Governance IT®

Email Archiving: Understanding the Reasons, Risks and Rewards

Proofpoint, Inc. 892 Ross Drive Sunnyvale, CA 94089 P 408 517 4710 F 408 517 4711 info@proofpoint.com www.proofpoint.com

Regulatory compliance, legal discovery and storage management issues are driving more organizations to consider email archiving. Here's what you should know when making decisions about your organization's use of email archiving technology.

Contents

Overview

Statistics show that as much as 60 percent of business-critical data now resides in email, making it the most important repository of data your company may own. This huge amount of data—which grows on a daily basis—translates into a significant burden on corporate storage resources.

These facts—combined with a recent onslaught of regulatory compliance rules—are forcing organizations to take a deeper look at email storage, retention, and archiving practices. In fact, if you are not already considering an archiving solution, it is very likely that your organization will be facing this decision in the coming months or years.

And it's not just compliance with regulations that is driving this trend to archive. As email messages increasingly take center stage in headlines and lawsuits, email has become the electronic equivalent of DNA evidence. Having a system in place that takes this risk into account is crucial for businesses that don't want to end up at the center of one of these scandals.

In most organizations, responsibility for archiving decisions falls to the IT department. Before embarking on email archiving, IT professionals need to understand a range of business and technology issues—from the key reasons for archiving to the best type of archive to meet those needs.

Why Should Your Organization be Archiving Email?

The majority of a company's business-critical data is stored in email—data that impacts revenue, business decisions, corporate reputations and end-user productivity. With all of this at stake, it's not surprising that email is subject to a growing range of legal, regulatory compliance, and business requirements. It's also not surprising that email can cause serious storage issues for businesses.

By providing a secure, searchable, and centralized repository for email, an archive can address the full range of legal, regulatory, business and storage challenges presented by email. These challenges, and the opportunities presented by email archiving solutions, are explored in more detail, below.

Electronic Discovery and Litigation

Understanding the reasons why your organization needs an archiving solution will play a key role in choosing the right solution. One of the most important considerations for businesses, regardless of size or industry, is the issue of electronic search and discovery.

Electronic discovery—or "e-discovery"—usually refers to the retrieval of data from a computer to meet a legal request. However, the term can also be used whenever data retrieval is required for regulatory compliance, HR concerns, validation of client correspondence or other corporate needs. As a result, all organizations require search and discovery capabilities for email, even if they are not currently involved in litigation.

Recently, the electronic discovery burden on IT organizations has increased both in frequency and demand. In fact, a survey performed by Osterman Research, Inc. found that:

- Two-thirds (66%) of IT organizations have referred to email or IM archives or backup tapes to support their organization's innocence in a legal case.
- Nearly two-thirds (63%) of organizations have been ordered by a court or regulatory body to produce employee email or instant messages.

This is not surprising when you consider that email is just as admissible in court as paper-based documents, and can be requested for legal discovery at any time. In fact, email evidence has been the "smoking gun" in numerous cases of illegal corporate activity. And that does not take into consideration the risks of non-business related content that can be found in email.

Sexist, racist and other inappropriate content—which would be deemed unacceptable in all other corporate arenas—can often be found in employee inboxes. In fact, according to the American Management Association, 27 percent of Fortune 500 companies have defended themselves against claims of sexual harassment stemming from inappropriate email and/or Internet use.

Legal Discovery Benefits of Using Proofpoint Email Archiving

The growing cost of e-discovery, compounded by new regulations such as the Federal Rules of Civil Procedure (FRCP), has changed the way businesses must deal with email. To be prepared for legal discovery, a business must know where all their email data is stored, and be able to search through and retrieve that data in a short period of time. They must also apply a consistent email retention policy, and have a way to enforce a litigation hold by preventing data from being deleted if necessary

For companies that allow PSTs and rely on backup tapes to store historical email, both the cost and time involved in meeting these requirements can be very high. Exposure to legal risk is also significant, with missing or corrupt data resulting in spoliation of evidence. This can lead to costly fines, guilty verdicts and damaged reputations.

The on-demand Proofpoint Email Archiving™ solution makes it easy to respond to e-discovery requests and meet the requirements of the FRCP by:

- Storing all email in a central repository with real-time search from a browser interface and a simple retrieval process.
- Enforcing consistent retention policies and litigation holds.
- Allowing legal counsel to conduct advanced searches for early case assessment and full e-discovery requests.

Without an archiving system with appropriate search and discovery capabilities, these requests can add up to a great deal of time, effort, and expense on the part of the IT department. According to Osterman Research, the IT department in a typical large organization spends five hours per 1,000 users per week performing backups, recovering users' deleted emails and dealing with other backup and archiving-related tasks. That works out to approximately $10 per user per year on labor alone. For smaller organizations, Osterman Research estimates that cost can go up to $34 per user per year on just the labor involved in managing backups and archiving.

In the case of litigation, the costs can rise even more dramatically. An employee discrimination suit known as Zubulake vs. UBS Warburg is a great example of this. UBS Warburg archived outgoing and incoming email for their registered traders on optical disk, with no effective means of searching. When the Zubulake discovery request sought internal mails stored on backup tapes, UBS Warburg was forced to pay the cost of recovery, despite the fact that recovery costs for a sample set of email on five initial backup tapes cost $19,003.43, or about $4,000 per tape. A second round of discovery requests resulted in costs of more than $100,000, before related litigation fees—costs that UBS Warburg, the defendant in the case, was once again responsible for covering.

Cost isn't the only concern when retrieving data for a discovery request. In most cases, a strict time limit is placed on when data must be produced. For example, the SEC generally requires that requested email be produced within 48 hours of a request. Failure to produce requested email in a reasonable timeframe can result in significant fines, as in a case involving J.P. Morgan Chase & Co. The investment banking firm was fined $2.1 million when they failed to produce all the emails sought because backup tapes could not be found in storage facilities, other tapes were damaged or contained errors, or backup tapes were not made for some periods.

While you might think that the best answer to these issues is to simply delete email on a regular basis, there are problems with this assumption. In the case of litigation, seemingly unimportant email messages can often support a company's claims of innocence. A deleted email trail can not only weaken an organization's defense, but it can also lead to a presumption of guilt, potentially costing a business millions in fines and settlements and causing immeasurable damage to corporate credibility.

Without an archiving discovery system, it is also difficult to limit searches for appropriate data before presentation to litigators, creating opportunities for unnecessary data to be exposed. Ultimately, the cost of innocence can be extremely high for organizations that do not proactively manage email usage and archiving.

Regulatory Compliance

In recent years, the archiving of email messages has become a business requirement driven by numerous federal and state regulations including Sarbanes-Oxley , SEC 17a 3-4, HIPAA, and NASD rules. With more than 10,000 regulations on data and record retention currently in force in North America, very few businesses are exempt from some form of regulatory scrutiny.

These regulations are forcing businesses to retain email just as they must retain other formal corporate records—or face penalties that can include significant fines or even criminal charges. As just one recent example (September, 2007), Morgan Stanley & Co. paid $12.5 million to resolve charges with the Financial Industry Regulatory Authority (FINRA) that a former affiliate failed, on numerous occasions, to provide emails to claimants in arbitration proceedings.

With a policy-driven archiving system in place, email can be checked for compliance with regulations, and then retained for the appropriate amount of time based on email content. These solutions can also reduce the risk of inappropriate content being exchanged, as employees can be alerted when an email doesn't comply with company policy.

Storage Management

Nearly every IT department has struggled with the issue of storage management for messaging servers. The pressure to increase storage limits continues to grow as the amount of email sent each day—as well as the size of messages and attachments—increases. This ever-increasing storage demand is driven in part by faster connection speeds, and partly by the fact that email's role as a primary channel for corporate communication continues to expand. This growth is not expected to slow down in the near future; in fact, Radicati Research estimates that corporate email traffic will almost double between 2005 and 2009, going from 64.9 to 120 billion messages a day.

An archiving system, by automatically offloading data into an archive, can dramatically help improve the efficiency of messaging servers, their reliability and the speed with which they deliver messages.

Knowledge Management

Beyond the capacity issues associated with storage management, email has also become the de facto filing system for many enterprises. According to IDC, as much as 60 percent of business-critical information is stored in email and other electronic messaging tools. Everything from sales proposals and marketing plans to competitor profiles, contracts, and personnel files can exist—sometimes exclusively—in an employee's inbox.

Maintaining an archive that allows end-users to easily access and search all previous email can greatly improve productivity. In addition, vital content cannot be deleted by a disgruntled employee; in the event of an employee leaving the company, the trail of information managed by that staff member can be accessed in the future.

Is Your Organization Exposed?

Before embarking on an email archiving strategy, every organization should evaluate their current email set-up to identify key concerns and potential future issues.

Server Backups

By reviewing practices around email storage and backup, a better understanding of the risks your organization may face can be gained.

Virtually all organizations perform some type of regular backup of their messaging servers in order to restore content in the event of a server crash or other problem. Common practice among most organizations is to create daily backup tapes that are recycled and overwritten on a 30-, 60- or 90-day basis. This can be an effective disaster recovery strategy, but it is not a viable archiving strategy, despite common misperceptions.

First of all, this "snapshot" method means that you never get a full view of your email repository. Email that is sent and deleted between backups can't be restored, making legal discovery difficult, if not impossible. And while some organizations may keep a copy of backup tapes for longer-term storage, these tapes are typically very time-consuming and expensive to restore from, as noted previously.

Mailbox Quotas

In the ongoing struggle to deal with excessive email storage demands, most organizations set a per-user quota for email. However, while most organizations have limits on the amount of data that can be stored, very few have enforced time limits on how long things can be kept.

A per-user quota system can deal with basic storage management issues. However, it exposes an organization to a number of risks. With so much business-critical data residing within email stores, end-users will often find other ways to archive their data. The result is confidential business data stored in multiple locations (often as PST files) with no record of these files and no way to easily retrieve them.

Regulatory Compliance Benefits of Using Proofpoint Email Archiving

From Sarbanes-Oxley to SEC rules, numerous legislative requirements have been introduced that dictate how electronic records are retained and retrieved. Organizations that fail to meet regulatory compliance requirements can face significant risks including large fines and prison sentences, plus serious, long term damage to their corporate reputations.

The on-demand Proofpoint Email Archiving solution was designed to meet the most stringent regulatory compliance requirements with:

- Policy-driven archiving that allows businesses to easily customize and enforce a consistent email retention policy.
- Supervision tools that allow businesses to implement a systematic and flexible supervision process for selecting and reviewing the content of electronic messages.
- Real-time search through a web-based user interface, allowing compliance staff to easily meet audit and discovery requirements.
- Guarantees that records cannot be deleted or altered after archiving as well as data authenticity measures such as digital fingerprinting, a full audit trail of user activities, and multiple copies of all data stored on SEC 17a-4 compliant storage.

Email Storage Management Benefits of Proofpoint Email Archiving

As email volume and attachment sizes continue to grow, the burden on storage also increases. Since corporate email servers weren't designed to store large volumes of data for extended periods of time, overloading Exchange can result in significant performance issues and prohibitively long backup windows.

Enforcing tighter email quotas can relieve this issue, but that often leads to an even bigger problem as end users save email data in personal folders or PST files. This simply shifts the storage problem to a different location while increasing your organization's exposure to legal risks.

By securely storing a copy of every email sent and received, Proofpoint's email archive can address these issues in multiple ways:

- Stubbing technology replaces storage-intensive attachments from Exchange with a link to the archived file, allowing IT to reduce the message store by up to 80 percent.
- A smaller Exchange message store means improved server performance, shorter Exchange backup times, and fewer demands on IT.
- With end user access to archived data, businesses can eliminate the use of PSTs while providing a virtually unlimited mailbox size.

Key Issues to Consider When Looking at Archiving

Email Policy Issues

The basis for a good archiving system—one that reduces an organization's exposure to risk and puts it in compliance with regulations—is a good policy. Organizations that don't develop, communicate and enforce formal policies that establish acceptable email behavior and storage guidelines put both their employees, and the organization itself, at serious risk of fraud, lawsuits and loss of confidential data—not to mention the risks of reputation damage, loss of business, and decreased productivity.

To effectively manage the risks of corporate email, businesses need to develop a set of formal policies to guide the use of email. An effective policy will provide specific rules for the acceptable use of email, addressing the use of business email for personal reasons, the forwarding of confidential documents, and acceptable language and content, among other things. A policy should also clearly identify required retention periods and any email monitoring processes.

Developing a policy from scratch can be challenging, but there are a number of resources available on the Web to help get an organization started. The Electronic Communications Compliance Council recently made available a Policy Builder to help businesses create an electronic messaging policy. This free tool can be accessed on the Council's Web site (http://www.TE3C.org), providing a comprehensive policy template that organizations can customize to meet their specific requirements. The policy can then be downloaded as a PDF document and distributed to staff.

To ensure that staff fully understands the policy guidelines, email policies should be made available and easily accessible to all employees. This could mean including it in employee handbooks or on company intranets. All staff should be required to review, sign and submit a copy of the policy to a manager or human resources staff. In addition, some companies are now taking the step of asking employees to sign a copy along with their employment contract.

With a corporate policy in place that outlines retention and deletion periods, it is usually left to the IT department to find a way to enforce that policy. Depending on how detailed the policy is, this can be a very complicated process. For example, some policies may apply only to email sent between two specific departments (i.e., between financial analysts and broker-dealers). Having a policy-based archiving system that was designed to deal with this type of situation—and that automatically enforces that policy—can save IT a great deal of time and headaches. Ideally, an archiving solution will allow non-technical staff with appropriate administrative rights to access and make changes to the policy directly. This type of direct access makes it much easier for the policy to be updated.

Data Security Concerns

When considering how and where to archive your organization's most confidential data, security is of critical importance. Numerous recent security breaches have highlighted how easily data can be lost in transit or can be stolen directly from storage facilities, particularly when stored in tape form. Reinforcing this point, Proofpoint's March 2008 survey on enterprise data loss prevention issues (see http://www.proofpoint.com/outbound) found that more than a quarter (27%) of US companies had investigated the exposure of confidential, sensitive or private information via lost or stolen storage media or mobile devices in the past 12 months.

Many organizations decide to maintain data in-house on the basis that it is more secure; however, this may not be the case. In fact, there is some evidence that shows that data may be more at risk from internal sources than from external attacks. According to the 2005 Global Security Survey released by the Financial Services Industry practices of the member firms of Deloitte Touche Tohmatsu (DTT), internal attacks on information technology systems are surpassing external attacks at the world's largest financial institutions. Specifically, 35% of respondents confirmed encountering attacks from inside their organizations within the previous 12 months compared to 26% from external sources.

Ongoing Management Considerations

Although the selection and implementation of an email archiving solution typically falls to IT, the drivers behind the need for archiving are other business units within the organization—not IT. It is crucial to find a solution that is user-friendly and that allows those business units to play an active role in maintaining the system. An archiving solution should not be so reliant on IT that compliance officers or legal counsel cannot conduct searches or make changes to the business-related or record management retention policies on their own.

For example, if your compliance officer decides to update your policy on a regular basis by adding new keywords to the unacceptable content list, it makes more sense for this to be a task they can conduct without the help of IT. In the case of legal discovery, many archiving solutions will allow legal counsel to conduct searches without the help of IT, making the process faster and easier for both departments.

Email Archiving Options: In-house, Outsourced or Hybrid?

There are three main types of archiving solutions available. The first—the in-house option—will involve the purchase and installation of storage hardware and software for policy enforcement. The second option is to contract with an outsourcer or application service provider (ASP) that provides archiving as a hosted service. Finally, businesses can deploy a hybrid solution that combines certain elements of the in-house and outsourced models. Understanding the differences between these solutions is crucial in determining what is best for your business.

On-premises or In-house Archiving Solutions

To deploy an email archiving solution in-house, an organization must define requirements, develop or purchase appropriate software, and buy the needed hardware. With the large amount of email data that most organizations send and receive, archiving requires a significant amount of storage hardware.

In-house email archiving solutions typically use a dedicated, server-based approach that copies all email from the message store into an archive. Some solutions also require that software be installed on all PC clients to facilitate searching and retrieval. In-house solutions offer a high level of control and data security, as well as convenient integration with other systems in the organization's existing infrastructure. However, these solutions can be costly to acquire and often require dedicated, skilled personnel to maintain.

When considering an on-premises email archiving solution, organizations should also consider the additional infrastructure, maintenance and facilities costs associated with deploying duplicate systems in remote locations, if they want to ensure true disaster recovery capabilities.

Hosted Archiving Solutions

An alternative to the in-house approach is to choose a hosted solution. This allows a company to archive their data at a third-party location, reducing the burden on internal IT resources. Outsourcing also allows a company to avoid the substantial cost of buying hardware and software, as well as the inconvenience of maintaining an archiving system. However, a serious disadvantage with some hosted solutions is a lack of data security. By storing confidential email data at an external location, a business may open itself to security breaches or Privacy Act concerns. In many hosted solutions, archived data is not stored in encrypted form, posing an even greater risk. In addition, without direct integration with the organization's email server, management of archives can be an additional challenge.

SaaS Hybrid Archiving Solutions

A third, emerging, approach is the SaaS (Software-as-a-Service) hybrid model. The typical setup involves an appliance installed at the customer's site, combined with secure storage managed "in the cloud" by a third-party provider. In some cases, encryption is performed before the data leaves the customer location, ensuring the content of archived email can never be accessed from outside the customer's own network. The hybrid approach combines the convenience of a hosted solution with the more robust features and security of on-premises solutions.

The hybrid model is based on the idea that customers want security and easy integration, but also wish to avoid the high costs and inconvenience of acquiring and managing large amounts

of storage. (And, of course, storage costs are not the only consideration. In-house solutions typically require high levels of administration, maintenance, and ongoing support.) As organizations better understand the long-term costs and maintenance required to archive email, the hybrid model is likely to become a common approach.

Conclusion

Clearly, email use within the corporate environment will only continue to rise. The Radicati Group stated that worldwide email traffic increased by 35 percent in 2004, totaling 76.8 billion messages per day. Corporate emails accounted for 83 percent of this traffic. If left unchecked, corporate email can leave a business vulnerable.

With regulatory compliance, legal discovery and storage management concerns growing, the question is not *whether* your organization will need an archiving solution, but rather, *when* it will need one. Starting now to understand the key risks, rewards and reasons for archiving will put you in a better position to make the right choice when the time comes.

About Proofpoint, Inc. and Proofpoint Email Archiving

Proofpoint provides unified email security, data loss prevention and email archiving solutions that help enterprises, universities, government organizations and ISPs defend against spam and viruses, prevent leaks of confidential and private information, encrypt sensitive emails and comply with regulations that affect email use. Proofpoint's products are controlled by a single management and policy console and are powered by Proofpoint MLX™ technology, an advanced machine learning system developed by Proofpoint scientists and engineers. Proofpoint solutions can be deployed in hosted service, hardware appliance, virtual appliance, software and hybrid models, for maximum flexibility and scalability.

Proofpoint Email Archiving is a SaaS hybrid solution that lets organizations easily access, search and retrieve archived data in real-time from Proofpoint's secure, state-of-the-art storage infrastructure. With industry-leading customer service, technology and expertise, Proofpoint offers customers a complete, worry-free way to meet email archiving, legal compliance and Exchange storage management needs.

For Further Reading

Proofpoint offers a variety of free educational whitepapers that further describe the risks associated with outbound email and the policies, processes and technologies that can be used to reduce those risks. Visit our online resource center at **http://www.proofpoint.com/resources** for the latest information.

©2008 Proofpoint, Inc. All rights reserved. Proofpoint, Proofpoint Email Archiving, Proofpoint Secure File Transfer, Proofpoint Protection Server, Proofpoint Messaging Security Gateway, Proofpoint on Demand, Proofpoint MLX, Proofpoint Content Compliance, Proofpoint Regulatory Compliance, Proofpoint Network Content Sentry, Proofpoint Secure Messaging and Proofpoint Digital Asset Security are trademarks or registered trademarks of Proofpoint, Inc. in the US and other countries. Version 06/08 - Rev A

For More Information

Proofpoint, Inc. US
892 Ross Drive
Sunnyvale, CA 94089
USA
P 408 517 4710
F 408 517 4711
E info@proofpoint.com
www.proofpoint.com

Proofpoint, Inc. Canada
60 Adelaide Street East, 9th Floor
Toronto, Ontario M5C 3E4
P (416) 366-6666
F (416) 366-6667
E info@proofpoint.com
www.proofpoint.com

Proofpoint, Inc. EMEA
The Oxford Science Park,
Magdalen Centre
Robert Robinson Avenue
Oxford, UK
OX4 4GA
T +44 (0) 1865 784808
F +44 (0) 1865 784809
E info@proofpoint.com
www.proofpoint.com

Proofpoint, Inc. APAC
56 Berry Street
North Sydney
NSW 2060
Australia
P +61 02 9455 0289
F +61 02 9455 0001
E info@proofpoint.com
www.proofpoint.com

Proofpoint Japan K.K.
906 BUREX Kojimachi
Kojimachi 3-5-2, Chiyoda-ku
Tokyo, 102-0083
Japan
P +81 3 5210 3611
F +81 3 5210 3615
E sales-japan@proofpoint.com
www.proofpoint.co.jp