Best Practice For Email Retention

Table of Contents

Objective

Developing a workable email retention policy is vitally important for most organisations, as it helps define what messages need to be kept and for how long. But how do you ensure that you retain only what you need and nothing more?

Email retention is especially tricky for a number of reasons.

Email Volumes:

The volume of email created is staggering. Consider these facts: more than 99 percent of all documents are created and stored electronically, and somewhere around 60 billion emails are being created and sent each day, according to analyst firm IDC. Because email is easier to store, more of it is being retained and archived on backup tapes, servers, desktops, laptops, mobile devices and within archiving solutions.

Informality:

There is still a casual informality associated with email. While some email threads are not business records, many others are. And, unfortunately, sometimes it is challenging to tell the difference. Is the email about scheduling lunch related to talking about your weekend or talking about your company's upcoming acquisition?

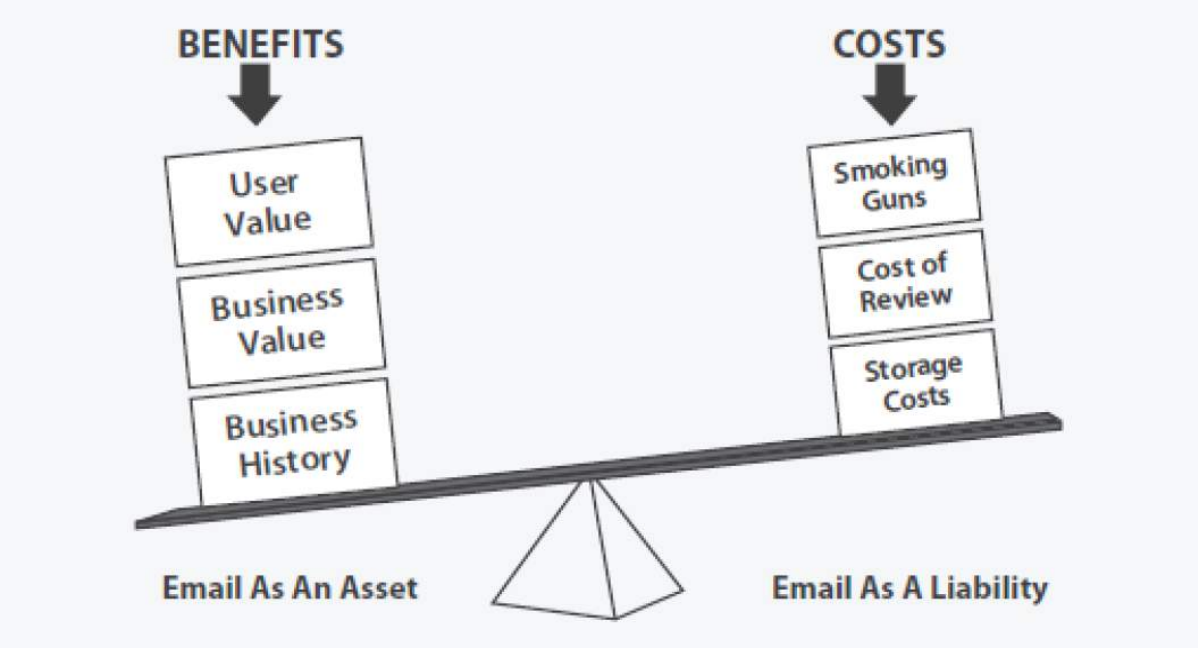
Universality:

Unlike some documents that may represent a company's intellectual property, which may only be created and shared by a handful of individuals at a company, email is ubiquitous and is used by everyone (not just 5 percent of your employees).

The purpose of this paper is to provide some best practices for clients grappling with email retention.

Throughout the course of our history, and as the leading hosted email archiving provider, we have witnessed companies struggling with email retention and provided guidance for hundreds of them looking to craft usable and workable email retention policies. We have seen organisations deploy a number of different models and frameworks with varying degrees of success. The fundamental question in email retention is whether to retain or delete each given message.

Exhibit A: The Unfair Tradeoff



Customers only want to retain what they need:

Inevitably, organisations must weigh the advantages of retaining information (in terms of its use to the business) with the liabilities of storing that information (e.g., storage costs, legal costs and risks that the messages come back to haunt you). This is further complicated by the fact that companies sometimes find messages they were not required to retain to actually be advantageous in arguing their case in an investigation or litigation matter.

Just because you've deleted your company's copy of a message doesn't mean the message no longer exists. Since email messages have a FROM and a TO, there are inherently multiple copies of every message, many of which are outside your company's control.

So how does a company balance all of these factors?

Bottom Line:

Though the decision on whether or not to retain data is complicated, if you have the data, it's better to store it all in one place. This way, you can easily and cost effectively search it for email discovery and other purposes, versus having it spread across servers, desktops, laptops, mobile devices and backup tapes.

Key Considerations

Companies are creating and storing electronic information at light speed. As email has emerged as a mission-critical business application, both the volume and size of emails have grown exponentially, causing storage requirements to increase more than 50 percent per year. According to technology market research firm, The Radicati Group, storage requirements will grow from almost 18 MB per user, per day in 2007, to more than 28 MB per user, per day in 2011. This growth rate has had a significant impact on Exchange/email administrators.

But when it comes to answering the fundamental question, "How long should you keep email around?" there is no one-size-fits-all policy. Regulatory issues aside, there are some key issues to consider:

What should you archive? Some companies choose to archive all email for all users, while others choose to archive selected users (e.g., those on legal hold or in regulated roles) or selected messages. Make sure you understand which regulations apply to your business before determining what to archive.

How long should you retain messages? Most companies retain information indefinitely, assuming that even if they deleted their copy, another copy likely exists somewhere. Some companies have a blanket retention period for all data (e.g., 7 years), while others have granular retention policies by user or by message.

At the end of the retention period, how do you dispose of data? You have to ensure no data on legal hold is deleted. In addition, you want to make this process as minimally invasive as possible.

Your answers to the following questions will help you decide what you need to archive, how long you need to retain these messages and how you dispose of email after the retention period has expired:

Table A: The Unfair Tradeoff

Consideration	Key Questions
What to **ARCHIVE**	• Do you need to archive all users or selected users? • Do you need to archive all email or selected email? • Is there minimal impact to end users?
How to **RETAIN**	• Do you need to retain everything the same way? • Can you really delete every copy of messages? • Is there minimal impact to end users?
How to **DISPOSE**	• Do you need to enforce non-tampering during retention? • Do you wish to automatically expire content? • Do you need to enforce litigation/legal holds?

Unfortunately, there is no general consensus about how long you should retain your email (unless you are in a heavily regulated industry, where the retention periods are clearly defined). This should not be surprising. It simply points to the complexity of matching business and legacy policies to the huge, unstructured and informal volume of email communications we have today.

Regardless of these considerations,in the US, the amendments to the Federal Rules of Civil Procedure, also referred to as FRCP, (see Appendix C) make it clear that what you have in your possession needs to be preserved and discoverable. The FRCP amendments apply to any organisation that has the potential to be involved in litigation in the U.S. Federal Court system. In short, the amendments mandate that companies be prepared for electronic discovery.

The same was applied to the Irish Court system in 2009 when order 31 of the Irish Rules to the Superior Courts were amended to include the discoverability of Electronically Stored Information.
The Civil Procedure Rules (CPR) in the UK essentially serve the same purpose as the Federal Rules of Civil Procedure (FRCP) in the United States and the issuance of Practice Direction 31B in October 2010 adds teeth to eDisclosure requirements much like the amendments to the FRCP in December 2006 added teeth to eDiscovery requirements in US Federal Court.

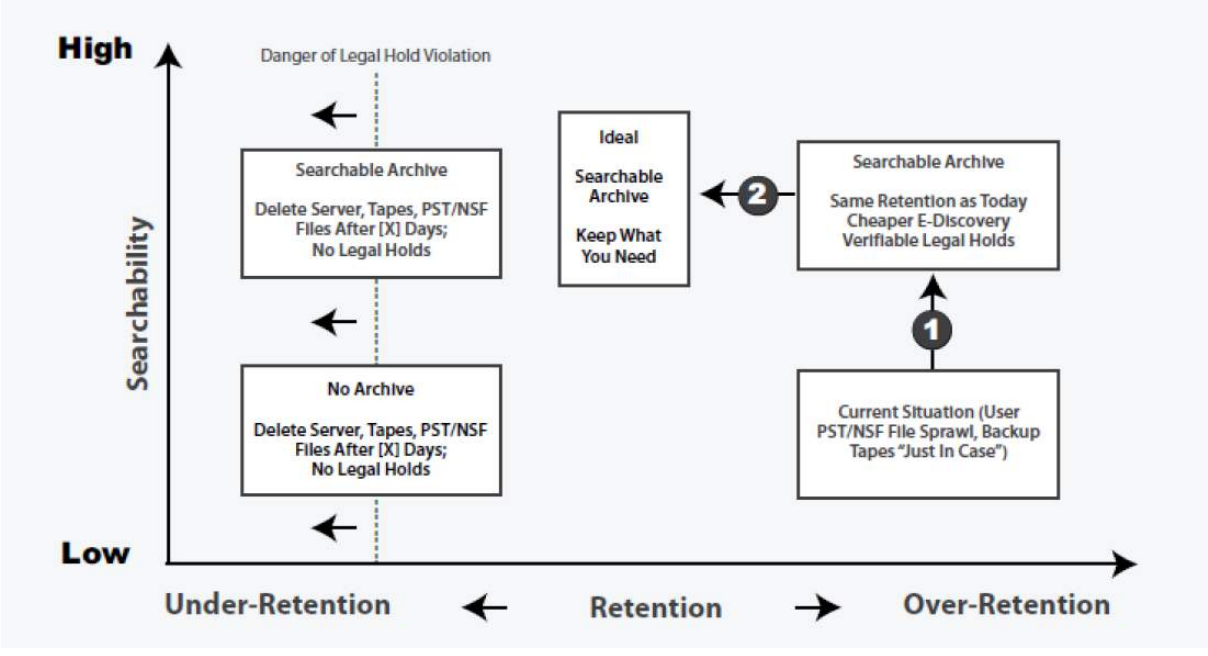
Your organisation must know where your data is, how to retrieve it, how to meet data requests and must determine what data is not subject to search.

All things considered, the ultimate question is, what system of retention yields the highest ROI and/ or least risk (in terms of the individual business)? Once you've thought through these issues for your email retention, you'll probably need to talk to an expert to make sure you are managing your risk as effectively as possible.

Email Retention: A Balancing Act

Unfortunately, many organisations and email administrators are facing challenges from all sides when it comes to email retention. Despite official policies or limits on your email server, if emails are retained indefinitely and stored in multiple formats (e.g., desktop, laptop PCs, PSTs/NSFs, thumb drives and/ or backup tapes), it becomes difficult to perform consolidated searches. Moreover, implementing an enforceable legal hold becomes impossible to guarantee, which creates legal risk and exposure.

Exhibit B: Retention vs. Searchability



Without an archive, the situation for most companies is the worst of all worlds:

Retention:

Employees decide what to keep and what to delete. Extra copies of data are buried on desktops, laptops, mobile devices and backup tapes. More often than not, the information you were supposed to keep (e.g., on legal hold) isn't available, while the information you could have deleted still exists.

Storage:

The storage approach without an archive leads to further headaches and costs for IT staff. Bloated email stores result in evermore storage purchases. Attempts to restrict mailbox size through email quotas just pushes the problem onto the corporate network, where users squirrel away local archives (e.g., PST or NSF files), clogging up storage space and creating recovery headaches. Exploding email storage also creates a backup window nightmare for IT. As a crude attempt to enforce legal holds, many IT organisations are forced to retain some or all backup tapes indefinitely, using up valuable tape capacity and IT budget.

Discovery:

When you want to find information in question for a legal matter or an internal investigation, IT fire drills and costs abound without an archiving solution in place. IT is often forced to devote staff time or third-party budget to backup tape restores, network file share searches and desktop/laptop collection. Inevitably, IT then produces a large preponderance of irrelevant data, increasing downstream data processing and legal review costs. Ultimately, IT is inherently stuck in the middle of the lawyers and the data they seek.

By simply implementing an email archive, even with indefinite or undetermined retention policies, IT organisations can vastly streamline their operations:

- Enforce consistent retention and adherence to legal holds
- Reduce storage and backup issues and costs
- Shrink discovery costs and simplify the process overall

Furthermore, with a hosted archiving model that offers unlimited storage, IT can truly offload the entire long-term email storage problem to the hosted provider.

To provide a framework for creating a "workable" email retention policy, we have developed a five-phase approach:

Phase 1: What is the Law?
Phase 2: Email Preservation and Searchability
Phase 3: Different Retention Approach
Phase 4: Creating and Evangelising an Email Retention Policy
Phase 5: Implementation and Flexibility

Phase 1: What is the Law?

Is your company in a heavily regulated industry that has existing data retention requirements? Outside of regulations governing certain industries, the answer is usually a bit nebulous in terms of defining clear retention periods. In the US For SEC- and FINRA-regulated firms, Rule 17a-4 of the Securities and Exchange Act requires retention of emails for at least three years, with the first two years stored in an easily accessible place. In the UK the Financial Services Authority (FSA) regulates financial services providers. The FSA's regulations require all financial institutions to store all business emails sent and received for up to six years, and some emails indefinitely, so that cases can be reviewed.

But outside of financial services, there is no universal law for document retention. The only far-reaching requirement is to preserve documents, emails and information when a company is on notice of pending litigation (per FRCP(US) CRP(UK)). At this point, a "litigation hold" must be implemented to retain information the company reasonably believes is discoverable in anticipated litigation. However, email retention requirements vary from industry to industry and from case to case.

Following is a breakdown of the primary regulatory bodies and/or regulations that apply to email retention at a variety of regulated industries and general businesses.

US

Banking: FDIC, OCC (Office of the Comptroller of the Currency)

Telecommunications: FCC – Title 47, Part 42

Pharmaceutical: FDA – Title 21, Part 11

Healthcare: HIPAA (Health Insurance Portability and Accountability Act)

Defense: DOD – 5015.2 Standard

Brokerage Firms: SEC – Rule 17a-3 and 17a-4

Investment Advisors: SEC Rule 204-2 (Books and Records Retention)

General Business Oversight: Sarbanes-Oxley Act (SOX)

SOX is the government's response to the Enron debacle. It contains provisions for record retention and audits. It strongly discourages anyone from altering, destroying, hiding or falsifying records in response to a federal investigation or bankruptcy proceeding. Penalties include significant fines and/or imprisonment of up to 20 years.

UK

Freedom of Information Act 2006

The Data Protection Act 1998 (DPA) applies

Court Action under the

The Sarbanes-Oxley Act

Financial Services Authority (FSA)

Employment Tribunals

The Data Retention Regulations 2009

Ireland

Freedom of Information Act 1998 Amended 2003

Data Protection (Amendment) Act 2003

Statutory Instrument No. 93 of 2009 has made some significant changes to electronic discovery in Ireland. Here is a summary of the effects:

- a party may seek electronic data in searchable form from its opponent;
- the court may order a party to give inspection and search facilities for electronic data on its computer systems to the other side

- where computers contain sensitive non-discoverable data, the court instead may order that an independent expert carry out the inspection and search for relevant electronic data (the party seeking that discovery will have to fund the expert's costs and expenses)
- where a party giving discovery finds that searching for the documents or data is excessively costly or burdensome, it may apply to the court to seek to narrow the scope of the discovery order
- a party giving discovery must list the documents or data according to agreed categories or in a sequence corresponding with the manner in which the documents or data has been stored or kept in the usual course of business – the intention is to make discovery more comprehensible
- all parties giving discovery must swear in an affidavit of discovery that they understand their obligation to give discovery of documents and electronic data (within the categories of discovery agreed or ordered by the court) which may help or damage their case in any way.

The Sarbanes-Oxley Act for US related companies

Employment Tribunals

Given such regulations, legal considerations and electronic discovery are quickly becoming the primary drivers for archiving and email retention policies. Increasingly, it is becoming imperative to have an email retention policy and a means of implementing litigation holds if your company even has a small chance of being sued in civil court (i.e., most organisations). Recent spoliation case law (see Appendix B for lessons gleaned from recent cases) demonstrates the devastating impact of not having these measures in place.

Are you saving a complete email data set?

If challenged or facing litigation proceedings, your email data must be complete. Can you retrieve the content of an email that is five years old? In addition, can you:

Identify clear policies applied to each email?

Demonstrate the inability to tamper with or delete email and attachments?

Ensure that messages involved in litigation or potential litigation are placed on legal hold?

Perform and save detailed searches of all company email?

If not, where do you start?

Phase 2: Email Preservation & Searchability

After understanding which regulations apply to your industry, one of the first phases we typically address with our clients is email preservation and the searchability of the archive. Our guidance to clients (regardless of industry) is to start archiving as soon as possible. You can apply retention policies after the fact, but you want to start consolidating your email stores into a single, online repository.

After your email is being securely captured, stored and indexed in the The Email Laundry archive, you can quickly search the entire contents of archived emails and attachments, using a variety of search criteria, including to, from, date, subject, message body, message attachments and other message properties.

Please see ***Exhibit B*** on page six for some of the challenging tradeoffs between email retention and searchability.

Reviewers can efficiently navigate through search results, identify highlighted search terms and tag potentially harmful emails, so they are easily retrievable for further review. Once you have tagged all emails related to a specific case or matter, you can export the results into a case management solution or other application for further review and analysis. Reviewers can create and save customised email searches based on your organisation's email policies and rerun them as necessary. Reviewers can also setup Policy Alerts to notify them when an email meets Saved Search criteria (e.g., contains specific words or phrases).

These features ensure that your archive can be searched without causing IT interruptions, searches can be performed by outside service providers or consultants (if necessary) and you avoid the typical cost over-runs associated with advanced searches. One of the biggest advantages of a hosted archiving solution with these types of searching capabilities is the ability to quickly cull large data sets and produce only the most relevant emails for in-house attorneys, case management tools and eventually opposing counsel. Given the current cost of e-discovery (typically more than 30 percent of a lawsuit's total cost), the cost savings from efficient data searches can be significant, since the most expensive part of any discovery phase is the attorney time spent reviewing documents and emails.

Phase 3: Different Retention Approaches

At The Email Laundry, we have seen firsthand how different organisations approach email retention with varying levels of success. Following is a snapshot of the most common type of retention policies that we've seen deployed:

Savers:

Most companies are concluding that information is going to exist no matter what, and it is better to save it. This way they know that the emails are preserved within the archive, they have them for business value and they don't have to deal with the implications of deleting email (i.e., from an end user, legal or business case perspective). Thus, they retain data indefinitely.

Procrastinators:

A large segment of companies have retention policies set, but set deletion dates well into the future. In these cases, many organisations have not yet had to delete emails from their archives. Others continually extend the expiration dates when they come due, which effectively nullifies the written policies.

Fixed Period:

A small group of clients want to keep data for all employees for a fixed period (e.g., three years), except for emails placed on litigation holds.

Group Level:

Some organisations stipulate different retention periods based on specific user groups (e.g., executives). This is often the case with large businesses, where certain groups (e.g., SEC-regulated employees) have specific retention periods mandated by regulations.

User Driven:

This approach applies a short default retention period for all items, unless a user tags an item as being appropriate for longer retention.

Comparing Your Retention Options

As discussed, email retention is clearly a balancing act, but understanding your options and the pros and cons associated with each option can help you develop your organisation's email retention policy. Based on our experience, we have seen the following retention policies put into practice.

Table B: Compaing Your Retention Options

Option	Who Uses It	How It Works	Pros	Cons
1. Retain All Emails Forever	• Vast majority of customers • Some large customers	• Journal all users • Infinite retention • Unclear on what can be deleted	• Never lose business information • Least issues with user acceptance • No risk of "under-retention" or legal hold violations • Retain data that could be useful in litigation	• Potential risk of keeping something you could have deleted that becomes a "smoking gun" (though perhaps it would have been produced anyway) • Extra storage costs (not relevant in a hosted, unlimited archiving model) • More information to search and cull for discovery and investigations
2. Expire archive after X days	• Some large customers	• Journal all users • Fixed retention (e.g., 90 days) • Typically place hold on items involved in litigation • Many have set date far in future so they haven't deleted yet • Replacing tape infrastructure with standard [X] day recycling • Unclear on what can be deleted	• Eliminated "over-retention" risk (assuming no other copy exists) • Controlled storage costs (not relevant in a hosted, unlimited archiving model)	• "Under-retention" of items that could be legally discovered • Risk that items still exist elsewhere (e.g., PSTs/NSFs) • Loss of important corporate information • Challenging user adoption
3. User-Driven Retention	• Law firms and other professional services organizations • Firms with sophisticated Records Management (RM) processes and taxonomies	• Present users with tags for various retention periods (e.g., 3 years, 7 years) • Short retention if user doesn't tag message	• Granular categorization • Theoretically keep only what you need	• Users need to be educated on Records Management • User effort for classification • User mistakes or intentional deletion can create risk • Users may just default everything to longest retention possible

Note: The Email Laundry can selectively archive (or exclude from archiving) an individual user's email. Users can also self-select retention periods for each email, using the tagging feature in The Email Laundry Personal Archive.

In light of these various shortcomings, a growing number of organisations are retaining everything indefinitely and make no systematic attempts to delete emails at all. In the end, the most effective retention periods are often the ones that are the simplest and easiest to communicate and implement.

Phase 4: Creating and Evangelising an Email Retention Policy

First and foremost, companies should have an email retention policy, and it must be actively enforced and audited.

Keep It Simple

When it comes to crafting your email retention policy, it's critical to keep it simple. First, let's review some best practices when creating email retention policies.

- **Simplicity is the key:** If you have a 100-page retention policy you created for your paper records management strategy, throw it out. Well, not really. But, you should trim it down to something that your users can understand in the electronic world.
- **Engaging your end users:** If you want your users involved, your retention policy needs to be super simple (i.e., no more than three to five categories and a simple action for categorising). Plus, make sure to explain the rationale for having an email retention policy in the first place.
- **Expect your users to cheat:** If you offer multiple retention periods, assume many users will choose the longest. Similarly, if you provide a restrictive policy, assume users will find ways to save data outside of the system (e.g., PST/NSF files or USB hard drives).
- **Apply common sense:** There is no way for a computer to automatically figure out what an email message really means. This means either your users have to be involved, or you have to use basic rules (e.g., assign retention periods to specific user groups, etc.).
- **Multiple copies of the same email:** There is no point deleting data in one place (e.g., archive) and leaving it exposed and discoverable in other places (e.g., in PST files on user desktops). If you are going to delete from the archive, make sure you: (a) are not retaining backup tapes longer than the archive retention period; and (b) disable the creation of local archives (PST/NSF files) from your email server.
- **Importance of legal holds:** No matter what retention policy you create, make sure you retain data that is on legal hold. Nothing is more detrimental to your case than spoliation of electronic evidence (i.e., the intentional or negligent withholding, hiding, alteration or destruction of evidence relevant to a legal proceeding). Even if you just anticipate litigation, you are mandated to preserve any email message(s) and ensure that you can make those emails available to opposing counsel (no matter how hard or expensive it is to search for and retrieve them).

Crafting an Effective Email Retention Policy

When crafting your email retention policy, make sure to address these important considerations:

- Identify clear policies applied to each email
- Demonstrate the inability to tamper with or delete email and attachments
- Ensure messages that are involved in litigation or potential litigation are placed on legal hold
- Perform and save detailed searches of all company email

Involving all areas of the company

Many companies make the mistake of not involving all areas of the company when creating an email retention policy. An email retention policy is not just a legal document, it affects employee productivity companywide. It is important that you understand how employees use the email system. Do they create their own personal archives? How often do they reference old emails? Understanding these things ensures you don't put procedures in place that will adversely affect employee productivity.

Enforcing the policy

Are you planning to put an automated email archiving system in place, or will you rely on manual procedures? You can rely on manual procedures, but you will need to include step-by-step email retention instructions that employees can follow and provide employee training to ensure the policy enforcement. In most cases, an automated email archiving system ensures policy enforcement and raises employee productivity.

Communicating the new policy to all employees

Employee communication and training can lower your compliance risk and legal liability. A good email retention policy should include the following information:

- Person or department responsible for the policy
- Scope/coverage
- Purpose of the policy
- Policy statement: This can include a company philosophy statement about the business/ legal/ regulatory reasons for records retention
- Definitions
- Responsibilities/Procedures
- Consequences if the policy is not followed
- Effective date

For a sample email retention policy, please see Appendix A.

Phase 5: Implementation and Flexibility

An email retention policy is only as good as its implementation. A policy needs to be rigorously enforced from top management down. Companies must make sure they educate their employees about not only the policy, but also the implications of not following it. The policy must be easy to follow, periodically reviewed and regularly audited.

The policy should also address the fact that employees may store and save information in different ways (e.g., save email to a PST) and on different hardware (e.g., some emails may get saved on BlackBerry devices). In addition, the policy must be flexible enough to be suspended if a litigation hold is necessary. The policy should also address the litigation hold process and how it is implemented, including any policy on email backup tapes.

By leveraging The Email Laundry's hosted archiving solutions, you can rest assured that all of your email is automatically being preserved in a secure, centralised repository. In other words, our service does not rely on your end users for preservation. You can further rely on The Email Laundry to follow your designated deletion policies, so the archive reflects your written policies. Finally, with The Email Laundry's legal hold functionality, you can easily comply with any email preservation request.

A Closing Note

Companies must walk a narrow course between the expensive and risky extremes of email management. An email retention policy should not just be a piece of paper. It should define a comprehensive process that includes the following steps:

Implement an email archiving solution to capture and store all emails and attachments

Develop a simple and enforceable email retention policy

Communicate your retention policy (and the rationale for your policy) to all stakeholders

Provide full-text search capabilities for reviewers and legal stakeholders

Preserve regulated data on non-rewritable, non-erasable formats (an important provision of the SEC regulations)

Automatically verify the quality, completeness and accuracy of the archiving, retention and deletion processes

As technology continues to change, so will the law. Consequently, organisations must be vigilant to ensure that retention policies conform to the rule of law, are clearly communicated to end users and are supported by an email archiving solution.

Appendix A: Sample Email Retention Policy

1.0 Purpose

The Email Retention Policy is intended to help employees and email administrators determine what information sent or received by email should be retained and for how long. (Note: This policy needs to be modified based on your specific retention requirements.)

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via email and instant messaging technologies. All employees should familiarise themselves with the email retention topic areas that follow this introduction. Important Note: All emails and attachments are automatically retained indefinitely by The Email Laundry unless advised otherwise by the client. Authorised administrators can apply tags to specify retention periods.

Using The Email Laundry Tags:

Authorised reviewers/administrators can create and save customised email searches based on your organisation's email policies, and rerun them as necessary. Approved
reviewers can efficiently navigate through the search results and tag potentially relevant emails,
so they can be deleted from the archive. Reviewers can also setup Policy Alerts based on retention tags to notify them when an email meets Saved Search criteria (e.g., contains retention dates).

Questions about the proper classification of a specific piece of information should be addressed with your manager.

2.0 Scope

This email retention policy is secondary to <Company Name> policy on Freedom of Information and Business Recordkeeping. Any email that contains information in the scope of the Business Recordkeeping policy should be treated in that manner. All <Company Name> email and instant message information are categorised into four main classifications with retention guidelines:

Administrative Correspondence (4 years)

Fiscal Correspondence (4 years)

General Correspondence (1 year)

"Ephemeral" Correspondence (Retain until read, destroy)

Note: The Email Laundry can selectively archive (or exclude from archiving) individual users email. Users can also self-select which emails they wish to archive if you do not want to archive all messages from all mailboxes.

3.0Policy

3.1*Administrative Correspondence*

<Company Name> Administrative Correspondence includes, but is not limited to, clarification of established company policy, including holidays, time card information, dress code, work place behaviour and any legal issues, such as intellectual property violations. All email with the information sensitivity tag "Management Only" shall be treated as Administrative Correspondence.

3.2 *Fiscal Correspondence*

<Company Name> Fiscal Correspondence is all information related to revenue and expenses for the company. We retain fiscal correspondence for four years, and all emails that fall into this category should be tagged accordingly.

3.3 General Correspondence

<Company Name> General Correspondence covers information that relates to customer interaction and the operational decisions of the business. The individual employee is responsible for email retention of General Correspondence.

3.4 Ephemeral Correspondence

<Company Name> Ephemeral Correspondence is by far the largest category and includes personal email, requests for recommendations or review, email related to product development, updates and status reports. These emails can be deleted from the desktop/laptop PC, but they will be retained in the archive for one year.

3.5 Instant Messenger Correspondence

<Company Name> Instant Messenger General Correspondence may be saved with the logging function of Instant Messenger or copied into a file and saved. Instant Messenger conversations that are Administrative or Fiscal in nature should be appropriately tagged within the archive to reflect a longer retention period.

3.6 Encrypted Communications

<Company Name> Encrypted Communications should be stored in a manner consistent with <Company Name> Information Sensitivity Policy, but in general, information should be stored in a decrypted format.

3.7 Recovering Deleted Email Via Backup Media

<Company Name> maintains backup tapes from the email server. Once a quarter, a set of tapes is taken out of the rotation and moved offsite. No effort will be made to remove email from the offsite backup tapes. Note: All email communications sent and received are also automatically captured in The Email Laundry's hosted email archives.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Terms and Definitions

Approved Electronic Mail

Approved Electronic Mail refers to all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, [insert corporate supported mail servers here]. If you have a business need to use other mail servers, contact the appropriate support organisation.

Approved Encrypted Email and Files

Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within <Company Name> is done via a license. Please contact the appropriate support organisation if you require a license.

Approved Instant Messenger

The [Insert your approved IM client here] IM Client is the only IM that is approved for use on <Company Name> computers.

Individual Access Controls

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command (use man chmod to find out more about it). On Macs and PCs, this includes using passwords on screensavers, such as Disklock.

Insecure Internet Links

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of <Company Name>.

Encryption

Secure <Company Name> sensitive information in accordance with the Acceptable Encryption Policy. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

6.0 Revision History

Use this section to record a log of all changes made to this document so there is written history of the changes made and when they were made.

Appendix B: Important E-Discovery Lessons to Learn

Source: The Concise Guide to E-Discovery, Osterman Research (June 2010)

There are a large and growing number of cases and decisions that are relevant to consider in the context of e-discovery that highlight some of the common e-discovery mistakes to avoid, including the following:

US Cases

You can win a lawsuit and still lose on e-discovery issues

Keithley v. Homestore, Inc.

Kevin Keithley v. The Home Store.com, Inc., 2008 U.S. Dist. LEXIS 61741 (August 12, 2008) Keithley won on summary judgment, but still had to pay $283,000 in fees for failing to preserve and produce required electronic evidence.

Using a work computer can eliminate privilege

Alamar Ranch v. City of Boise

Alamar Ranch, LLC v. City of Boise, 2009 WL 3669741 (D. Idaho Nov. 2, 2009)
This case held that emails sent by a non-party to a lawyer are not protected by attorney-client privilege if a company policy exists stating that emails sent using company facilities are subject to monitoring.

If you withhold emails, the sanctions can be significant

Qualcomm, Inc. v. Broadcom Corporation

No. 05-CV-1958-B (BLM), 2007 WL 2296441 (S.D. Cal. August 6, 2007)
Although Qualcomm initially prevailed in this case, it was discovered after the ruling that thousands of emails were withheld during the case; the Court subsequently awarded $8.5 million in attorney's fees and costs against Qualcomm.

If all you have is backup tapes, you might still be required to produce data

Disability Rights Council of Greater Washington v. Washington Metropolitan Area Transit Authority

2007 U.S. Dist. LEXIS 39605
Production of email from backup tapes was ordered by the Court at the expense of the producing party. The Court also noted that the Safe Harbor provisions of Rule 37(e) do not apply if data destruction is not suspended after a litigation hold.

Omnicare, Inc. v. Mariner Health Care Mgmt. Co.

2009 WL 1515609
The court ruled in this case that just because "ESI is now contained on backup tapes instead of in active stores does not necessarily render it not reasonably accessible."

You might need to produce metadata in addition to electronic documents

Ryan v. Gifford

Civ. No. 2213-CC, 2007 WL 4259557 (Del. Ch., Nov. 30, 2007)

The Court ordered "the production of documents identified in plaintiffs' ... motion to compel in a format that will permit review of metadata, as plaintiffs have clearly shown a particularised need for the native format of electronic documents with original metadata."

Your employees' home computers might be subject to e-discovery

Orrell v. Motorcarparts of America, Inc.

2007 WL 4287750 (W.D.N.C. Dec. 5, 2007)

The court ordered the production of a plaintiff's home computer for forensic examination.

You might have to produce data, no matter how difficult it is or how much it costs

Auto Club Family Insurance Co. v. Ahner

2007 WL 2480322 (E.D. La. August 29, 2007)

"Like other courts that have addressed this issue, this court will not automatically assume that an undue burden or expense may arise simply because electronic evidence is involved." FRCP Rules 34 and 45 "were amended ... to provide for routine discovery of electronically stored information from parties and non- parties. In fact, whether production of documents is unduly burdensome or expensive turns primarily on whether it is kept in an accessible or inaccessible format (a distinction that corresponds closely to the expense of production). But in the world of electronic data, thanks to search engines, any data that is retained in a machine readable format is typically accessible." [Emphasis added]

Don't intentionally delete data that might be discoverable

Ameriwood Ind., Inc. v. Lieberman

2007 WL 5110313 (E.D. Mo. July 3, 2007)

The defendants in this case deleted electronic content and used disk-scrubbing software on a number of hard drives a short time before they were to be provided to a forensic expert in a case involving misappropriation of trade secrets. The court entered a judgment for the plaintiff and ordered the defendant to pay the plaintiff's attorney fees and other costs.

Micron Technology, Inc. v. Rambus, Inc.

C.A. No. 00-792-SLR (January 9, 2009)

Rambus' "aggressive" document deletion policy destroyed documents that the court ruled it had a duty to preserve, resulting in the court's sanction that certain patents were not enforceable against Micron.

UK Cases

Al Sweady v the Secretary of State for Defence4

The defendant denied having further disclosable documents, but then realised that it had more documents than it could deal with; it was ordered to pay costs of £1 million, had to concede the claim, and was severely criticised.

Shoesmith v Haringey, OFSTED and the Secretary of State for Education

Civ. No. 2213-CC, 2007 WL 4259557 (Del. Ch., Nov. 30, 2007)

Office of Fair Trading against BA and Virgin

OFT gained access to a corrupted file in mid-trial; they were unable to comply with the court's deadline for disclosure of the file's contents, and withdrew the prosecution.

Irish Cases

Dome Telecom, Ltd. v. Eircom, Ltd. (2007) IESC 59

The Supreme Court held that in the future and depending on the circumstances, "[i]t may ... be necessary to direct a party to create documents even if such documents do not exist at the time the order is made". This analysis comports with prior Irish and also UK treatment of ESI and the creation of reports on that data in certain circumstances.

About The Email Laundry

Established in 2007 as a email security technology provider to the IT sector The Email Laundry quickly became the standard bearer for accurate spam and virus filtering. The company currently holds seven Virus Bulletin awards for accuracy of its service, having come first worldwide in its reputation based filtering in six of the tests.

The company expanded its services to include an archiving and e-discovery service for email in 2009. This was then tied together with an email continuity service providing their customers with a very high end resilient service. The service became very popular in the London based Financial services sector where the rules for email retention and discoverability are very clear. The Email Laundry service provided IT companies the means to make their customers compliant with FSA regulations.

In 2010 the security as a service package was completed with the establishment of a web security service.

In 2011 the company was shortlisted for the ICT excellence award for world class innovation.

The Email Laundry has over 3500 companies using its services .

More information is available at www.TheEmailLaundry.com