Email Archiving vs. Destructive Retention Policies

An ArcMail Technology Research Paper

 www.arcmail.com

Email Archiving vs. Destructive Retention Policies

One of the greatest dilemmas businesses face when it comes to email is balancing security and storage concerns. Email continues to be the preferred method of communications today, and as a result businesses are often overwhelmed with the amount and size of emails. Emails have been deemed by the courts to be business records so they must be preserved. In addition to the legal rulings, there are also a number of industry guidelines that require organizations to retain all of their communications, which provides cost, security and storage challenges, particularly for small businesses.

The dilemma leaves organizations with several questions regarding email archiving and retention policies, including:

> When is it more appropriate to archive emails for long periods of time?
>
> Is it ever more appropriate to implement a destructive retention policy that deletes emails that exceed a specific amount of days, whether, 60, 90 or more?

Retention

If you ask most people, they will probably say they have some sort of personal retention routine, or at least their email program has an archiving function. In fact, these retention routines or functions may be the only email retention solution that people know of. A recent study by Osterman Research found that 53 percent of companies lack a policy to govern email retention and destruction. The same study found that 67 percent of the companies even allow individual end-users to determine how long messages are retained.[i]

While retaining some email is important, does an organization need to save every email for extended periods of time? Is it preferable to reduce the amount of "old" data stored on mail servers, and delete sensitive data that could be leaked or stolen? This practice is defined as *destructive retention*, a policy whereby email is retained for a limited time and then permanently deleted from the network.

Advocates of destructive retention cite three primary arguments to support the practice:

Change fron the traditional retention policies

Change can be difficult for organizations, particularly if it requires employees to change the way they are accustomed to doing something. The pace of modern business quickly makes yesterday's email irrelevant and not worth the cost, effort and additional load on the network required to retain it. Tradition also has relied on email programs, such as Microsoft Outlook, to manage just how long email is retain in each individual user's PST file. Each month, a pop-up window asks users if they want to automatically archive their email. By simply clicking "Yes," employees can feel that they have done their part in backing up their relevant email, while deleting older messages that needlessly take up space on their hard drive or network server. A case can also be made that, by automatically updating their PST file, users are reducing the organization's potential legal and regulatory exposure.

Storage / Data Overload

Organizations of all sizes are being overwhelmed with data. A 2006 Gartner study found that 55 percent of IT managers identified the growing requirement for storage capacity as their number one storage challenge. Those surveyed estimated that "their capacity needs would grow by an average 25 percent in one year and by 41 percent in two years."[ii] The Enterprise Strategy Group estimates that the average retention period for database records is roughly 6-10 years.[iii]

One of the leading culprits of this data overload is email. According to the Radicati Group, "the

average corporate e-mail user received 126 messages a day in 2006, up 55 percent from 2003. By 2009, workers are expecting to spend 41 percent of their time managing e-mails."[iv] The Radicati Group also found that the average corporate email account receives 18 MB of mail and attachments each business day. That figure is projected to grow to 28 MB a day by 2011.[v]

With organizations already faced with growing data demands, an obvious solution is to delete email regularly to help reduce this management and storage strain.

Eliminate the potential threat of data loss/leakage

Among companies surveyed by McAfee, the average cost of a data-leak incident was estimated at $1.82 million. A popular argument for a destructive retention policy is that, by periodically destroying emails, organizations are reducing this threat. Before deleting email messages, many organizations will download attachments onto secure servers to retain potentially important documents, a practice they see as akin to keeping the groceries and discarding the bag.

Archiving

Email archiving is becoming increasingly important as e-mail communications now play a central role in everyday business operations. Communications previously conducted via phone, fax and snail mail now take place in email, from routine conversations to contract negotiations and document exchanges. Consequently, email content is more business-critical than ever and increasingly relevant to an organization's competitive, legal and regulatory concerns. For public companies, finance organizations and legal firms, email archives are being deployed in litigation, used to demonstrate regulatory compliance, as well as to facilitate disaster recovery and business continuity.

While the cost of email archiving continues to decline, many organizations resist changing their email retention policies. They may not want to invest resources into preserving information they regard as obsolete, sensitive or which could potentially come back to hurt them. Or they may simply want to reduce information clutter. However, an increasing number of these organizations are coming around to the concept of email archiving, due to the three arguments outlined below.

Compliance

More and more organizations, regardless of size or industry, are facing government or industry compliance requirements that reflect the expanding role of email in organization communications and business transactions. Many of these requirements specifically address an organization's responsibility to retain and produce electronic records.

Technology industry analyst group International Data Company reported, "The introduction of legislation such as the Sarbanes-Oxley Act of 2002 and the Health Insurance Portability and Accountability Act [HIPAA] has significantly increased the importance of managing, securing and storing all information within the enterprise. More specifically, because of regulations such as SEC Rule 17a-4 that are very prescriptive for the retention for email, and the numerous and very costly public lawsuits in which an email has been the deciding factor, email has emerged as one of the most important content types that need to be retained."[vi]

Sarbanes-Oxley, HIPAA, and Gramm-Leach-Bliley Act are among several government and industry regulations that have made securing and archiving email correspondence a fundamental requirement. Ignorance of the law or claims of inadequate storage resource are no longer viable excuses for non-compliance With an archiving policy in place supported by reliable archiving technology organizations can be confident of practicing due diligence by enabling internal and external auditors to easily review all virtual paper trails that may come under question.

Productivity

A recent study by IDC found that a company with 1,000 information workers can expect to lose

more than $5 million in annual salary costs due to of the time employees spend on unproductive (email?) searches.[vii]

Email archiving solutions can dramatically lower this cost by making employees more productive. When organizations have self-imposed email quotas in order to control mailbox sizes, users are often forced to manually delete emails to be able to continue sending and receiving emails. Automated archiving solutions eliminate the need for users to manage their own email box and email archiving. If their organizations are already capturing their employees' inbound and outbound email messages, then employees won't have to create personal archives or spend time trying find and restore email messages and attachments.

Discovery

Data is being created and stored in multiple databases across the enterprise. Employees are now using multiple storage devices to facilitate the transport and exchange of information, from USB flash drives, to multi-gigabyte portable hard drives and Web-based hosting services. This is in addition to their personal computers and their companies' network servers. The multitude of storage locations makes it difficult to readily find information, which can suddenly become imperative in the event of a discovery order arising from litigation. The number of places to search only adds to the time, labor and cost associated with searching through records and locating files.

Having an archiving solution that captures all inbound and outbound email in a single location helps to reduce the time and expense. An archiving system that can comply with all of the e-discovery requirements by preserving information for a long period of time is ultimately a practical and cost-effective business tool. A solution that automatically captures and indexes data from multiple sources supports an organization's strategic objectives to be prepared in the event that information needs to be located, reviewed and restored quickly.

With litigation on the rise, archiving emails presents a formidable solution for helping to reduce discovery costs and enhance the organization's ability to respond to inquiries in a timely and comprehensive manner.

Conclusion

While destructive retention policies may still have a place in certain organizations, a comprehensive archiving policy and process is a much sounder approach for most companies today. Faced with the threat of litigation, industry and government compliance regulations and the challenge of maintaining employee productivity, organizations simply cannot afford to leave their email retention policies in the hands of individual employee routines or default software functions.

Advanced archiving policies provide a clear case against destructive retention policies by relieving users of the responsibility to manage email volumes, providing a single, centralized solution for capturing and storing all email data, along with enhanced security to prevent data loss or leaks. Archiving ensures that the invaluable asset that is corporate knowledge-base is retained and stored in an accessible format, while protecting the integrity of the database by preventing users from altering or deleting files.

Destructive email retention policies are no longer a viable strategy for today's businesses. Companies that have paid strict fines as a result of their poor email retention policies have learned the hard way that email content is now regarded as essential business data. An automated archiving system ensures compliance with government and industry regulations and the new Federal Rules of Civil Procedure, while reducing storage costs, enhancing network performance and employee productivity.

ArcMail Defender

Defender by ArcMail Technology is a high-performance, comprehensive email archiving and management solution that includes the right combination of features and functionality that makes it the right archiving solution for small and medium-sized enterprises. ArcMail helps to remove email management from individual users, and its enhanced security eliminates any concerns of rogue access and data theft or leakage.

The independent device provides up to 12TB of onboard storage, and automatically archives and indexes all email and attachments in a secure, centralized location. Everyone from end-users to the IT department can access Defender's user-friendly, Web-based interface to quickly and easily search and restore emails. Defender does not require additional software or hardware, and is easy to install, configure and use.

About ArcMail Technology

Founded in 2005, ArcMail Technology is a cutting-edge provider of simple, secure, and cost-effective email archiving and management solutions for small and medium-sized businesses. The company's ArcMail appliance is easy to buy, easy to install, and easy to use, and improves the end-user experience, reduces the load on IT resources, and safely and securely retains the business information contained in emails. ArcMail provides broad coverage for the SMB market and is capable of meeting the archiving and management requirements for an organization with as few as five users up to more than 4,000 users. The company is developing a global channel program to help deliver its products to organizations worldwide. ArcMail is headquartered in Shreveport, La., and has development groups in Washington and Arizona.
For more information, visit www.arcmail.com

---

[i] Leaf, Nate, "Survey: Most Businesses Lack Clear Email Retention Policy," December 17, 2007, http://www.yourtv20.com/news/technology/12563691.html

[ii] Mullins, Robert, "Storage budgets may not keep up with demand in 2007," *InfoWorld*, October 19, 2006, http://www.infoworld.com/article/06/10/19/HNstorbudg_1.html?STORAGE%20ARRAY%20SYSTEMS

[iii] Prince, Brian, "Database Archiving Market Evolves with Exploding Data Needs," December 13, 2007, http://www.eweek.com/article2/0,1895,2232738,00.asp

[iv] Buckman, Rebecca, "The E-mail Overload," December 17, 2007, http://www.courier-journal.com/apps/pbcs.dll/article?AID=/20071217/BUSINESS/712170371

[v] ibid

[vi] http://accounting.smartpros.com/x46588.xml

[vii] http://www.networkworld.com/news/2007/012307-wasted-searches.html