imerge
CONSULTING

A Management Primer

Presented by

MessageSolution™
Customer Driven, Trusted Partner.

 © 2007 Robert F. Smallwood Copyrighted material

imerge
CONSULTING

About IMERGE Consulting

IMERGE Consulting is North America's largest and most experienced team of experts in the fields of enterprise content management (ECM) and business process optimization. We are also a leading provider of tactical education courses in records management, electronic document capture and legal compliance. IMERGE has offices in major cities including Boston, San Francisco, Toronto, Chicago, Houston, Los Angeles, Minneapolis, Seattle, New Orleans and Washington, DC.

What IMERGE has achieved

Our track record speaks for itself: We have completed more successful projects, published more articles and given more expert presentations than any other enterprise content management consulting firm in the world. We are proud that our clients include some of the world's best and largest public and private organizations. Learn more about us at imergeconsult.com today.

About the Author

Robert Smallwood, MBA, Master of Information Technology, Laureate of Information Technology is a founding Partner of IMERGE Consulting and has built outstanding international credentials in his 25 years in the Information Technology industry. He has been recognized as one of the industry's "25 Most Influential People" and "Top 3 Independent Consultants" by *KM World* magazine. Some of his past clients include Bank of America, AT&T, Xerox and IBM. He has published more than 100 articles and given more than 50 conference presentations on document and content management, specializing in email management expertise.

About MessageSolution

MessageSolution is the leading innovator of email and file archiving, compliance, electronic discovery, and data storage management solutions that help enterprises and organizations to streamline business processes, mitigate risk, and reduce costs.

 © 2007 Robert F. Smallwood Copyrighted material

Table of Contents

 © 2007 Robert F. Smallwood Copyrighted material

Table of Contents – continued

The Foundation: Policy Formation – continued

 © 2007 Robert F. Smallwood Copyrighted material

Executive Overview

The purpose of this Management Primer is to give managers charged with formulating email policies, procedures and technology strategies an overall framework for accomplishing their objectives. Although policies, once formed, can serve as useful constructs for a time, they must continuously be tuned to keep in step with regulatory demands, governance policies and technological advances.

Email management (EMM) technologies change almost daily and keeping up with the new technology releases, mergers & acquisitions and other dynamics of the EMM marketplace can be overwhelming. So this publication's critical goal is to provide lasting expert advice that will serve the manager well even as those technologies and markets evolve. The approach presented is practical; one that attempts to explain in plain language the challenges and details of email policy, management strategies and technologies with real-world examples of decisions, policies and technologies that have been time-tested. This will include, where possible, Best Practices and examples from a variety of business sectors.

Email has become the business communication mode of choice. It saves time and reduces costs. But it has become so ubiquitous and voluminous that knowledge workers are virtually drowning in the deluge they receive daily. Managing messages and attachments, and the potentially damaging content they contain, has become a serious challenge for organizations. In addition to the fantastic business benefits of email, it has become an overwhelming task to manage. Things stated in the heat of battle have come back to bite managers in compliance, governance and litigation proceedings. No one is immune: Executives in business, the media and government have been heavily fined and even jailed for what

they've written in email messages. So it is critical to enforce governance policies and adhere to compliance requirements as close to the point of origin *before* they become damaging and lead to costly litigation or government investigations.

Policies must be formed and new technologies must be deployed to manage email content *before* it enters or leaves an organization and renders it out of compliance with regulations or governance policies.

This Management Primer will not only provide a blueprint and samples of successful e-policies and electronic records management practices, but also a framework for evaluating and implementing technologies, even though they are ever-changing. This publication will help protect an organization from the potentially disastrous effects of improper email communications and the risks of email in today's business environment.

 © 2007 Robert F. Smallwood Copyrighted material

Email: The Most Critical Enterprise Application Today

When computers first came into business use decades ago, the first application to be automated was accounting. About 20 years ago, the first application to have electronic document management capability was accounts payable invoice verification and reconciliation within accounting systems. With the emergence of databases, focus on database applications fueled the rapid growth of companies such as Oracle Corporation (oracle.com) in the 1980s and 1990s. But today, databases are no longer the most critical applications in business.

In a recent survey by IMERGE Consulting, more than 60% of information technology (IT) and business professionals named email as the most critical enterprise application, well above the next choice, database transaction processing (36%).

The technical challenges are significant. Imagine this: large electronic document management systems may handle a few million documents, perhaps even tens of millions. But archiving all email for seven years for an organization of 25,000 employees adds up to over 4.5 *billion* documents. And email management software installations may have as many a 600,000 users, so scalability is key.

 © 2007 Robert F. Smallwood Copyrighted material

Email Archiving or Email Management?

The EMM software marketplace initially was dominated by software and hardware vendors that focused on storage management solutions. The management of email messages began with storage on the back-end in farms of magnetic disk drives, optical disc jukeboxes or racks of CD drives (following the conclusion of the communications). As volumes grew, new methods and software approaches for compressing and more efficiently moving the messages to optimal storage media, (based strictly on their age), came about. Hierarchical storage management (HSM) is a method for moving messages from magnetic disk to more permanent forms of media such as write-once-read-many (WORM) optical disc, CD/DVD or unalterable magnetic tape that mimics WORM.

As court cases were increasingly influenced by the "smoking gun" of email messages, and as government regulators tightened the noose with regulations such as Sarbanes-Oxley and Health Insurance Portability and Accountability Act (HIPAA), software entering the marketplace began to focus more on the actual *content* within those messages, rather than on basic storage efficiency. Companies began to focus their efforts on the content of messages, while retaining the native format. Content addressable storage (CAS) emerged to store email to the most appropriate media based on content, not date of creation or archiving. It is also a mechanism for retrieving information based on its content, not its storage location. It is typically used for faster retrieval of fixed content, such as documents stored for compliance with government regulations.

Regulatory requirements dictate that email messages and their attachments be preserved for significant periods of time, usually five to seven years. Email archiving capabilities not only save these electronic messages, but also provide the ability to search and retrieve messages and attachments

 © 2007 Robert F. Smallwood Copyrighted material

based on their content. Search capabilities range from very basic searches for key words to searching for phrases and even words and phrases that use synonyms by employing a built-in thesaurus capability. Specialized fields such as medicine, chemistry and law often require that industry-specific definitions are recognized by using a dictionary and thesaurus of vertical market-specific terms.

In addition to basic search and retrieval capabilities, these functions within email archiving software help organizations comply with broad regulatory demands by: 1) preserving the original message format on a storage medium that is unalterable; and, 2) calculating the proper length of time for saving different types of messages, based on their date of creation, department or user and often the content within the messages

Archiving email messages and attachments, Instant Messages (IMs) and collaborative communications (also known as groupware) simply preserves these e-communications, but does not, by itself, aid in the enforcement of corporate governance policies or federal regulations. That is where more sophisticated email management, which *can* stop wrongful e-communications from entering, exiting or being circulated through the organization, comes in to play.

Most everyone is familiar with spam filters that stop unwanted email from entering the organization. But email management software can actually monitor and quarantine suspect messages for review before they leave the organization and possibly cause a violation in governance or regulatory requirements. This active monitoring of outbound email is a growing trend and is called Outbound Content Compliance (OCC).

Using OCC capabilities, firms set up their list of watch words, phrases and recipients to ensure that nothing leaves the bounds of the organization that could potentially cause a violation. These watchwords and definitions are not only industry-specific, but also they must be customized to be organization specific, based on established corporate governance policies.

Email management software has many more capabilities, but the key difference between email archiving and email management is that there is a much greater focus on the *content* within messages in the latter, and there are greater proactive capabilities built in to foster compliance efforts.

A Growing Problem: Managing the Email Chaos

EMAIL AND INSTANT MESSAGING VOLUMES AND PROJECTIONS

Email has become our primary mode of business communication today. It has largely replaced faxes, written communications and even telephone calls. And the volume is overwhelming.

It is obvious to those in business and government that email and Instant Messaging volumes are large and continue to grow each year. The average business user receives more than 100 messages a day. You can leave for a meeting and return to find you have another 15-20 messages in your mailbox and each one requires some sort of action on your part.

Research bears this out. According to The Radicati Group of Palo Alto, California, corporate users are increasingly becoming inundated with email and IMs. In 2004, corporate users exchanged approximately 64 billion email messages daily and this is expected to *nearly double* by 2008, to a projected 103 billion messages.

Growing at an even faster rate, perhaps reflecting the increasing velocity and decreased cycle times of business decisions and transactions, is the growth of Instant Messaging. Daily IMs are projected to be exchanged at a compound annual growth rate of 43%, from 10 billion

messages in 2004, to 43 billion messages per day in 2008. Is there no end in sight?

Perhaps not. And legitimate messages are not the only factor straining corporate email systems.

Email volumes on the Internet as a whole have historically risen each month since email has come into use. According to research by EMM specialist Email Systems, Inc. (emailsystems.com), since mid-2006 the trend line has worsened considerably, growing at a rate of 25 percent to 35 percent monthly. The volume of mail swirling around the Internet will continue to explode unless spam growth slows. But that's not likely, since spammers continue to innovate with new tactics.

Many corporate email systems are now coming under tremendous stress, according to Neil Hammerton, the CEO of Email Systems. "Winter 2005-06 was a frenzied period for spam and viruses, with viruses in particular accounting for more than half of all email traffic sent," he said. "If that trend continues, then the quantity of viruses distributed will be many times more than has ever been seen previously, simply due to the escalation in volume."

Framingham, Massachusetts-based research firm IDC estimated that nearly 84 billion email messages, more than 33 billion of which were spam messages, were sent worldwide on a daily basis in 2006.

Demonstrating the ubiquity of email, business-to-business email overtook direct mail pieces worldwide for the first time in 2006, according to several sources.

FAILURE TO MANAGE EMAIL: CONSEQUENCES AND IMPACT

We shoot email messages out in the heat of the business battle. Email is quick, less formal than communications on paper and hence is used as a truer indicator of motives and opinions by attorneys and regulators. No one is immune: Bill Gates' emails cost Microsoft dearly in anti-trust litigation; the real opinion of stocks that Merrill Lynch analysts were (unduly) promoting was revealed by email; and the shredding of documents at audit firm Arthur Andersen was uncovered by digging into archived email. All led to financial penalties, and often criminal penalties applied.

In response, new e-discovery amendments to the Federal Rules of Civil Procedure (FRCP) went into effect in December 2006. These new rules dictate the discovery process for electronically stored information.

The spur-of-the-moment character of email can cause otherwise prudent people to let their guards down and to communicate thoughts they would never put in writing. Do not be lured into the idea that deleting email messages really does get rid of them permanently. All this does is rename the file and allow it to be overwritten in the future. But computer forensic experts have little difficulty in recovering the messages. In fact, "UNDELETE," a simple DOS command, will bring back messages deleted at the desktop. Employees may find themselves explaining under oath that a message was deleted or "spoiled." So the suspect email messages may well be examined much more closely than all the rest of the materials and content under review in the litigation process.

So the key rule to bear in mind *is do not put anything into an email message that you wouldn't put in a typed letter that may be reviewed later during litigation or compliance hearings.*

 © 2007 Robert F. Smallwood Copyrighted material

WHERE EMAIL FITS IN ENTERPRISE CONTENT MANAGEMENT (ECM)

Email is but one piece of the total enterprise content management pie. ECM includes all an organization's electronic content. This includes content on Web sites and intranets, digital images of scanned paper documents, electronic documents such as e-forms, word processing files, spreadsheets, presentation files (PowerPoint), desktop publishing files, electronic reports and any other electronic file types. The goal of ECM software is to provide a single point of management of all these file types, regardless of their location or rendition. Renditions are created when the same content appears in different formats, such as a Microsoft Word document and a Portable Document Format (PDF) of the exact same content.

ECM is important to keep content up-to-date and various renditions synchronized. When a change is made to the content of an electronic document or report, it will be reflected accurately throughout the organization, regardless of its format or rendition. This assists in compliance efforts and ensures employees are using the most up-to-date information.

ARE ALL EMAILS A RECORD?

This has been argued for years. *The short answer is "No," not all email messages constitute a record.* But how do you determine whether certain messages are a business record or not? The general answer is that a record documents a transaction or business-related event that may have legal ramifications or historic value. Most important are business activities that may relate to compliance requirements or those that could possibly come into dispute in litigation. Particular consideration should be given to financial transactions of any type.

Certainly evidence that you have completed required governance oversight or compliance activities needs to be documented and becomes a business record. Also, business transactions, where there is an exchange of money or the equivalent in goods or services, are also business records. Today, these transactions are often documented by a quick email. And, of course, any contracts, (and any progressively developed or edited versions) that are exchanged through email become business records.

The form or format of a potential record is irrelevant in determining whether it should be classified as a business record. For instance, if a meeting of the board of directors is recorded by a digital video recorder and saved to DVD, it constitutes a record. If photographs are taken of a ground-breaking ceremony for a new manufacturing plant, the photos are records too. If the company's founders tape-recorded a message to future generations of management on reel-to-reel tape, it is a record also, since it has historical value. But most records are going to be in the form of paper, microfilm or an electronic document.

Some basic guidelines for determining whether an email message should be considered a business record are:

1. The email documents a transaction or the progress toward an ultimate transaction where anything of value is exchanged between two or more parties. All parts or characteristics of the transaction, including who (the parties to it), what, when, how much and the composition of its components are parts of the transaction. Often seemingly minor parts of a transaction are found buried within an email message with the pace of today's business environment. One example would be a last-minute discount offered by a supplier based on an order being placed or delivery being made within a specified timeframe.

2. The email documents or provides support of a business activity occurring that pertains to internal corporate governance policies or

compliance to externally mandated regulations.

3. The email message documents other business activities that may possibly be disputed in the future, whether it ultimately involves litigation or not (that is to say, most business disputes are actually resolved without litigation, provided proof of your organization's position can be shown). For instance, your supplier may dispute the discount you take that was offered in an email message and, once you forward the email thread to them, they acquiesce.

REAL-WORLD GOVERNANCE, COMPLIANCE AND LEGAL ISSUES

Corporate governance is the formal structure and the interrelationships defined by policies and processes that dictate the way a corporation is directed and controlled. Governance has become increasingly important during the last decade, seen as a necessary mechanism to protect companies from fraud and non-compliance. The board of directors is fundamentally responsible for creating and enforcing corporate governance, although committees typically carry out research and make recommendations to the board. Governance also includes the way that stakeholders (including shareholders, suppliers, creditors, customers, employees, management and the board of directors) interact in pursuit of the firm's goals. The corporate governance structure is affected by the corporate culture, management history, legal, regulatory and ethical environment of the business.

Corporate governance enforces and monitors compliance, accountability and fiduciary duty through guidelines and controls to protect shareholders. This most formally takes place through the creation of, amendment to and passage of corporate by-laws. In non-profits, governance protects members, the community served and/or customers.

Lack of proper governance polices and oversight has brought down major American corporations and forced them to go out of business or to radically restructure for a potential acquiring firm. Major business debacles such as WorldCom, Tyco, Adelphia and Enron were caused, in large part, by a lack of enforcement of prudent governance policies. These business failures were the impetus behind the creation and passage of the Sarbanes-Oxley Act (often called SOX), also known as the Public Company Accounting Reform and Investor Protection Act of 2002, which, among other things, requires the CEO of a publicly-traded company to sign off on or "certify" that financial reports are accurate. With possible criminal penalties, such officers are much more motivated to dig into the veracity of financial statements. Some have avoided the risk altogether by resigning their position as CEO and assuming only the less hands-on position of chairman of the board.

When determining governance policies, one size does *not* fit all. No two organizations are alike in their characteristics: goals, culture, history, technological infrastructure or management. Even if two firms are competitors located across the street from each other, their governance policies will vary.

Every established organization has governance policies. In business, they begin at the top with the by-laws adopted by the board of directors. They are further delineated in policy manuals, Standard Operating Procedures and other formal management guidelines. Governance is not a very exciting area and often policies lag behind organizational changes, market pressures and regulatory influence, often remaining out-of-step until a formal governance review is undertaken.

Keeping governance policies current requires that a standing governance committee review and evaluate the effectiveness of policies while considering changes to the internal and external environment of the organization. Typically, a governance committee is made up of various sub-committees that focus on areas such as compliance, audit and legal. An

evaluation of the effectiveness of governance policies should be an ongoing process, and constant adjustments should be considered. Internally, the evolving organization reporting structure is organic and dynamic and governance polices must be monitored and fine-tuned to reflect that. Externally, changes in markets, supplier policies and consumer demands dictate consideration of internal governance changes. Of course, when new federal, state or local regulations go into effect, the resultant impact on the organization and its ability to monitor compliance efforts must be considered and new governance polices put into place.

AMENDMENTS TO FEDERAL RULES OF CIVIL PROCEDURE (2006)

The Federal Rules of Civil Procedure (FRCP) apply to U.S. district courts, which are the trial courts of the federal court system. The district courts have jurisdiction (within limits set by Congress and the Constitution) to hear nearly all categories of federal cases, including civil and criminal matters.[1]

The FRCP procedures were amended in 2006, and some of the revisions apply specifically to the preservation and discovery of electronic records in the litigation process. These procedures went into effect in December, 2006.[2] These changes were a long time coming, reflecting the lag between the state of technology and the courts' ability to catch up to the realities of electronically generated and stored information.

The U.S. district judge has the ultimate authority in courtroom legal procedure, and has a role in advancing common law practice and establishing new positions. When making decisions, the district court judge applies the substantive laws of the

[1] "New Federal Rules to Civil Procedure" www.uscourts.gov/districtcourts.html

[2] Ibid.

state. Federal courts must apply the substantive laws of the states as rules of decision in cases where state law is in question. However, the federal courts usually use the FRCP as their rules of procedure. States make their own rules that apply in their own courts, but most states have adopted rules based on the FRCP.[3]

After years of applying traditional paper discovery rules to electronic discovery, on April 12, 2006, the Supreme Court of the United States approved several proposed amendments to the FRCP to accommodate the modern practice of discovery of electronically stored information. The goal of the amendments is to recognize the importance of electronically stored information and to respond to the increasingly prohibitive costs of document review and protection of privileged documents. These amendments reinforce the importance of procedures governing the handling of electronically stored information for litigants thinking about electronic discovery.[4]

---

[3] "New Federal Rules to Civil Procedure" www.uscourts.gov/districtcourts.html
[4] Ibid.

 © 2007 Robert F. Smallwood Copyrighted material

GUIDELINES FOR FRCP PREPARATION

1. Map out all places where electronic information is stored. Locate any data source including deleted data, data on systems no longer in use, data in remote or third-party locations, copies of production data used in demos, test systems, etc.

2. Update your records retention policy to include all electronic information. Corporate retention policies should be applied to email and other electronic records.

3. Ensure your litigation hold policy fully covers all electronic information including backup tapes. Make sure it includes rules for all relevant electronic records, such as email, electronic documents, scanned documents, storage discs and backup tapes.

4. Establish systems that simplify identification, retrieval and production of potentially relevant data. Purchase software that provides online risk management and Web application security.

5. Establish a plan of action. Evaluate how you can organize your data storage to actively prepare for electronic discovery requests.[5]

[5] AIIM Compliance Solution Center Primer on the FRCP, 2006

E-DISCOVERY

Rules 26 and 34 of the Federal Rules of Civil Procedure specifically cover discovery and disclosure of information that is relevant to civil suits.

Discovery is the part of the litigation process in which opposing parties exchange relevant information and testimony. This process helps both sides understand the facts and evidence before the commencement of a trial.

Electronic discovery (often called e-discovery or ediscovery) refers to "any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case." This includes but is not limited to computer forensics, email archiving, online review and proactive management. The emergent e-discovery field augments legal, constitutional, political, security and personal privacy issues.

FRCP 26(b)(5) deals with General Provisions Governing Discovery; Duty of Disclosure; Discovery Scope and Limits; and Claims of Privilege or Protection of Trial Preparation Materials. FRCP 34(b) focuses on the Production of Documents, Electronically Stored Information, and Things. These amendments to the FRCP address a common corporate problem — the volume of electronically stored information and its maintenance. During an electronic discovery process, all types of data serve as evidence, including text, images, calendar/scheduling files, databases, spreadsheets, audio files, video files, animation, Web sites and computer programs. Because of lax corporate management, email is often the most valuable source of evidence in civil or criminal litigation.

A common, specialized form of e-Discovery is computer forensics (cyber forensics), which is "the application of computer investigation and analysis techniques to gather evidence suitable for presentation in a court of law." Computer forensics executes a structured investigation while maintaining a documented chain

of evidence to discover the contents of the hard drive of a specific computer. After physically isolating the computer, investigators make a digital copy of the hard drive and store the original computer in a secure facility. The cyber forensics team performs all investigation on the digital copy.

Under these amendments, corporations must proactively manage the electronic discovery process to avoid sanctions, unfavorable rulings and a loss of public trust. Corporations must be prepared for early discussions on electronic discovery with all departments. Topics should include the form of production of electronically stored information and the preservation of information. Records Management and IT departments must have made available all relevant electronically stored information for attorney review.[6]

Amendments to the FRCP include, according to the Advisory Committee notes:

[6] AIIM Compliance Solution Center Primer on the FRCP, 2006

• **Rule 16 — Pretrial Conferences; Scheduling; Management:** New subsections 16(b)(5) and 16(b)(6) provide that the scheduling order may address "disclosure or discovery of electronically stored information" and any agreements "for asserting claims of privilege or of protection as trial-preparation material after production."

• **Rule 26 — General Provisions Governing Discovery; Duty of Disclosure:** Subsection 26(a)(1)(B) is amended to substitute "electronically stored information" for "data compilations" as a category of the required initial disclosures. Subsection 26(b)(2)(B) is added to excuse a party from providing discovery of electronically stored information that is "not reasonably accessible because of undue burden or cost," but the burden remains on the producing party to make the required showing. Subsection 26(b)(5)(B) is added, providing a procedure for a party to maintain "a claim of privilege or of protection as trial-preparation material" concerning any discovery, even after it is produced. As the Advisory Committee Notes clarify,

"Rule 26(b) (5) (B) does not address whether the privilege or protection that is asserted after production was waived by the production," but rather it "provides a procedure for addressing these issues." Finally, similar to new Rules 16(b)(5) and 16(b)(6), new subsections 26(f)(3) and 26(f)(4) are added to make sure the Rule 26(f) conference includes a discussion of any issues relating to "disclosure or discovery of electronically stored information," and "claims of privilege or of protection as trial-preparation material." Form 35 (Report of Parties' Planning Meeting) is revised to reflect the changes to Rule 26(f).

• **Rule 33 — Interrogatories to Parties:** Rule 33(d) is amended to specify that electronically stored information may qualify as appropriate business records from which an answer to an interrogatory may be derived or ascertained.

• **Rule 34 — Production of Documents, Electronically Stored Information, and Things:** Rule 34(a) is amended to reference electronically stored information, and Rule 34(b) is amended to supply a procedure for specifying and objecting to the form in which electronic information is to be produced. Under new subsections 34(b)(ii) and 34(b)(iii), the default form for producing electronically stored information is that "in which it is ordinarily maintained [or] reasonably usable," and "a party need not produce the same electronically stored information in more than one form."

• **Rule 37 — Failure to Make Disclosure or Cooperate in Discovery; Sanctions:** New subsection 37(f) is added and states, "Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of routine, good-faith operation of an electronic information system." The Advisory Committee Notes explain that the premise for this amendment is that ordinary computer use necessarily involves routine alteration and deletion of information for reasons unrelated to litigation.

• **Rule 45** — Subpoena: Rule 45 is amended to incorporate the changes to Rule 26(b) and Rule 34 as applied to the production of documents by third parties pursuant to a subpoena.

• **Proposed Rule of Evidence 502 — Attorney-Client Privilege and Work Product: Waiver By Disclosure:** The Advisory Committee on Evidence Rules has proposed a new Rule 502 that would formalize a "subject matter" waiver of the attorney-client or work product privileges through voluntary disclosure, with an important exception for "inadvertent" disclosure. Specifically, upon a voluntary disclosure of privileged or work product information, Rule 502(a) would further require production of "undisclosed information concerning the same subject matter if that undisclosed information ought in fairness to be considered with the disclosed information." Rule 502(b), however, would provide an exception where "the disclosure is inadvertent… and if the holder of the privilege or work product protection took reasonable precautions to prevent disclosure and took reasonably prompt measures, once the holder knew or should have known of the disclosure, to rectify the error, including (if applicable) following the procedures in Fed. R. Civ. P. 26 (b)(5)(B)." The Committee Notes explain that the new Rule 502 would resolve disputes over the effect of inadvertent disclosure and selective waiver of privileged or work product information, and responds to the prohibitive litigation cost of reviewing and protecting privileged or work product material, particularly in cases involving electronic discovery.

• **Local E-Discovery Rules:** Several local jurisdictions have already amended their court rules to reflect the importance of discovery of electronic data. A summary of the applicable local rules can be provided upon request.

• **Citation of Unpublished Opinions:** The Supreme Court also approved a new Federal Rule of Appellate Procedure 32.1, which will allow litigants to cite any "federal judicial opinion, order, judgment, or other written disposition" issued on or after January 1, 2007, even if it has

been given an "unpublished" or similar designation. The effect of the new rule, as stated in the Committee Note, is that "a court of appeals may not prohibit a party from citing an unpublished opinion of a federal court for its persuasive value or for any other reason."[7]

[7] AIIM Compliance Solution Center Primer on the FRCP, 2006

 © 2007 Robert F. Smallwood Copyrighted material

JUST WHAT IS "LITIGATION READINESS?"

Litigation readiness is just that: being ready for litigation. Being ready means that regardless of the specific issues in a lawsuit, *your organization has taken steps to minimize preparation and research time, and therefore has more time to consult and develop strategies for a defense.*

If your firm does few things differently in terms of technological infrastructure and information management than it did five years ago, it is most certainly not as well-prepared to go into battle as it could be.

Having information at hand, and the ability to search, filter and sift through it quickly will give your company an advantage over the opposing counsel's team. If they are still pouring through boxes of paper documents with an army of paralegals while your team is mining and analyzing electronic data for the little details that can make a difference in a case, then you have an advantage and are more "litigation ready."

Implementing up-to-date governance policies and harvesting information from a state-of-the-art email management system will give your company a decided advantage in the litigation process. This is true not only with initial salvos, but also as the discovery and litigation process progresses. You can simply be more efficient and cost-effective while the opposition flounders with manually attempting to determine patterns and find that "smoking gun."

BEST PRACTICE CONSIDERATIONS

Best Practice is a management idea which asserts that there is a technique, method, process, activity, incentive or reward that is more effective at delivering a particular outcome than any other technique, method, process, etc. The idea is that

with proper processes, checks and testing, a project can be rolled out and completed with fewer problems and unforeseen complications.

Best Practices do not have one template or form for every organization to follow. In the context of business management, Best Practice is the concept that a good process and planning are being followed in the Execution Management of a project plan, and that changes to the initial plan, contingencies, and goals are being tracked and documented.

The notion of Best Practices does not commit people or companies to one inflexible, unchanging practice. Instead, *Best Practices is a philosophical approach based around continuous learning* and continual improvement.[8]

The American Productivity and Quality Centre (APQC) states: "Three themes resonate through successful benchmarking and best-practice transfer efforts:

1. Transfer is a people-to-people process; meaningful relationships precede sharing and transfer.

2. Learning and transfer is an interactive, ongoing, and dynamic process that cannot rest on a static body of knowledge. Employees are inventing, improvising, and learning something new every day.

3. Benchmarking stems from a personal and organizational willingness to learn. A vibrant sense of curiosity and a deep respect and desire for learning are the keys to success."[9]

Although several texts have been published on e-policy, Best Practices in email management are new and evolving. They arise from the study of methods that have proved to be the most effective across an industry or in deploying technology sets. In the rapidly changing field of email management, some practices have been employed with success, but they cannot be firmly and convincingly called Best Practices.

[8] http://en.wikipedia.org/wiki/Best_practice

[9] www.apqc.org/portal/apqc/site

So, you must undertake your own study of Best Practices to determine the lowest risk course of action for implementing email management.

How do you undertake a study to determine developing Best Practices for implementing, monitoring and controlling your email management system? There are several steps you can take to gather current empirical information about what works and what does not.

Here are some suggestions:

1. Make a list of probing questions for the vendors' implementation teams: What has worked at other organizations? Are there certain caveats you have learned from experience? Do these observations hold true across industries? What about the vertical market we are in?

2. Ask the vendors for reference sites of companies that currently use the product you are evaluating. Ask the users at these sites the same types of questions you asked the vendors. Be sure to dig deep into these organizations — don't just interview the contact names they give you.

3. Get your project team together and compare notes. Distill the information into specific actions you will take (or avoid) in the selection and implementation process. Keep an eye to these items and continue to refine your approach as the project progresses.

4. After the implementation is complete, review the project at least quarterly in a post-implementation audit. Continue to refine and revise your methods and processes.

Bear in mind, though, that the most relevant information is that which applies to your organization, its technological infrastructure and management approach. Ideas gleaned from surveying vendors and other end-user organizations are just ways to point you in the right direction.

The Foundation: Policy Formation

Before you start off on a search for just the right email management software, you must first define the requirements the software will need to fulfill. This begins with deciding formally to implement, monitor and update e-policy, and then more specifically establishing your own organization's detailed email policy. Most email policies are not updated regularly to reflect changes in the external technological environment and the internal IT infrastructure, management environment and culture of the organization. Email policy will dictate what acceptable content is and how to manage and maintain email messages within the constructs of current technological capabilities, both internal and external.

EMAIL POLICY RATIONALE: WHY DO YOU NEED IT?

Twenty years ago a new hire out of college may have been assigned to read the Policy and Procedures Manual. It was likely a three-ring binder about four inches thick and it covered every aspect of employee conduct, management oversight, paperwork and other daily operations. It was dry and as boring as it could be, but once a recruit was assigned to read it and signed off as having done so, that person could be held accountable at any point for following every sentence in it to the letter. There were no online references, indexes, manuals — or email. So if employees ran into situations where they needed to consult the manual, they had to search the index and thumb through it manually.

But the corporation had no other choice for establishing and communicating policy. Today, these guidelines and Standard Operating Procedures are typically online and a

 © 2007 Robert F. Smallwood Copyrighted material

quick search will answer employee questions. This does not obviate the need to have employee briefings to articulate policy, especially when there are significant changes. But clearly, companies must have standard ways of doing things or management becomes too capricious. Also, it can protect the company in litigation or compliance examinations.

Of course, everything in the policy manuals before the electronic age referred to paper forms and reports. Perhaps surprisingly, though, a large segment of American businesses today have not established thorough e-policies even though they operate primarily in the electronic realm, using accounting and management software, email and automated reports to help run their businesses.

Large institutions, for instance, typically have detailed policies and rules regarding workplace conduct but fail to extend these rules to the creation and transmission of email. Behind that oversight lurks potential long-term damage.[10]

Content rules keep email free of personal opinions, off-color jokes, and inappropriate commentary, which can haunt organizations during litigation, audits, or other formal proceedings. Take the case of the large consulting firm sued by a client for inadequate performance. During the trial, damaging internal email messages undercut the firm's defense. In one message, a consulting firm employee expressed the opinion that one of the consultants in question "should be taking a community college course, not billing for this."[11] Had management established and enforced policy banning personal opinions or commentary critical of the firm and its employees, it is unlikely that damning messages like this ever would have been written.[12]

By having a good email policy in place you can secure your company in several ways. First, the email policy helps prevent email threats, since it makes your staff aware of the corporate rules and guidelines, which,

[10] Nancy Flynn and Randolph Kahn, *Email Rules* (New York: AMACOM, 2003)

[11] Gregory S. Johnson, "A Practitioner's Overview of Digital Discovery," *Gonzaga Law Review* 33, no.2 (1998), 347.

[12] Nancy Flynn and Randolph Kahn, *Email Rules* (New York: AMACOM, 2003)

 © 2007 Robert F. Smallwood Copyrighted material

if followed, will protect your company.[13]

Secondly, an email policy can help stop any misconduct at an early stage by asking employees to come forward as soon as they receive an offensive email. Keeping the incidents to a minimum can help avoid legal liability. For instance in the case of Morgan Stanley, a U.S. investment bank that faced an employee court case, the court ruled that a single email communication (a racist joke, in this case) cannot create a hostile work environment and dismissed the case against them.

If an incident does occur, an email policy can minimize the company's liability for the employee's actions. Previous cases have proven that the existence of an email policy can prove that the company has taken steps to prevent inappropriate use of the email system and therefore can be freed of liability. WorldCom Corporation, for instance, faced a court case from two former employees for allowing four racially offensive jokes on its email system. WorldCom successfully defended itself because it had an email policy that spelled out inappropriate content and because it took prompt remedial action against the coworker who sent the racially harassing email messages.[14]

Finally, if you are going to use email filtering software to check the contents of your employees' email, it is essential to have an email policy that states the possibility of email monitoring. If you do not have such a policy, you could be liable for privacy infringement.[15]

[13] www.email-policy.com

[14] Ibid.
[15] Ibid.

BEFORE YOU CREATE YOUR EMAIL POLICY

Before you start creating an email policy, do some investigation into already existing company policies, such as guidelines on writing business letters, access to confidential information, personal use of the telephone systems and sexual or racial harassment at work. It is important that your email policy is compatible with your company's existing policies. You will also need to decide whether your company is going to allow personal use of the email system, and if so, to what extent. It may be unrealistic and even imprudent to completely forbid personal use, since it often saves time for employees when they have personal issues to deal with such as sick children, doctor appointments and the like.

The email policy should be drafted with the help of human resources, IT and the board of directors in order to reflect all viewpoints in the organization. It is also advisable to have several employees look at the policy and provide feedback. Make sure that your policy is not so restrictive that it will compromise your employees' morale and productivity.[16]

[16] www.emailreplies.com, 2006

 © 2007 Robert F. Smallwood Copyrighted material

WHAT SHOULD BE INCLUDED IN AN EMAIL POLICY?

For the policy to be effective the document should use clear and simple wording and not be longer than three or four pages. You cannot expect employees to read and follow a long complicated document, since you want them to remember and abide by what it says. List short bullet points, so that an employee can easily find rules in case they are unsure.[17]

Commercial: Guidelines on how to write effective email messages

- Corporate email style (formal/informal) guidelines, including guidelines on salutations and ending of messages.
- What kind of signatures should be used? (Should signatures include company name, job function, telephone and fax number, address, Web site, logo and a corporate slogan?).
- Basic rules on how to write email (see email etiquette).
- Expected time in which email messages should be answered. For example, you could set a general rule that each email message should be answered within at least eight working hours, but perhaps 50 percent of email should be answered within four working hours.
- How to determine which email messages should receive priority.
- When to send cc: or bcc: messages and what to do when you receive them.
- How and when to forward email messages and how you should handle forwarded messages.

Productivity: Rules on the usage of the email system could include:

- Whether personal email messages are accepted and if so, to what extent. For instance you could limit the amount of personal email sent each day, or you could require that personal email messages be saved in a separate folder. You could also limit or eliminate certain email

[17] www.emailreplies.com, 2006

attachments from being sent or received, and include rules on sending chain letters. Include examples and clear measures taken when these rules are breached.

- Rules about use of newsletters and news groups. For instance, you can require a permission request to subscribe to a particular work-related newsletter/group.
- A warning that users should not engage in non-business activities that unnecessarily tie up network traffic.

Legal: Prohibit inappropriate email content and warn of risks

- Include a list of "email risks" to make users aware of the potential harmful effects of their actions. Advise users that sending an email is like sending a postcard: If you don't want it posted on the bulletin board, don't send it.
- The policy should expressly state that the email system is not to be used for the creation or distribution of any offensive or disruptive messages, including messages containing offensive comments about race, gender, age, sexual orientation, pornography, religious or political beliefs, national origin or disability. State that employees who receive any email messages with this content should report the matter to their supervisor immediately. Furthermore, mention that employees should not use email to discuss competitors, potential acquisitions or mergers or to give their opinion about another firm. Unlawful messages, such as copyright infringing email messages should also be prohibited. Include examples and clear measures taken when these rules are breached.
- If you are going to monitor the content of your employees' email, you must mention this in your email policy (in most countries/states you are allowed to monitor your employees' email if your employees are made aware of this). Warn that employees should have no

expectation of privacy in anything they create, store, send or receive on the company's computer system and that any of their messages may be viewed without prior notice.

Finally, include a point of contact for questions arising from the email policy.

PUBLISHING THE EMAIL POLICY

When you have formulated an email policy, you should make sure that all employees are aware of it. You can do this by handing out printed copies, publishing it on your intranet and including it in staff handbooks. Also, when a new employee starts at your company, this employee should be given a copy of the document as a standard procedure.[18]

It is a good idea to include the most important points of the email policy in the employment contract, so that employees must sign that they have read, understand and acknowledge receipt of the policy. Cover the most important issues, such as the personal use of email, possible email monitoring, and the prohibition of defamatory, sexual and racist remarks in email messages. Also expressly state that breach of these rules can lead to termination of employment.

Furthermore, you could organize email training sessions to explain the email risks to users and why the email policy is so important. If users understand the potential threats, most of them will understand why the rules need to be set up and will have less difficulty obeying them. A training session will also help you obtain feedback to ensure that the policy is feasible and can actually be put into practice.[19]

[18] www.emailreplies.com, 2006

[19] Ibid.

CAUSES OF EMAIL POLICY FAILURE

Email policy failure can arise from one of two things — failure to establish proper policy or failure to enforce it. Your company can head off the first possible cause by establishing a prudent email policy tailored to your organization, and by communicating that policy to employees and stakeholders clearly and frequently.

Email management, active policy management (APM) and electronic records management (RM) software are tools that can help enforce email policy, which can be monitored by a Chief Compliance Officer or similar functionary.

RECORD-FREE EMAIL

What types of tools can you use to encourage the free flow of ideas in collaborative efforts without compromising your email policies or risking litigation or compliance sanctions?

Stream messaging is an innovation that became commercially viable in the 2006 timeframe. It is similar in resultant impact to digital enterprise rights management (D-ERM) software, which limits the recipients' ability to forward, print or alter data in an email message (or report, spreadsheet, etc.), but goes further by leaving no record on any computer or server.

Stream messaging is a simple, safe, secure electronic communications system ideal for ensuring that sensitive internal information is kept confidential and not publicly released. Stream messaging is not intended to be a replacement for corporate email, but is a complement to it. If you may need an electronic record, email it; if not, use stream messaging.[20]

[20] www.vaporstream.com, 2007

What makes stream messaging unique is its "recordless-ness." Streamed messages cannot be forwarded, edited or saved. You cannot print a copy of a message as you can with email. That's because stream messaging separates the sender's and receiver's names and the date from the body of the message, never allowing them to be seen together. Even if the sender or receiver were to attempt to make a "print screen" copy, these elements are never captured together.[21]

The instant a stream message is sent, it is placed in a temporary storage buffer space. When the recipient logs in to read the message, it is removed from the buffer space. By the time the recipient opens it, the complete stream message no longer exists on the server or any other computer.

This new communications system is Web-based, meaning that no hardware or software purchases are required. It also works with existing email systems and email addresses and is completely immune to spam and viruses. Other solutions (both past and present) have been offered, but these have taken the approach of encrypting email or generating email that disappears after a pre-set time. Neither of these approaches is truly recordless.

Stream messaging is unique because its technology effectively eliminates the ability to print, cut and paste, forward or save a message. It is currently the only electronic communications system that separates the header information — date, name of sender, name of recipient — from the body of the message. This eliminates a traceable record of the communication.

In addition, there is added protection of stream messaging as an indiscriminate Web-based service, meaning that the messages and headers are never hosted on the subscribing companies' networks. This eliminates the risk that employers, competitors or hackers could intercept stream messages, which is a great security benefit for end-users.[22]

[21] www.vaporstream.com, 2007

[22] Ibid.

EMAIL PRIVACY CONSIDERATIONS

Employees have no expectation of email privacy in the workplace, right? They have been informed through established email policy (in more than five out of six organizations) that clearly outlines the employers' right to monitor employee email. After all, employees are being paid to work for the company, which owns the workspace, computers, software and the network, so the company has a perfect right to monitor your communications, right?

Well, yes — mostly.

Even with a well-defined corporate privacy policy stating that all employee communications may be monitored in the workplace, the legality of email monitoring is not as clear cut as one might think.[23]

Laws differ, depending on the state you are operating in. Under California law, for instance, you can't record someone's conversation without telling them. No such law exists in Georgia. Georgia law only requires that *one* of the parties to the conversation consent to the recording to make it legal. Thus, you can record your own conversations, or, if your boss has obtained your consent (they say it's "my way or the highway"), your boss may record your conversation with others. California, on the other hand, requires that everyone on the call consent to the monitoring.[24]

In many states, the same law that prohibits the interception or recording of telephone calls also prohibits the interception or recording of electronic communications without the consent of all parties. So if you send an email message from California to someone in Georgia, and your boss reads it in accordance with your company's policy (but without your consent) is it legal? It must be legal because we all do it, right? How could it be illegal? How could you expect any privacy in an email to a Georgia company? [25]

[23] Mark Rasch, "Email Privacy in the Workplace,"*securityfocus.com,* 7/31/2006

[24] Mark Rasch, "Email Privacy in the Workplace,"*securityfocus.com,* 7/31/2006

[25] Ibid.

Interception of electronic communications is much more complicated than the listening in or recording of telephone calls. The laws typically differentiate between intercepting a communication (and recording it) and accessing it when it is stored. To intercept or record a conversation requires all party consent in those all party consent states. To access it after it has been stored typically does not (although there are still legal protections for stored communications.) In fact, emails are actually almost *never* intercepted. All email is "store and forward" — (unless it is streamed and therefore recordless). While the packets "travel" across the Internet, it's not like a physical pod is traveling down a tube. The "original" packet stays on the server, allowing its doppelgänger to travel to the next point of departure. Indeed, it would be impossible to "read" an email "in transmission" — you have to stop it, and then reassemble it to get it to appear on the screen. [26]

Thus, the principal legal loophole we rely on in allowing us to read email messages with only one-party consent is this legal fiction that the email is already "received" and stored — whether the recipient has ever seen it or not.[27] So these scenarios are all unique and therefore arguable. As a manager, your best bet is to make your email policy as comprehensive as possible and consistently reinforce and review that policy on a regular basis.

There's another exception. Not only do the physical states of transmission and receipt have a bearing on the legality of monitoring, but also the nature of the communications, especially when to a privileged individual, such as an attorney, doctor or psychiatrist. Your e-policy would be strengthened if it prohibits these types of communications from company-owned computers.

In one case, a California resident named Weibin Jiang was arrested for a sexual offense and used his employer's computer to communicate with counsel, retaining these files in a subdirectory called "Attorney."

[26] Mark Rasch, "Email Privacy in the Workplace,"*securityfocus.com,* 7/31/2006

[27] Ibid.

Despite the fact that the computer belonged to the company, and that Mr. Jiang signed an agreement expressly indicating that he had, "no expectation of privacy in any property situated on the Company's premises and/or owned by the Company," the court found that the government could not simply subpoena the attorney-client-privileged records from the employer. So even consent may not be fully effective.[28]

What about an employer's right to read emails as they come in? As they hit the inbound server? This situation isn't clear-cut either. If the email is not subject to the consent of all parties, and one of the parties (either the sender or recipient) lives in a jurisdiction that mandates all-party consent, then this *could* be an unlawful interception under state law. (Federal law requires only one-party consent.) Under the new California case, it may not matter that you are in a state that permits one-party consent. The truth is, we monitor these kinds of communications all the time, and everybody kind of expects this kind of monitoring. We are now at the point where most people would agree with the statement that, "I have no expectation of privacy in the email I use at work." This statement probably applies equally to the contents of work-related email as well as to any personal (Web-based) mail you send using your employer's computers, cell phones, personal digital assistants or networks. Fundamentally, when at work expect NO PRIVACY.[29]

Not so fast. You see, despite this fact, if you probe further you will find that people DO have expectations of privacy in both corporate and personal email used at work — and, these expectations are reasonable. Is it OK for you to read your cubicle mate's email on the screen just because you are curious? Is it OK to forward that email? Can you (or more accurately, may you) read your boss's email? If the opposite of "private" is indeed "public," does this mean all email is "public?" Of course not. We expect that email may be read by anyone we send it to, and anyone they may forward it to. We expect that

[28] Mark Rasch, "Email Privacy in the Workplace,"*securityfocus.com,* 7/31/2006

[29] Ibid.

those higher than us on the corporate pecking order (including the system administrator and his or her denizens) may also read it *for legitimate business purposes*, and not for idle curiosity. Access may be granted for corporate compliance purposes, regulatory purposes, law enforcement purposes or other legitimate purposes. But that does not mean there is NO privacy — just very limited privacy.[30] All these details need to be spelled out in your email policy statement. It's impossible to cover every situation, but do the best you can, and continue to refine and expand the policy periodically.

[30] Mark Rasch, "Email Privacy in the Workplace,"*securityfocus.com,* 7/31/2006

 © 2007 Robert F. Smallwood Copyrighted material

DOMESTIC OR GLOBAL? CONSIDERATIONS FOR MULTINATIONAL CORPORATIONS

What about corporations that operate internationally? This is another layer of complexity you must consider when drafting email privacy policies. *True, under U.S. federal law, management can use written email policy to inform employees that they have no reasonable expectation of privacy when it comes to sending and receiving email. However, a multinational corporation based in the U.S. may not be able to apply this policy to European, Asian or Middle Eastern employees.* The Supreme Court of France, for example, has ruled that monitoring employee email is improper, even with a written policy giving employees notice that management may be reading electronically over their shoulders.[31]

Before implementing domestic privacy policies abroad, have the lawyers responsible for your international facilities review, and as necessary, adjust them to meet the regulatory, legal and cultural needs of each country in which the organization operates.[32]

[31] Nancy Flynn and Randolph Kahn, *Email Rules* (New York: AMACOM, 2003)

[32] Ibid.

 © 2007 Robert F. Smallwood Copyrighted material

HOW DO YOU CREATE AN EMAIL POLICY?

Basically, an email policy should include all the do's and don'ts concerning the company's email system:

Email risks: The policy should list email risks to make users aware of the potential harmful effects of their actions.

Best practices: This should include email etiquette and writing rules in order to uphold the good reputation of the company and to deliver high-quality customer service. Also include instructions on compressing attachments to save bandwidth.

Personal usage: The policy should state whether personal email messages are allowed and if so, to what extent. You can, for instance, set limits on the amount of personal email sent each day, or you could require personal email be saved in a separate folder. You will probably want to prohibit the sending of chain letters and mass mailings and limit or eliminate certain email attachments from being sent or received. In every case, include examples and clear measures taken when these rules are breached.

Wastage of resources: Warn users that they are making use of the company's email system and that they should not engage in non-business activities that unnecessarily tie up network traffic. The policy must also cover the use of newsletters and newsgroups. For instance, you can require a user to request permission before subscribing to a newsletter or newsgroup.

Prohibited content: The policy should expressly state that the email system is not to be used for the creation or distribution of any offensive or disruptive messages, including messages containing offensive comments about race, gender, age, sexual orientation, pornography, religious or political beliefs, national origin or disability. State that employees who receive any email messages with this content should report the matter to their

supervisors immediately. Moreover, employees should not use email to discuss competitors, potential acquisitions or mergers or to give their opinion about another firm or co-worker. Unlawful messages, such as copyright infringing email messages, should also be prohibited. Include examples and clear measures taken when these rules are breached.

Document retention policy: Your organization is required to archive email messages for some specified period of time, particularly in the case of government, health care and financial institutions. It is best to create a policy rule that dictates deletion of email after a certain amount of days to limit liability and storage requirements. Make sure, though, you are on firm legal ground. It is also a good idea to provide an option to save certain emails in a different folder to avoid deletion. If you provide this option, spell out which emails may be saved and which must be deleted.

Treatment of confidential data: Include rules and guidelines on how employees should deal with confidential information and trade secrets. Make employees encrypt any confidential information that is sent via email and change passwords regularly. Also include measures that will be taken if an employee is found to be sending out confidential information unlawfully.

Email disclaimer: If you are adding a disclaimer to employees' email, you should inform them of this and state the disclaimer text that is added.

Email monitoring: If you are going to monitor your employees' email, you must state this in your email policy. Warn that employees should have no expectation of privacy in anything they create, store, send or receive on the company's computer system and that the company may, but is not obliged to monitor messages without prior notice. If you do not mention that the company is not obliged to monitor messages, an employee could potentially sue the company for failing to block a particular message.[33]

[33] www.email-policy.com

SAMPLE EMAIL POLICY

Below is a sample email policy. DO NOT use this as is, but rather use it as a starting point and add to/edit as needed to customize your policy for your organization's needs and business scenario. And don't stop there, continue to review and refine it on an ongoing basis.[34]

"The purpose of this policy is to ensure the proper use of [Your Company]'s email system and make users aware of what [Your Company] deems as acceptable and unacceptable use of its email system. The [Your Company] reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

LEGAL RISKS

Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply. Therefore, it is important that users are aware of the legal risks of email:

- If you send email messages with any libelous, defamatory, offensive, racist or obscene remarks, you and [Company] can be held liable.
- If you forward email messages with any libelous, defamatory, offensive, racist or obscene remarks, you and [Company] can be held liable.
- If you unlawfully forward confidential information, you and [Company] can be held liable.
- If you unlawfully forward or copy messages without permission, you and [Company] can be held liable for copyright infringement.
- If you send an attachment that contains a virus, you and [Company] can be held liable.
- By following the guidelines in this policy, the email user can minimize the legal risks involved in the use of email. If any user disregards the rules

[34] www.email-policy.com/

set out in this Email Policy, the user will be fully liable and [Company] will disassociate itself from the user as far as legally possible.

LEGAL REQUIREMENTS

The following rules are required by law and are to be strictly adhered to. It is prohibited to:

- Send or forward email messages containing libelous, defamatory, offensive, racist or obscene remarks. If you receive an email of this nature, you must promptly notify your supervisor.
- Forward a message without acquiring permission from the sender first.
- Send unsolicited email messages.
- Forge or attempt to forge email messages.
- Disguise or attempt to disguise your identity when sending mail.
- Send email messages using another person's email account.
- Copy a message or attachment belonging to another user without permission of the originator.

BEST PRACTICES

[Company] considers email as an important means of communication and recognizes the importance of proper email content and speedy replies in conveying a professional image and delivering good customer service. Users should take the same care in drafting an email as they would for any other communication. Therefore [Company] wishes users to adhere to the following guidelines:

- Writing email: Write well-structured email messages and use short, descriptive content.
- [Company]'s email style is informal. This means that sentences can be short and to the point. You can start your email with 'Hi', or 'Dear', and the name of the person. Messages can be ended with 'Best Regards.' The use of Internet abbreviations and characters such as smileys however, is not encouraged.

- Signatures must include your name, job title and company name. A disclaimer will be added underneath your signature (see Disclaimer)
- Users must spell check all mails prior to transmission.
- Do not send unnecessary attachments. Compress attachments larger than 200KB before sending them.
- Do not write emails in all capitals.
- Do not use cc: or bcc: fields unless the cc: or bcc: recipient is aware that you will be copying a mail to him/her and knows what action, if any, to take.
- If you forward mails, state clearly what action you expect the recipient to take.
- Only send email messages the contents of which could be displayed on a public notice board. If they cannot be displayed publicly in their current state, consider rephrasing the message, using other means of communication or protecting information by using a password (see confidential).
- Only mark emails as important if they really are important.
- Replying to email: Email messages should be answered within at least eight working hours, but users must endeavor to answer priority emails within four hours.
- Priority email messages are messages from existing customers and business partners.
- Newsgroups: Users need to request permission from their supervisor before subscribing to a newsletter or news group.
- Maintenance: Delete any email messages that you do not need to have a copy of, and set your email client to automatically empty your "deleted items" on closing.

PERSONAL USE

It is strictly forbidden to use [Company's] email system for anything other than legitimate business purposes. Therefore, the sending of personal email messages, chain letters, junk mail, jokes and

executables is prohibited. All messages distributed via the company's email system are [Company]'s property.

CONFIDENTIAL INFORMATION

Never send any confidential information via email. If you are in doubt as to whether to send certain information via email, check this with your supervisor first.

PASSWORDS

All passwords must be made known to the company. The use of passwords to gain access to the computer system or to secure specific files does not provide users with an expectation of privacy in the respective system or document.

ENCRYPTION

Users may not encrypt any email without obtaining written permission from their supervisor. If approved, the encryption key(s) must be made known to the company.

EMAIL RETENTION

All email will be deleted after 60 days. If a user has sufficient reason to keep a copy of an email, the message must be moved to the folder "For archiving."

EMAIL ACCOUNTS

All email accounts maintained on our email systems are property of [Company]. Passwords should not be given to other people and should be changed once a month. Email accounts not used for 60 days will be deactivated and possibly deleted.

SYSTEM MONITORING

Users expressly waive any right of privacy in anything they create, store, send or receive on the company's computer system. [Company] can, but is not obliged to, monitor email without prior notification. If there is evidence that you are not adhering to the guidelines set out in this policy, the [Company] reserves the right to take disciplinary action, including termination and/or legal action.

DISCLAIMER

The following disclaimer will be added to each outgoing email:

'This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the company. The recipient should check this email and any attachments for the presence of viruses. The company accepts no liability for any damage caused by any virus transmitted by this email.'

QUESTIONS

If you have any questions or comments about this Email Policy, please contact [Name], [Tel], [Email]. If you do not have any questions [Company] presumes that you understand and are aware of the rules and guidelines in this Email Policy and will adhere to them.

DECLARATION

I have read, understand and acknowledge receipt of the Email Policy. I will comply with the guidelines set out in this policy and understand that failure to do so might result in disciplinary or legal action." [35]

Signature: _____

Date: _____

Printed Name: _____

[35] www.email-policy.com

ENFORCING THE EMAIL POLICY

There are a number of ways in which you can enforce the company email policy: [36]

PROVIDE TRAINING

Regularly train users in applying the email policy. Help users send effective email messages by informing them of best practices, explain that offensive jokes and remarks can be much more harmful than they seem, and stress that employees who witness abuse of the email system must report this to their supervisor. Encryption techniques and the use of digital signatures should also be covered.

TAKE PROMPT ACTION

If an employee complains about offensive email, it is extremely important that this be dealt with fairly and quickly. Internal procedures should be in place in order to allow investigation into complaints. Employees must also be encouraged to come forward if inappropriate email content is detected. Prompt action can potentially save your company a large amount of legal costs, as was the case with WorldCom corp. Within 10 days of hearing the employees' complaints about offensive email messages, supervisors arranged two meetings to discuss the incident. They also reprimanded the sender of the messages by placing a written warning in her personnel file and issuing a verbal reproach. WorldCom supervisors also requested that several workers, including the two plaintiffs, review the company's email policy. The result was that the court deemed that the employer had "acted reasonably" and dismissed the case against WorldCom.

[36] www.email-policy.com

MONITORING EMAIL

Monitoring of email is the only way to make sure that no email policy rules are being breached. You can monitor email messages that are stored on the company's systems to detect patterns of misuse, but the best way to monitor email is to automatically block or quarantine messages before they are sent or received. The practicing of email monitoring could also be of help in a court of law, since it shows that the company is serious about preventing offensive messages and unlawful use of the email system. Apart from monitoring mails for legal purposes, attention must also be paid to protect the email system from viruses and spam messages. Many email filtering and monitoring programs that are capable of performing these actions. Real-time spam-killing software can be used with filtering software.

ABOUT MESSAGESOLUTION

MessageSolution is the leading innovator of email and file archiving, compliance, electronic discovery, and data storage management solutions that help enterprises and organizations streamline business operations, mitigate risk, and reduce costs. MessageSolution's email and file archiving products enable clients to cost-effectively manage messaging resources, fully comply with industry regulations and quickly respond to urgent legal, audit and HR discovery needs. MessageSolution actively works with clients to re-define their IT infrastructure worldwide.

MessageSolution's technologies enable organizations to capture, preserve and access unstructured emails, attachments, files and other important electronic records. Innovative, flexible, and highly scalable information retention and content storage management solutions address the following issues in electronic document and business information processing:

 © 2007 Robert F. Smallwood Copyrighted material

- Email, file, attachment, and instant message archiving;
- Storage and server optimization;
- Regulatory compliance;
- Litigation support;
- Electronic discovery;
- HR risk management;
- Governance of Corporate Intelligence.

MessageSolution's Enterprise Email Archive multi-platform edition was the first archiving solution launched in the market to support Windows and Linux operating systems at a native level. Since its inception, Enterprise Email Archive has developed fluid integration with Domino, GroupWise, and multiple Unix-based platforms. Enterprise Email Archive's highly flexible open standard technology enables it to be compatible with all major email servers in the marketplace.

 © 2007 Robert F. Smallwood Copyrighted material

Conclusions

Email has become the business communication mode of choice. It saves time and reduces costs. But it has become so ubiquitous and voluminous that knowledge workers are virtually drowning in the deluge they receive daily.

Email is the most critical enterprise application, well above the next choice, database applications.

Regulatory requirements dictate that email messages and their attachments are preserved for significant periods of time, usually five to seven years.

Not all email messages constitute a legal record. A record documents a transaction or business-related event that may have legal ramifications or historical value.

The active monitoring of outbound email is a growing trend and is termed outbound content compliance (OCC).

Using OCC capabilities, firms set up their organization- and industry-specific list of watch words, phrases, senders and recipients to ensure that nothing leaves the bounds of the organization that could potentially cause a violation.

Stream messaging is a secure email system that leaves no record on any computer or server. It is ideal for ensuring that sensitive internal information is kept confidential and not publicly released. Stream messaging is not intended to be a replacement for corporate email. If an electronic record is needed, email it.

It is critical to adhere to compliance requirements and enforce governance policies as close to the point of origin *before* they become damaging and lead to costly litigation or government investigations.

The key difference between email archiving and email management (EMM) software is that there is a much greater focus on the *content* within messages in EMM, and there are greater proactive capabilities built in to foster compliance efforts.

 © 2007 Robert F. Smallwood Copyrighted material

Before starting off on a search for EMM software, requirements the software will need to fulfill must be defined. This begins with deciding formally to implement, monitor and update e-policy, and then more specifically establishing an organization's detailed email policy.

For the policy to be effective the document should use clear and simple wording and not be longer than three or four pages.

Under U.S. federal law, management can use written email policy to inform employees that they have no reasonable expectation of privacy when it comes to sending and receiving email. However, a multinational corporation based in the U.S. may not be able to apply this policy to European, Asian or Middle Eastern employees.

Employees should not put anything into email that they wouldn't put in a typed letter that may be reviewed later during litigation or compliance proceedings.

Litigation readiness is being ready regardless of the specific issues in a lawsuit, by taking steps to minimize preparation and research time, and implementing enabling technologies.

New e-discovery amendments to the Federal Rules of Civil Procedure (FRCP) went into effect in December, 2006. These new rules dictate the discovery process for electronically stored information.

The FRCP apply to U.S. district courts which are the trial courts of the federal court system. Some of the FRCP revisions apply specifically to the preservation and discovery of electronic records in the litigation process.

Specific steps must be taken in advance to prepare for compliance and governance proceedings, potential litigation and the discovery of electronically stored information. These steps include updating email policies and implementing enabling technologies such as EMM.