written policy in place for your email usage? Request our **free** Word template '**Policy on Email Usage and Archival**' that you can customize to your environment in less than thirty minutes. This could become a notable first step to addressing email compliance in your workplace. Contact info@enclavedata.com for a copy.

Please feel free to republish this article provided a working hyperlink remains to our site