

Make Email a Better Business Tool

Written and produced by OTG Software, Inc.

Enterprise Email

Email—it's a reliable, fast, inexpensive, and widely accessible method of communication. In its most basic form, email is a "store-and-forward" process of transmitting electronic messages through a computer network. The attachment of spreadsheets, documents, presentations, graphics, and even applications to email adds to its potency. As a result, email has displaced traditional corporate communication systems—including postal services, couriers, faxes, and to a lesser extent, telephones—and has suddenly become an integral part of daily business operations. In fact, it has become a treasure trove of information critical to the ongoing success of the enterprise.

However, the power of email as a business tool is compromised by a lack of centralized administration and record management inherent to traditional communications systems. When a letter is sent, a copy is stored in a filing system. Similarly, faxes are retained and filed as originals. When needed for later use or review, these items are easily retrieved. Not so with email messages.

Additionally, because attachments can be included with messages, email is vulnerable to virus attacks—attacks that can cripple an entire organization for hours or even days. Once infected with a virus, organizations may experience system damage or a complete loss of email messages and archives—which in turn affects productivity. Consider the "Love Bug" virus, which in May 2000 brought millions of computers worldwide to a halt and caused an estimated \$8 billion in damage, largely from lost productivity.¹ While virus scan tools and alert users may help limit the spread of viruses, even one infected user can cause an enterprise-wide shutdown as IT staff race to prevent further propagation. Further, new computer viruses have recently become so prolific that the threat of potential crashes is now a major concern.

With no central control or administrative support for classifying, indexing, filing, storing, and retrieving the 2.9 billion email messages² that U.S. businesses are transmitting daily, it's no surprise that everyone is experiencing some sort of fallout. The remainder of this technical guide discusses the issues introduced by the pervasiveness of email, current methods to manage email messages, and guidelines for improvement.

¹ *The Washington Post*, June 15, 2000.

² *Email Forecasts and Trends*, Mark Levitt, IDC, July 1999.

Issues Introduced by Email

The explosive growth in the use of email is affecting everybody, from users and IT administrators to management and record keeping professionals.

Typical users find themselves coping with an average of 70 email messages per day. They can barely find time to respond, never mind devise a method for managing their personal email archives. Thus, it becomes increasingly difficult to locate information when it's needed, and users spend countless hours searching for or reproducing data that is often inaccessible or lost. For messages that are a year old, it can take an email administrator more than 11 hours to recover from the archive.³ The limited processing and storage capacity of workstations further hinders the ability of users to accomplish their business objectives. Research shows that a typical 3,000 user email system handles more than one terabyte of message traffic annually.⁴

The increased use of email also places a burden on IT administrators, who must deal with burgeoning message stores that bog down the email servers. Because end users don't want to discard messages, there is a constant struggle to provide adequate storage space without compromising system reliability. Not only are IT

Forrester Research asserts that e-marketplaces are evolving from a transaction/commerce focus to include collaboration via email, which will not only increase the volume of email messages but will make them more mission critical.

Forrester predicts that over 50% of online trade will flow through e-marketplaces by 2004, reinforcing the need for collaborative software and better email management.

managers responsible for ensuring continuous availability of the server, but they must protect email communications during and following virus attacks.

Meanwhile, management needs to protect confidential information contained in email from loss, theft, or inappropriate disclosure. Just as important is an email policy that prevents the waste of employee time and computer resources due to junk mail, spam, chain mail, and other frivolous or non-productive mail. One multi-national company placed the cost of junk mail at one dollar per employee per day⁵.

Finally, despite the fact that email is an integral part of business communication, the lack of administrative control over email jeopardizes record management procedures and the ability to comply with regulatory and legal requirements. Without a formal filing and retention policy, past emails become a maze of unrelated communications that make responding to legal discovery and FOIA requests

time consuming and costly. So time consuming and costly, in fact, that many

³ *Email Archive and Retrieval: A Hidden Enigma, A Hidden Cost*, CNI, 1999.

⁴ *Email Archive and Retrieval: A Hidden Enigma, A Hidden Cost*, CNI, 1999.

⁵ *e-policy*, Michael Overly, AMACOM 1999.

organizations opt to risk non-compliance or settle disputes rather than incur the expense of retrieving archived email.

Current Practices in Email Storage Management

Currently, each user is responsible for managing and archiving the estimated 300MB of email received on his desktop annually⁶. Even when desktop archive utilities and training are provided, the results vary according to individual user needs and work habits, especially given the lack of formal policies on message categorization or retention. The lack of formal retention policies also contributes to swollen message stores, as users dislike discarding messages, which can lead to service shutdown. Therefore, an unmanaged collection of personal archives and over-full mailboxes is not in the best interests of the organization.

With responsibility for email system performance and availability, the IT department is concerned with preventing over-full message stores—a serious and routine threat⁷ to email server performance. Because one email server houses the mailboxes of multiple users in an organization, the server can easily fill up, resulting in a system shutdown, and consequently cutting off email service to those users. To safeguard against overfull message stores and ensure removal of old messages, current IT practices include sending “delete your messages” notices to all users, or blind purging of the message stores. In the case of Microsoft Exchange, which accounts for approximately 50 percent⁸ of the email market, the send and receive services are shut down when the message store exceeds its limit (after administrative notices have been sent). In addition to reducing the volume of messages on the server, such practices also encourage IT organizations to implement guidelines⁹ that treat old email messages as potential liabilities and recommend actively removing them from server message stores.

Current IT practices to minimize message storage also include encouraging personal desktop archives, routinely making backup tapes of all email servers, and restricting the size of messages or attachments. Since personal archives will be spotty in that not every employee will properly archive email, and in that they might be discarded should the employee leave the organization, backup tapes become the only centrally controlled and available archive of message stores. When it is necessary to recover messages—either for enterprise users in need of information or for discovery requests—IT administrators can do so only by accessing the data on backup tapes – an expensive and time consuming task.

⁶ Conservatively estimated from multiple sources, including market reports from Ferris Research (1999), and *Email Archive and Retrieval: A Hidden Enigma, A Hidden Cost*, Creative Networks, Inc (CNI), 1999.

⁷ “The typical Exchange message store, assuming that messages are not deleted, fills up in less than 27 days.” As found in *Email Archive and Retrieval: A Hidden Enigma, A Hidden Cost*, CNI, 1999

⁸ Various sources, including *Corporate Email Systems Within Fortune 50 Corporations*, July 1998, The Radicati Group, Inc. Corroborating data was received from Steve Lecompte, 1999, Federal Computer Week.

⁹ *Market Research Reports*, Ferris Research, Inc, 1999.

For example, recovering all archived messages that concern a specific subject requires initiating a server with the appropriate email program, loading an archive tape, and searching the tape for relevant email messages—over and over, until all the tapes have been loaded and searched. With the cost of searching an individual tape running as high as thousands of dollars, this method is extremely costly.

Limits on message or attachment size can impact an organization's effectiveness. For example, if a sales person is unable to receive a large RFP as an attachment to email, the organization cannot respond, and loses the opportunity. Similarly, if an employee is unable to send a large file in response to a customer request for information, it reflects poorly on the organization.

Conflicting with the need to maintain system availability are two factors: (1) the onus on the IT department to ensure disaster recovery, and (2) the need to retain email for the necessary length of time to enable the organization to satisfy external requests for information—such as SEC audits, due diligence requests, FOIA requests, and legal discovery requests.

Information contained in old email messages may also be required for any number of internal business purposes. For example, the sales department may need to access a draft of a contract; customer service may need to review communications that promise certain rewards to customers; human resources may have a question about an employment offer. And because each individual user decides which email messages to retain or delete, much of this information is hidden from the rest of the organization. Thus, when an employee leaves, or is suddenly unavailable or even on vacation, the treasure trove of mission-critical information in his archived email could be lost.

Meanwhile, discovery requests may arise as a result of FOIA requests in state or federal organizations or as a routine part of enterprise litigation. Regardless,

Current Email Client Technologies and Message Store Practices

Adopted technologies and practices determine where message stores reside within the email organization, including the user workstation, the email server, or on backup tape archives. Uncontrolled and widely dispersed message stores bear greatly on the escalated costs of message recovery, retention practices, and risk management.

The choice of email client protocol impacts where a user's messages are kept. POP (Post Office Protocol) is the most widely deployed messaging protocol for email clients. User messages are downloaded from the email server and kept on the user workstation. Following download, no message copies remain on the server. In addition, the message stores on the workstation are uncontrolled and hard to manage, and so represent a significant risk from a record management perspective.

IMAP (Internet Message Access Protocol) provides much greater flexibility regarding the transmission and permanent storage of messages. The premise of IMAP is that the server provides a better permanent message store than does the workstation. IMAP offers a command set that enables a client to work with messages remotely. Message headers can be downloaded separate from the body or attachments, for example, and reviewed at the desktop. When using IMAP, messages remain on the server until the user 'deletes' them. In actuality, this just sets a delete flag, which allows a server-side 'EXPUNGE' function to later remove them from the server.

With the increasing deployment of Microsoft Exchange, many user workstations are configured to use MS-Outlook running the MAPI (Messaging Application Programming Interface) protocol. The default MAPI profile does not download messages to the workstation. However, MAPI supports a remote-user mode, where messages are downloaded to the client workstation, so they are available when the workstation is disconnected from the Exchange server. Note that, in either case, message copies remain on the Exchange server in the Private Information Store.

In the cases of IMAP and MAPI, the server's message store is archived to backup tape for disaster recovery purposes. Since most organizations retain these backup tapes for years, they are often targeted in discovery requests during litigation, audit, or other investigation.

responding to these requests places a significant burden on IT resources. Backup tapes must be restored to a replica of the production email server. A search may span several email servers and, in some cases, the personal archives on hundreds of desktop computers. The search may also need to cover a series of backup tapes made through a target calendar period. Thus, the estimated costs for fulfilling a single discovery request run from tens to hundreds of thousands of dollars. For example, the cost of recovering 246,000 emails from approximately 4900 backup tapes will cost the White House an estimated \$10 million¹⁰. No wonder many companies choose to settle cases, even when they are not at fault, so as to avoid the high cost of discovery.

Guidelines for Effective Message Store Management

Government and industry organizations have worked for several years to develop record management guidelines for electronic documents, communications, and email. Several publications can serve as references for various types of organizations.

One such reference is the DoD 5015.2 specification, titled “*DESIGN CRITERIA STANDARD FOR ELECTRONIC RECORDS MANAGEMENT SOFTWARE APPLICATIONS*,” which is designed to meet federal (NARA) guidelines and existing regulations.

For corporations, ARMA International released the draft version of the “Guideline for Managing E-Mail” in April of 1999¹¹. ARMA’s International Standards Advisory and Development Committee and the members of its E-mail Guideline Task Force received input from a wide range of state, federal, educational, and commercial representatives to develop the guidelines

For financial institutions regulated by the SEC, requirements for managing electronic communications including email were published as amendments to SEC Rule 17 in February of 1998¹².

While these various guidelines apply to a diverse range of organizations, it’s clear that any effective solution for managing email must include the following capabilities:

1. Archival of email documents and attachments—and associated address and routing information—in original electronic form;
2. Creation of an email policy that addresses message retention and filing requirements;

¹⁰ *Washington Times*, May 4, 2000.

¹¹ The draft document “*Guideline for Managing E-Mail*” is available through the ARMA web site.

¹² 17 CFR 240.17-a. SEC Rule 17a establishes record retention and retrieval policies for exchange members, brokers and dealers.

3. Automatic and content-based classification of email to folders/categories within the system;
4. Creation and execution of disposition instructions for each email folder/category;
5. Protection of the archive against unauthorized access;
6. Inviolable auditing of administrator access to archived documents (i.e., administrators cannot tamper with audit records);
7. Powerful search and retrieval tools for end users and administrators, based on a full-text index and user-defined metadata; and
8. Use of random-access, low-cost, and non-volatile media for long-term storage.

Adding Value to Email Message Store Management

Ideally, a message store management solution should both address the basic requirements stemming from published guidelines and add value by bringing the power of data management to email systems—in essence, channeling the daily stream of email messages and attachments into a tool that provides competitive advantage.

Any such solution should address the requirements of users, IT administrators, management, and record keeping professionals by providing the following benefits:

- ◆ **Superior email server management.** A product that combines automated capture, integrated support for low-cost mass storage, and content-based classification rules can transform an organization's temporary cache of messages on the server into a tool for enterprise document management. Email servers are freed of message overload, improving performance and availability. Additionally, without the requirement to restrict message size, larger and more complex documents can be transmitted. As a result, email can serve as the basis for strategic planning and business development efforts, without impacting IT.
- ◆ **Fast and efficient access** to the historical body of email messages and attachments. Full-text indexing combined with a powerful search engine would allow end users to access their own messages, while only authorized managers or administrators could search across multiple mailboxes to meet audit/regulatory requirements, discovery requests, or other business needs.

- ◆ **Reduced costs.** Research shows a typical user will need to recover messages or documents from an email archive about 15 times a year. Subsequent analysis shows that large companies spend an average of \$193 per user, per year to retrieve messages from their email archives¹³ using current methods. Reducing the per-user, per-year costs of retrieval should be an inherent factor in any message store management solution.
- ◆ **Record Management.** An effective solution ensures adherence to formal email policies with enterprise-level data management tools that categorize and manage email through a useful life cycle. By using a tool that integrates record management functionality into email systems, organizations can easily comply with SEC, federal, and state/local requirements.
- ◆ **Quicker, lower-cost discovery actions.** A product with full-text indexing and cataloging features enables email discovery actions to be completed in hours instead of weeks, greatly reducing expenses. A 'freeze' feature that may be used at the onset of any investigation to protect message categories from automatic destruction is also desirable.
- ◆ **Protection of business communications.** A message store management solution that ensures that email records are tamper-proof throughout their life cycle and guards against abuse by monitoring compliance with corporate policy is critical. Additionally, it should facilitate clean up of message stores following virus attacks, enabling recovery within hours rather than days and guarding against loss of information.

Conclusion

One organization that has spent a significant amount of time working to address email message store management is OTG Software, a leading provider of online data storage management and data access software. Well known for its application-centric product suite, XtenderSolutions™, OTG is continuing to develop innovative products for data access and connectivity. EmailXtender™ is the latest addition to the XtenderSolutions suite and offers a practical, cost-effective approach to enterprise-level email storage and retrieval.

¹³ *Email Archive and Retrieval: A Hidden Enigma*, A Hidden Cost, CNI 1999.

Glossary

FOIA – Freedom of Information Act

NARA – National Archives and Records Administration

ARMA – American Records Management Association

SEC – Securities and Exchange Commission