

THE TEN BIGGEST MISTAKES OF E-MAIL RECORDS MANAGEMENT — AND HOW TO PREVENT THEM

IS YOUR COMPANY COMMITTING ANY OF THE TEN BIGGEST MISTAKES OF E-MAIL RECORDS MANAGEMENT?

If the answer is yes (or you're not sure) your company may be incurring additional costs and risks that can be avoided. This white paper describes the problems, costs and risks associated with these mistakes - and unveils industry best practice recommendations on how to prevent them.

MISTAKE #1: WE CAN LIVE WITHOUT AN E-MAIL MANAGEMENT SYSTEM FOR NOW.

Most companies understand the power of e-mail as a business tool - too few understand its costs and risks. Many companies keep buying new e-mail servers as they fill up. They let employees do whatever they want with e-mail or they have e-mail policies, but they don't enforce them.

E-mail has gained too much prominence to let it run rampant. The costs of storage, the impact on overwhelmed e-mail servers, and the legal and credibility risks from not being able to find e-mails when required, can make complacency a costly and damaging mistake. The damage can go beyond fines and settlements to a loss in corporate credibility that drives down a company's stock price.

Research firm IDC estimates corporate e-mail volumes have increased 29% annually, from 9.7 billion per day in 2000 to 16.2 billion in 2002 and 20.9 billion daily messages in 2003. [IDC, 2002]. The Radacati Group estimates that a typical corporate e-mail account sends and receives about 7MB of data per day. For a company with 1,000 users, that's an average of 140 GB per month. [The Radicati Group]. The average e-mail server is saturated in just 18 days.

IT administrators spend eight to 12 hours per week on e-mail backup and archiving, and an additional five to six hours per week recovering deleted or lost messages for users. [Creative Networks, Inc. (CNI) 2001]. That means IT administrators are spending more than a quarter of their workweek on e-mail management.

Courts are generally unsympathetic to a company's excuses about the difficulties of obtaining information because of technology problems or excessive workload. Federal Rule 26 of Civil Procedure explicitly requires that litigants affirmatively turnover "relevant" discovery information early in the litigation process. The bottom line is that e-mail discovery can burden organizations that have not implemented rules and invested in technology to retain and access required e-mail. [N. Flynn and R. Kahn ESQ, 2003]

What is Discovery?

Discovery is the part of the litigation process in which opposing parties exchange relevant documents, testimony, and other information. Litigants generally request and receive information necessary to build a case in preparation for trial. Discovery helps each side understand the material facts and evidence in advance of the trial. It also prevents anyone from being ambushed in the trial. [N. Flynn and R. Kahn ESQ, 2003].

In a recent ruling, *Zubulake v. UBS Warburg*, the U.S. District Court of New York set a clear precedent that e-mail should be treated like any other "accessible" data to be produced in discovery, and therefore the producing party will likely be responsible for all or at least the vast majority of the e-discovery costs.

Recommendation

Companies that have ignored the problem of e-mail management need to begin to develop a comprehensive e-mail management program - now. Here are Iron Mountain's recommendations:

- Establish appropriate employee e-mail usage and content rules. Monitor employee e-mail to ensure compliance with these rules.
- Apply the organization's records retention schedule to e-mail records.
- Establish that e-mail messages are only to be saved for legitimate business or legal reasons.
- Migrate official e-mail records to an approved e-mail management system.
- Purge e-mails that are not official records from the e-mail system on a regular, but pre-defined schedule.

MISTAKE #2: DESTROY ALL E-MAIL BY AUTO-PURGES OR MAILBOX CAPS IN THE HOPE THAT IT WILL SOLVE THE PROBLEM.

Some companies concluded that drastic action was needed to control the exponential volumes of e-mail on servers, and the potential time bombs contained in them. So they implemented 30-day e-mail deletion policies or mailbox sizes limits.

This approach is inherently flawed and flies in the face of decades of records management practices. Good records management practices dictate that you find out what you legally and operationally need to keep, determine the retention period, and implement that policy consistently, regardless of the record's format.

Today, many industries have explicit regulatory requirements for keeping e-mail - notably broker-dealers and investment firms regulated by the SEC. Five big Wall Street brokerages were fined \$8.25 million in December of 2002 for failing to preserve electronic messages. Even for companies in industries that are not heavily regulated, e-mail has become an essential tool for doing business, hence an increasing number of e-mails have become official records. These e-mail records are subject to the same legal retention requirements as paper documents. (For example, companies are required by law to retain all employment records (paper, electronic and e-mail) such as hiring documents, job applications, resumes, job inquires, and refusals to hire for one year following dates of personnel action. 29 U.S.C. 62;29 CFR 1627.3. [Cohen and Mohr LLP 2002].)

From an operations perspective, employees often have a need to access their own archived e-mails. IDC estimates that 60 percent of business critical information is stored in messaging systems - but 81 percent of business users cannot access their own archived messages and attachments [IDC, 2000]. This is often the result of companies forcing a "destroy all e-mail" edict through auto-purges or mailbox caps.

To get around these edicts, employees often store messages locally in personal folders. The end result - e-mails are often difficult to find, impossible to search, prone to corruption and remain a legal liability long after the point when they should have been purged.

Recommendation

Companies should do for e-mail what they do for other business records:

- Establish a policy that includes legal and operational needs.
- Train employees and provide ongoing e-mail policy communications and education.
- Give employees the tools by which appropriate e-mail can be archived.
- Allow managers to immediately modify the system to identify and protect additional classes of e-mail as new obligations to preserve information and evidence is required. [Cohen and Mohr, 2002].

MISTAKE #3: USE YOUR BACKUP TAPES AS AN ARCHIVE.

Many companies think they are archiving their e-mail because they back them up onto tapes. But backups are designed to restore entire systems - locating unindexed, individual records is difficult and expensive.

The goal of tape backup is to create a temporary copy that can be accessed and restored if the primary system has a failure. They are not intended for routine exploration, discovery or retrieval. They are almost impossible to efficiently search because they are not indexed.

Compounding the problem, IT has a tendency to hoard multiple copies to support system recovery and avoid data loss rather than purge based on retention. These redundant volumes increase discovery costs and risks of uncovering "surprises". For example, discovery searches can cost up to \$2500 per backup tape. A single search can start at \$90,000 and quickly climb to seven figures. [Computer Forensics Inc. 2001]. Plus, delays encountered as a result of difficulty in locating information, may be interpreted as bad faith.

Recommendation

Companies need to recognize that backups are a critical, but separate process from archiving. Compliance, records management and legal, need to work closely with IT to ensure that the backup policy is reasonable and in synch with the organization's retention policy. A good, reasonable practice for back up is to only keep daily tapes and to rotate those tapes every 30, 60 or 90 days based on your operational requirements.

E-mail business records need to be stored and managed in a digital archive designed for low-cost, long-term archiving. This archive should have tools for easy searching, discovery organization and retention management. According to IDC, digital archiving will come to be seen as a critical part of overall data and content management. This process will be adopted as a way of avoiding legal and financial exposure, meeting regulatory requirements, and organizing and leveraging resources and corporate knowledge. [IDC,2002].

MISTAKE #4: CONSIDER E-MAIL MANAGEMENT SOLELY AS AN IT ISSUE.

To some firms, e-mail management is purely an IT issue. IT has sole responsibility for designing policy and for implementing archiving practices. In addition to the fact that IT systems are designed for recovery, not retention, it is unrealistic to expect IT alone to:

- Understand all the specific legal retention requirements.
- Develop a policy in synch with existing paper records management policy.
- Drive adoption of the policy throughout the company without senior management leadership.

Implementing technology without the proper policy guidance is irresponsible.

Recommendation

E-mail management is an IT, legal, compliance, and records management issue. Companies should ensure that stakeholders from all of these departments are involved in the e-mail management system design and implementation, in order to ensure that all business risks are being addressed.

MISTAKE #5: CONSIDER E-MAIL MANAGEMENT SOLELY AS A LEGAL OR COMPLIANCE ISSUE.

Some companies approach e-mail management purely from a legal or compliance view. They forget about IT and end-user concerns. Legal or compliance departments working alone may stipulate that IT save all e-mails. This results in strained storage budgets, e-mail systems performance degradation and system crashes. Legal or compliance may also define archive systems that only they can access. If employees can't easily access their archived e-mails, they will store them locally - defeating the purpose of the archive system. Compliance or legal departments working alone are likely to define an onerous e-mail archive system that requires the employees to take so many steps to save e-mail that they just ignore it. Developing an e-mail management program without practical technology will be ineffective.

Recommendation

Companies need to engage all stakeholders: compliance, legal, IT and end users to design and implement a compliant e-mail management solution that is cost effective and manageable for IT and practical for employees.

MISTAKE #6: ASSUME THAT YOUR EXISTING DOCUMENT MANAGEMENT SYSTEM CAN HANDLE E-MAIL.

Companies that have a major investment in a document management system may believe that this system can be adopted for e-mail management archiving. Big mistake. The volume and indexing requirements for enterprise-wide e-mail archiving are dramatically greater than standard document management volumes. For example, a major corporation will often need to store over 20 million e-mails per month. That translates into archiving terabytes of e-mail per month. Assuming both the message content and attachment are indexed, over a six-year period, that would add up to 72 terabytes of storage and a 21 TB database - a much bigger volume than most document management systems can scale to handle. Even if your document management system can scale, you'd have to spend a lot of money to add the horsepower needed to scale to your company's needs. For many firms, this will mean having to purchase a whole new system.

Recommendation

Companies should determine their monthly and yearly e-mail archiving volume and indexing requirements. IT needs to determine whether or not the existing document management system can scale to support the companies e-mail volumes. IT should also evaluate the scalability and costs of dedicated e-mail management archiving solutions vs. upgrading their document management solutions. In most instances, a dedicated e-mail management solution will be more cost-effective and provide much greater scalability than enhancing the document management system.

MISTAKE #7: IMPLEMENT AN E-MAIL RETENTION POLICY THAT WAS OPTIMIZED FOR PAPER.

Many companies make the mistake of trying to implement paper records retention policies without any consideration of the unique requirements of e-mail. But the user classification processes for paper records don't work for e-mail due to:

- The massive volume of e-mail.
- Everyone within an organization uses e-mail.
- Administration can't be easily delegated like paper records.
- Too many record classifications to be practically used by end users.

Implementing e-mail retention based solely on a paper records retention policy will almost certainly result in an onerous process that employees will not adopt.

Recommendation

E-mail retention must be made simple for employees. Companies need to use their existing paper records retention policies as a framework for developing record classifications, rules, schedules, and policies that have been simplified and optimized for e-mail records. User intervention should be kept to a minimum to help insure adoption.

MISTAKE #8: UNCONSCIOUS DESTRUCTION OF E-MAIL EVIDENCE.

Companies that are being investigated or audited who destroy e-mail as part of their standard retention policy may not even know they are taking a big risk. Companies that have reason to believe they will be party to a lawsuit, investigation or audit are breaking the law if they destroy any relevant e-mail - even e-mail that would normally be scheduled for destruction.

[N. Flynn and R. Kahn ESQ, 2003].

Recommendation

Companies are obligated to retain evidence that's likely to be relevant to pending or imminent legislation. Every company needs a "records hold" mechanism to ensure that required paper and e-mail records and other evidence are preserved in the context of imminent or pending litigation, audits, investigations and other formal proceedings. Through a documented process, all affected employees should be informed of their obligations to find, preserve and produce required records and other evidence. [N. Flynn and R. Kahn ESQ, 2003].

MISTAKE #9: CONSIDER E-MAIL MANAGEMENT TRAINING AND EMPLOYEE COMMUNICATIONS AS AN AFTER-THOUGHT.

A number of organizations are guilty of mistake #9. They invest heavily in developing e-mail management policy and technology solutions. But they under invest in the proper training and communications required for adoption of the policies. E-mail management policy and technology without training is wasteful and potentially dangerous.

Recommendation

Companies must take the necessary steps to ensure that employees are:

- Made aware of the organization's e-mail policy.
- Provided easy access to the policy.
- Provided training regarding the policy's importance and requirements.
- Sign a statement that they have received, read and understood the policy.
- Provided ongoing communications to help them keep e-mail policy in mind.

MISTAKE #10: ONLY CONSIDER DEVELOPING YOUR E-MAIL MANAGEMENT SOLUTION IN-HOUSE.

After realizing they need an e-mail management solution, many companies automatically assume that implementing an in-house solution is the best way for them to go. For many companies this could be a major mistake for one or more of the following reasons:

- Implementation timeliness - an in-house solution can take six to nine month to implement. That's a long time to be at risk in today's regulatory climate.
- Expense - depending on your company's e-mail volume, additional storage technology investments can quickly run into the millions of dollars. For a large broker-dealer generating 9.5 terabytes of e-mail per year, the in-house archiving costs for the SEC's required three years would be over \$2.8 million. A mid-sized firm storing an average of 1.8 terabytes of e-mail would spend about \$1.1 million over three years. Even a small firm storing just 12 gigabytes can easily spend more than \$270,000 over three years. Storage costs may be decreasing, but not nearly as fast as e-mail volumes are increasing - resulting in overall higher expenses.
- Expertise - finding either qualified IT staff with archiving experience and expertise, or records management experts for e-mail management is no easy task. The indexing of e-mail and instant message records typically requires a huge database - as much as 3 terabytes - that will require top-notch database administration expertise.
- Maintenance - trying to store and manage the blistering volume growth of e-mail means constant headaches and the tying up of IT personnel resources. On average, most organizations find that archive maintenance of 1 terabyte of archived e-mail messages results in a \$100,000 expense annually. [Legato, 2002].

Recommendation

Companies should evaluate both in-house and outsourced solutions for e-mail management. Here are Gartner's recommendations on what you should focus on in your evaluations:

| Considerations for Internal Implementation and Management | Considerations for Evaluating Outsourcers |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> • Capital spending • Application of critical IT skills • Managing capacity • Asset life/refresh • Maintenance costs • Costs to migrate storage media • Real estate use | <ul style="list-style-type: none"> • Service line viability • Technical quality • Ease of doing business • Customer satisfaction • Contract terms and conditions/ Service Levels |

[Gartner, 2002]

When evaluating outsource solutions companies should consider Iron Mountain's Web-based e-mail archiving solution to take advantage of the following benefits:

- Faster implementation - weeks not months
- Lower costs - on average 30+% lower TCO than an in-house solution and dramatically less expensive for discovery searches
- Credible e-mail and records retention program designed by experts.

All from the service provider more companies trust to manage and protect their important information - Iron Mountain.

Conclusion

These ten mistakes are the most prevalent and dangerous. If you think your company is committing one or more of them, we urge you to consider:

- e-mail as a vital communications tool will only become more prevalent
- e-mail volumes in your organization (and your potential e-mail storage costs) will continue to escalate for the foreseeable future
- e-mail is now referred to by many lawyers as "evidence mail" [Fortune, 2003]
- The rash of accounting irregularities and allegations of wrongful document destruction are driving both stronger enforcement of existing regulations as well as new laws with stronger penalties.

Ignoring these mistakes is not worth the costs, headaches and legal risks - contact us today.

Iron Mountain Digital Archives
(800) 935-6966 x2800
digital_archives@ironmountain.com
www.ironmountain.com/digital