



ESG REPORT

E-mail Archiving in the SMB: Addressing Enterprise Requirements with Fewer Resources

By Lauren Whitehouse
With Brian Babineau

March, 2008

Table of Contents

Table of Contents	i
History is Repeating Itself	1
Why Build a Message Archive?	1
E-mail is a Business Record.....	1
E-mail is Evidence.....	2
E-mails (Especially Older Ones) can be Useful	3
Current Methods Aren't Effective	3
Building an E-mail Archive	4
The Basics	4
The Benefits	5
The Considerations	6
Conclusion	6

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at (508)482-0188.

History is Repeating Itself

Once the SEC, NASD and NYSE included e-mail under the umbrella of business records, large Wall Street firms immediately began saving backup tapes to address new regulations. As regulators began requesting e-mails as part of ongoing investigations, the big banks realized that traditional backup tape methodology was no longer going to work. They quickly turned to message archive software solutions that index records and keep them in a readily accessible format. This same trend quickly permeated pharmaceutical, healthcare and any other highly regulated industries where e-mail was ubiquitously used in business transactions. In 1997, an e-mail from a Merck scientist to executives outlined the potential risks of Vioxx a few years before the drug became a mainstream prescription. As a result, message archiving became a commonplace solution for large enterprises that need to address record retention rules while facing an onslaught of electronic discovery requests involving messages.

It appears as though history is about to repeat itself, but this time, small and medium-sized businesses (SMBs¹) will also be in the mix. Thousands of small community banks, hedge funds and investment advisers will face increased regulatory scrutiny due to the lax lending standards currently plaguing the U.S. economy. There is no question that a subset of these financial services firms will also find themselves required to produce records that range from loan applications to e-mails between mortgage brokers. U.S. State Attorney Generals have already targeted lenders and asset management firms in an attempt to recoup some of the financial losses suffered by homeowners. ESG research² suggests that one out of two SMBs have gone through an electronic discovery event—the same ratio as enterprise organizations two years ago. This current research also shows that two-thirds of enterprises have now been through an electronic discovery, indicating that SMBs—including those outside the financial services industry—will continue to face similar e-mail management and retention challenges.

Since SMBs use e-mail just as much as their enterprise counterparts, creating an online, disk-based archive makes sense. The biggest difference is that SMBs rarely have IT staff dedicated to manage e-mail applications. Therefore, adding an e-mail archive solution to the mix cannot create an incremental burden for SMB IT departments. Installing and maintaining the solution must be easy; otherwise, the benefits of keeping messages accessible for compliance and electronic discovery purposes could be outweighed by operational headaches. But making an e-mail archive solution easy-to-use e-mail archive solution should not impact its feature set. SMBs must be able to retain, search, preserve and produce messages when requested.

E-mail archive solutions have been around for the better part of 10 years, but most are targeted at large enterprises because that is where the regulatory and discovery challenges started. There are several trends that indicate SMBs will need e-mail archive solutions sooner rather than later. When looking at the potential offerings in the marketplace, SMBs should keep in mind considerations such as ease of deployment, the ability to securely search an archive and others that can increase an e-mail archive implementation's value,.

Why Build a Message Archive?

E-mail is a Business Record

Many SMBs rely on e-mail to conduct business. Contracts, invoices, medical instructions and construction blueprints—among other important files—are sent with commentary via e-mail. Local government officials may use e-mail to discuss an upcoming school committee meeting or how budgets for the next fiscal year can be balanced. Many e-mail communications and attachments contain information relevant to the business, which constitutes the entire message as a business record. As such, these e-mails must be retained according to record retention regulations such as HIPAA (Healthcare), Sunshine Laws (U.S. state-specific rules) and the Investment Advisors Act of 1940. In Germany, the Federation of Organisation and Information Systems e. V.

¹ ESG defines SMBs as organizations with 1000 or less employees.

² ESG Research Report: *Electronic Discovery Requirements Escalate*, November, 2007.

(VOI) trade association has defined policies for 'revision safe' electronic archiving. At a minimum, most of these laws and recommendations dictate the types of records that must be created and how long they must be kept. Because many of the rules were put in place well before the advent of e-mail, none of them specifically call out electronic messages. However, many courts and regulatory bodies have issued opinions, interpretations and statements concerning business records sent via e-mail whereby the method of creating or transmitting records should not impact its retention. Basically, if e-mail is used to send a business record or if the message itself contains information making it a record, it is subject to the same retention requirements as paper records.

SMBs are subject to record retention regulations and at some point, some of those records will be e-mails. Additionally, more organizations are expanding records management programs to include information that is important to the business, but not subject to a specific law. E-mails containing information on compensation, hiring, merger and acquisition activity, and correspondence with external counsel are retained in response to an increased focus on corporate governance. SMBs looking at corporate governance initiatives will realize the importance of proper records retention processes inclusive of e-mail.

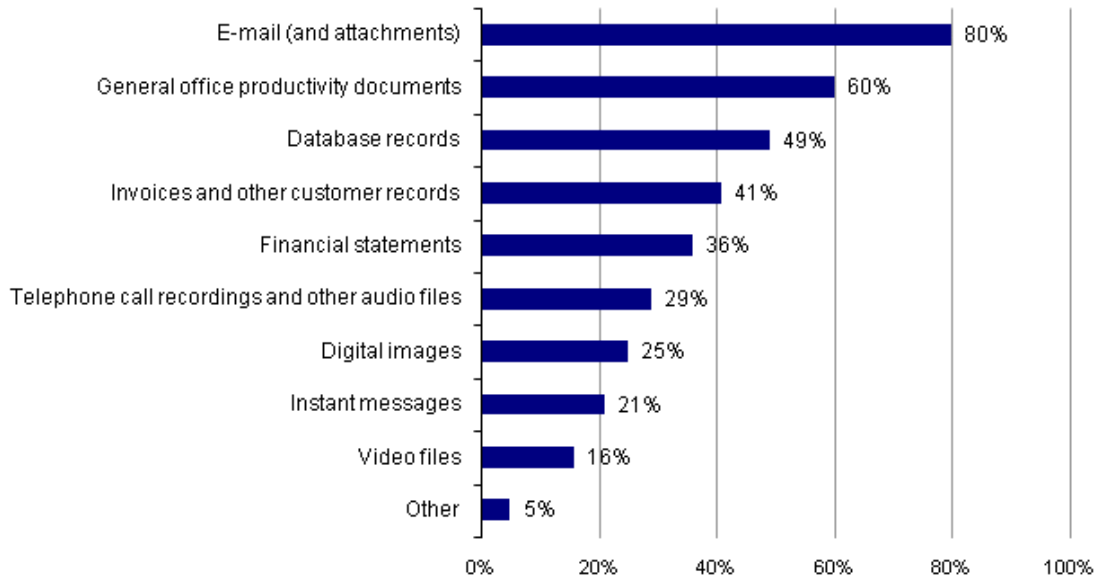
E-mail is Evidence

Saving greater numbers of e-mails is a doubled-edged sword. On one hand, an organization has to do it because of the law or because it is the right thing to do for stakeholders. On the other hand, messages and other information can be requested as part of a legal or regulatory discovery inquiry. The benefit of saving information is compliance with regulatory and governance policies; the threat manifests itself in the potential legal liability that saving more messages carries. In December 2006, new amendments to the Federal Rules of Procedure (FRCP) outlined requirements that all organizations must follow when dealing with Electronically Stored Information (ESI). One of the most predominant additions is Rule 26(f) that states an organization must know its ESI sources and how accessible this data is for a "Meet and Confer" session between opposing counsels.

Because of its role in business processes and the fact that employees may communicate anything in a message, e-mail is the most commonly requested form of ESI (Figure 1). Messages provide a unique perspective into any business and for SMBs that often employ e-mail in accounting, hiring and other critical operations, it is not a matter of *when* a discovery request occurs, it is a matter of how often. In response to Rule 26(f), organizations should be aware of all e-mail it has retained, where it is and how much it will cost to produce it if necessary.

FIGURE 1. MOST FREQUENTLY REQUESTED RECORD TYPES DURING AN ELECTRONIC DISCOVERY

To the best of your knowledge, which of the following record types has your organization been asked to produce in a legal proceeding or regulatory inquiry? (Percent of respondents, N = 107, multiple responses accepted)



Source: ESG Research Report, *Electronic Discovery Requirements Escalate*, November 2007

The biggest misconception in dealing with e-mails during electronic discovery is that the process ends when the appropriate messages are located and turned over to the attorneys. The reality is that organizations must also preserve messages by preventing deletion or modification until either the case is over or the e-mails are deemed irrelevant. Failing to preserve evidence creates problems. Even if specific messages are not admissible as evidence, if they are deleted, the courts may infer that the e-mails contained incriminating evidence, which creates a perception of guilt. In either case, an organization may not be able to adequately support or defend its claim and fines can be levied by courts or regulators.

E-mails (Especially Older Ones) can be Useful

Two-thirds of organizations surveyed by ESG enforce e-mail quotas.³ The rationale is simple: control e-mail server and storage costs. While this seems like a good idea, it can hurt productivity and increase legal risk. Employees are often forced to create personal archives (.pst files or personal folders, commonly referred to as PSTs) because their inboxes are full and e-mail cannot be sent or received after an inbox has reached its quota. Personal archives solve the problem, but when it comes time to search for a specific message due to a legal or regulatory discovery event, attorneys have to search through message applications, PCs and file shares in the hopes of finding responsive e-mails. Of course, employees could simply delete messages, which may not be the best course of action given that the e-mails may contain important information needed for future reference. The challenge for SMBs is to control e-mail storage costs while providing central access to messages.

Current Methods Aren't Effective

Record retention regulations and electronic discovery are not new challenges. IT departments have been trying to address these obstacles as an increasing amount of information is born digital. Traditionally, tape was used

³ ESG Research Report: *2007 E-mail Archiving Survey*, November, 2007.

as a corporate archive when media was removed from normal backup rotations and kept for an appropriate period of time. Essentially, backup processes were modified to create a corporate archive, which addressed the challenges posed by the growing quantity of records and evidence being created by computer systems. There is a big difference in archive process and technology when compared to backup—and e-mail magnified these nuances.

Backups create copies of data that may be used if data is deleted or corrupted. Backup software that initiates the copy and controls access to the media is the most common technology used to support data protection operations. A backup process works well for protecting data, but gets complicated when record retention and electronic discovery are overlaid. Dealing with a large amount of tapes, quickly accessing data and managing too many retention periods could become serious issues. The intersection of e-mail with compliance and electronic discovery forces organizations to introduce an archive. The variety of records created or sent using e-mail means that there is a high likelihood that several retention periods have to be applied or that the longest retention period prevails. At any time, e-mail may be requested to support compliance or discovery processes, so accessibility is paramount.

Organizations forced to deal with increased accessibility and multiple retention periods within an e-mail archive found that tape storage became less feasible. SMBs will be deterred from choosing tape as the media of choice for an e-mail archive due to the lack of resources to handle tapes during a discovery or investigation and the cost of restoration during a discovery event. Legal service providers can charge between \$500 and \$2,000 per tape (depending on the format and amount of data) for such services. Additionally, because tapes are usually used in a rotation, there is a risk that they may be accidentally erased when they should be preserved as part of an ongoing legal matter.

When people need access to e-mail, time is often of the essence. Compliance Officers, litigation support specialists and corporate counsel must be able to search messages, requiring them to be indexed. Backup software creates a catalog and the data has to be restored to its native format before it is indexed. Waiting for this process to take place leaves attorneys helpless, wasting valuable time.

Further, if an organization wants to keep mailbox quotas in place while ensuring that messages are accessible in a central location, backups will not work. Every time an employee needs access to an older message, IT would have to restore data from tape and move the message back into the mailbox. SMB IT departments would have to spend most of their time helping employees look for older messages.

Building an E-mail Archive

The Basics

If tape is no longer feasible as the primary means of e-mail archiving, an SMB will quickly realize that an alternative solution is required to move messages from the primary environment to a secondary one. There are typically two components of an e-mail archive solution: software that identifies and manages messages in the archive and the storage platform that retains the information. The software typically accepts e-mails from the primary messaging application (Microsoft Exchange or Lotus Notes) or scans inboxes using pre-built policies to identify messages to be archived. Most records management and discovery implementations leverage Exchange's Journaling features to feed the archive software (journaling creates a copy of every message sent by a mailbox and sends that copy to a predetermined destination, in this case the archive software). Once the e-mail archive software receives the messages, it indexes the e-mail and associated attachments, sets a retention period and stores the content—in native format—within a repository. The message repository can sit on any storage media, but as previously discussed, a disk-based archive is recommended so that the data is readily searchable and accessible.

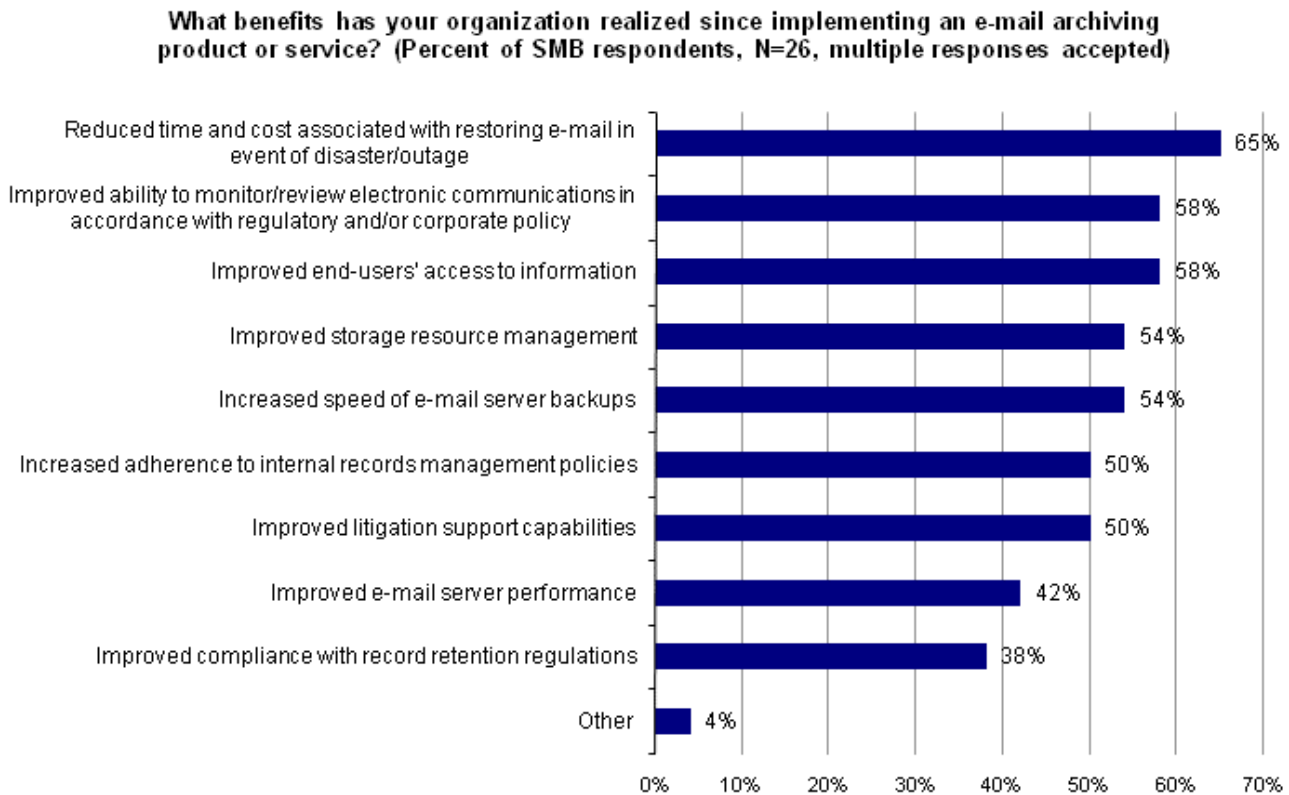
The Benefits

With a copy of all messages centrally indexed and stored, an SMB can comply with record retention regulations and corporate governance programs. Additionally, mailbox quotas can be enforced without requiring message deletion or creation of personal archives. The archive software presents an interface for users to search messages within a repository and is also responsible for enforcing retention periods. It is imperative that the archive software support permission-based searches so that employees can see only their own messages, but auditors and attorneys can query the entire archive. With several information privacy rules forcing organizations to properly secure information, these access controls must be in place.

When a message is being preserved for legal or regulatory purposes, the e-mail archive solution can prevent modification with access controls and—because it is a separate environment (from the primary messaging application)—it can track any attempts to change or delete information within the archive. The archive software should supply an audit trail, which can be presented in courts or to regulators to prove the authenticity of a subset of messages.

An e-mail archive can also reduce storage costs, as many of the software solutions can single instance messages. Single instancing involves identifying duplicate messages or attachments already in the archive and creating pointers to other similar messages so that only one copy is ultimately saved. Backup and recovery of primary environments can be completed faster as mailboxes are smaller (due to quotas) and personal archive folders on file shares are no longer needed. SMBs that have already invested in an e-mail archive have witnessed these operational benefits more so than others (Figure 2).

FIGURE 2. E-MAIL ARCHIVING BENEFITS REALIZED BY SMB ORGANIZATIONS



Source: ESG Research Report, 2007 E-mail Archiving Survey, November 2007

The Considerations

The downside of introducing an e-mail archive solution to an SMB environment is that it adds more things (hardware and software) to the environment for IT to manage. SMBs may not have the resources to manage their primary messaging environments and backups, never mind an archive solution. One alternative to address this issue is to outsource e-mail archiving to a service provider. In this scenario, messages are copied to an external location and searches can be conducted via a Web interface.

Because of the importance of e-mail as key business records and the risk that some of them may become evidence, some SMBs want to have more control over the archive. If outsourcing is not an option for an organization and IT resources are scant, SMBs have two other options. The first is to buy the e-mail archive software and hardware separately and the second is to buy an integrated appliance. An appliance approach is useful for SMBs that want to buy all at once and do not want to install the archive software themselves. The downside of appliances is that the capacity of the archive is limited to what is available inside the box. When an e-mail archive fills up, another appliance has to be purchased.

When choosing archive software separately (or an appliance with the software pre-loaded), an SMB should keep a few things in mind. The first, as previously mentioned, is that it employs permission-based search functionality. Also, organizations should understand how the indexing and search process works. Some solutions utilize proprietary search technology, while others leverage open source—with the major difference being how queries (Boolean, Keyword, etc.) are handled. Accurate searches are required as attorneys and investigators need to be sure they have all relevant content when responding to a discovery request. E-mail archive solutions also vary in performance metrics—how quickly they can ingest and index messages, complete searches and retrieve messages, for instance. These are important metrics as multiple constituents (employees, attorneys, etc.) will be accessing the archive and response times are critical.

Conclusion

Some industries are more regulated or involved in a greater number of litigious matters than others. However, compliance and electronic discovery apply to any organization, regardless of its size. E-mail is a business record and a viable source of evidence. Despite these trends, organizations continually enforce mailbox quotas, which hamper productivity and rely too heavily on backup processes. SMBs may have gotten away with these dated processes because they did not have the IT resources to install and run an enterprise-class e-mail archive solution. Times have changed and so have the offerings in the marketplace. There are now plenty of archive alternatives for SMBs to choose from. It's just a matter of finding the right one.

If it isn't already, e-mail is going to be a staple in any business; therefore, people will need to access it. Some will access it for productivity, while others will want to use messages as the foundation of a legal matter. SMBs can make this process easier with a central e-mail archive, while getting the benefits of compliance and reduced storage costs.

Some SMBs have bucked the trend and already started archiving messages. In these organizations, e-mail archive capacity has increased over 200% in the past 18 months.⁴ This research suggests that organizations are facing the challenges posed by compliance and electronic discovery, and that there are benefits in investing in a central e-mail repository rather than sticking with older processes.

⁴ ESG Research Report: *2007 E-mail Archiving Survey*, November, 2007.



20 Asylum Street
Milford, MA 01757
Tel: 508-482-0188
Fax: 508-482-0218

www.enterprisestrategygroup.com