

Key Issues in Improving Your Messaging Capabilities

An Osterman Research White Paper

Published September 2009

SPONSORED BY



Why You Should Read This White Paper

Email is critical to both users and the organizations that employ them. For example, a recent Osterman Research survey found that email is considered important or extremely important by 97.6% of individuals in larger organizations in the course of doing their work – 99.2% anticipate email will be this important to them in 2010. By contrast, other communications tools are viewed as much less important than email:

- Phone (88.8% view as important/extremely important in 2009, falling to 84.8% in 2010)
- Instant messaging (41.6% in 2009, 58.1% in 2010)
- Web conferencing tools (41.6% in 2009, 61.6% in 2010)
- Twitter (6.4% in 2009, 13.7% in 2010)

In short, despite the growth in alternative communication tools, email continues to remain a critical capability and it is becoming more so.

EMAIL MANAGEMENT IS NOT PLEASANT

However, email management is fraught with difficulties. Email systems are often an assemblage of multiple vendors' point solutions for providing basic message transfer capabilities, malware filtering, spam filtering, archiving, encryption, policy management, monitoring, mobility and other functions. Many organizations have hundreds or thousands of Message Transfer Agents (MTAs) in the backbone to handle large volumes of email messages that need to be sent to customers or prospects on a timely basis. A large proportion of emails that are sent by automated systems are never archived, putting an organization at risk of non-compliance. The result is that infrastructure costs are higher than they need to be, policy management becomes fragmented and inconsistent, relationships must be maintained with large numbers of vendors, power requirements are driven up, and IT staff spend more time managing the email infrastructure than they should.

What organizations need, then, is the ability to manage their email infrastructure more efficiently and at lower cost. They need to be able to replace a sea of MTAs with a more streamlined capability that provides higher throughput and easier maintenance. They need to be able to comply with the growing body of regulations that require email preservation and appropriate management of that content. And, given that IT labor is the largest single cost in managing an email system, they need to minimize the amount of time that IT spends managing the infrastructure.

ABOUT THIS WHITE PAPER

This white paper discusses the key problems in managing email systems, including compliance, migration, archiving, maintaining point solutions and the cost of managing these capabilities. It also provides some advice on what organizations should consider to improve the efficiency and lower the cost of their email capabilities. Finally, it discusses the offerings from ColdSpark, the sponsor of this white paper, and how its solutions can address the most important issues facing email managers.

Messaging Problems Organizations Have Today

Businesses and non-commercial organizations of all sizes experience a number of problems in managing their messaging infrastructure, but larger organizations experience the most difficult, onerous and expensive problems. The key issues that we have identified are discussed below.

COMPLIANCE

Regulatory and legal compliance obligations are increasing in terms of the severity of the penalties associated with being non-compliant. Further, given the growing number of obligations, the tools that can generate electronic content and the venues where this data may be stored, compliance is becoming more difficult and more expensive to manage over time. Among the more important statutory requirements with which organizations must comply are:

- **Sarbanes-Oxley**
The Sarbanes-Oxley Act of 2002 – sometimes called the “Corporate Reform Act” – was enacted following corporate accounting and reporting scandals involving large public companies such as Enron, Global Crossing and WorldCom. This Act has a number of different components, focusing on areas such as corporate governance, financial reporting and disclosures, financial auditing, and the adequacy of the internal controls that ensure the accuracy and integrity of the reported financial results. This Act also contains significant criminal penalties for failure to comply. It holds corporate officers criminally liable for the actions in a company – an attribute that has ensured that this Act has gotten board-level attention in most large companies and in many smaller firms as well.
- **Health Insurance Portability and Accountability Act**
The Health Insurance Portability and Accountability Act (HIPAA) of 1996 addresses the use and disclosure of an individual's health information. It defines and limits the circumstances in which an individual's protected health information (PHI) may be used or disclosed by covered entities, and states that covered entities must establish and implement policies and procedures to protect PHI. Penalties for violations are up to \$25,000 and \$1.5 million, depending on when the violations occurred. Further, an individual who knowingly obtains or discloses individually identifiable health information may face a criminal penalty of up to \$50,000 and up to one-year imprisonment. There is a specification for encryption of health information communicated over any network for which the transmitter cannot control access (45 CFR Part 142.308[d][1][ii]).

As part of the American Recovery and Investment Act of 2009 (ARRA), the provisions of HIPAA have been significantly expanded. A key component of ARRA is the Health Information Technology for Economic and Clinical Health Act (HITECH) that includes an expansion of HIPAA to encompass business partners of entities already covered by HIPAA like pharmacies, healthcare providers and others. The new HIPAA will now include attorneys, accounting firms, external billing companies and others that do business with covered entities. While these business associates were accountable to the covered

entities with which they did business under the old HIPAA, these associates are now liable for governmental penalties under the new law.

Further, the penalties for HIPAA violations have been expanded dramatically. For example, if a covered entity or one of their business associates loses 500 or more patient records, they must notify HHS and a “prominent media outlet” to let them know what has occurred. Fines for violations can now reach as high as \$1.5 million per calendar year.

- **Gramm-Leach-Bliley Act**

The Gramm-Leach-Bliley Act requires that financial institutions protect information collected about individuals, including names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers. The Act gives authority to eight federal agencies and the states to administer and enforce the Financial Privacy Rule (16 CFR Part 313) and the Safeguards Rule (16 C.F.R. Part 314). The wide-ranging Safeguards Rule mandates what companies should include in their written information security plan and how to secure this information, including using tough-to-crack passwords and encrypting sensitive customer information when it is transmitted electronically via public networks.

GLBA also addresses steps that companies should take in the event of a security breach, such as notifying consumers, notifying law enforcement if the breach has resulted in identity theft or related harm, and notifying credit bureaus and other businesses that may be affected by the breach.

- **Payment Card Industry Data Security Standard**

The Payment Card Industry Data Security Standard (PCI DSS) encompasses a set of requirements for protecting the security of consumers’ and others’ payment account information. It includes provisions for building and maintaining a secure network, encrypting cardholder data when it is sent over public networks and assigning unique IDs to each individual that has access to cardholder information.

- **Other statutory compliance obligations**

In addition to the requirements noted above, there are a large number of other important regulations that impact organizations in various industries, including Regulation S-P, a Securities and Exchange Commission (SEC) rule that requires the SEC and a variety of other US federal agencies to implement safeguards to protect non-public consumer information and to define standards for financial services firms to follow in this regard; Red Flag Rules that require financial institutions and creditors to implement a program to detect, prevent, and mitigate instances of identity theft; US state rules, such as S.B. 1386 that requires the disclosure of data breaches for California residents; and the Family Educational Rights and Privacy Act of 1974, which is focused on protecting the privacy of students’ education records, includes provisions for how states can transmit data to Federal entities.

- **Legal obligations**

E-discovery is becoming much more important in the context of civil litigation – for example, roughly three out of four discovery orders today require email to be produced as part of the discovery process. E-discovery today represents 35% of the total cost of

litigation, and companies that fail to produce emails in a timely or appropriate manner face the risk of paying millions of dollars in sanctions and fines, not to mention loss of corporate reputation, lost revenue and embarrassment. The new amendments to the Federal Rules of Civil Procedure (FRCP) that went into effect on December 1, 2006 have raised the profile of Electronically Stored Information (ESI) dramatically, requiring organizations to preserve electronic content in email systems, document repositories, on file servers, on individual machines and in any other venue that might house corporate records.

It is also important to note that while many organizations have deployed email archiving, outbound content filtering and other tools in their email infrastructure to help them manage their compliance obligations for email, a significant proportion of messages are generated by automatic systems. For example, a customer relationship management system or a billing system can generate millions of emails each day that will never pass through the primary corporate email system, yet they contain content that an organization must manage in accordance with their compliance obligations. These types of systems can be used to send financial data, stock research reports, billing notifications, airline travel update notifications and other pertinent and timely information to customers and prospects. Those emails that contain business records or other content that should be preserved or managed in accordance with compliance requirements must be handled appropriately.

MANAGING POINT SOLUTIONS

Most organizations' email infrastructure has grown slowly over time: email servers were deployed along with anti-virus and anti-spam servers or appliances, followed by archiving servers, data leak protection systems, encryption servers, various other gateways and endpoint solutions, monitoring systems, mobile messaging servers and the like.

For example, in a major survey of messaging and Web security practices published by Osterman Research in June 2009, we found that only one-fifth of the respondents indicated that they use a consolidated, comprehensive, centrally managed messaging security solution. The vast majority are dealing with separate vendors for their various best-of-breed solutions. Yet, when we examine what organizational decision makers want, the number of respondents who prefer a consolidated, comprehensive, centrally managed messaging security solution is twice as high.

While managing point solutions is particularly difficult for security capabilities given the large and growing number of servers and appliances that must be managed for anti-malware and anti-spam services, point solutions present difficulties for all aspects of email management. Managing a set of point solutions from different vendors makes platform management more difficult because different vendors must be managed along with different upgrade cycles and the incompatibilities that arise when using multiple vendors' solutions. This increases the amount of IT labor that must be devoted to managing the email infrastructure, driving up costs in the process. IT labor is a particularly important consideration, since it typically represents roughly one-half of the lifecycle cost of an email system.

MIGRATION

Migration from one messaging system to another can be difficult and expensive, even when migrating from one version of a vendor's solution to another. For example, upgrading from one version of Microsoft Exchange – the most widely messaging system in corporate North America – to a more recent version is not *really* an upgrade. Because an “upgrade” cannot be performed in place, new servers must be set up with the new version of Exchange and data migrated to them. In essence, then, this is akin to a “rip-and-replace” model that is expensive and time-consuming for IT to carry out. The difficulty of migration prevents organizations from being as nimble as they otherwise could be.

ARCHIVING

Email archiving is, arguably, the most versatile messaging-related application and the one that impacts that greatest number of different functions within an organization with real business value. For example, an email archiving system (or one that manages more electronic content than just email) can reduce storage costs, speed the process of responding to an e-discovery or regulatory request for information, eliminate the end-user impact of mailbox-size quotas, make disaster recovery easier, and can improve email server performance.

Email archiving is a best practice for virtually any organization serving any industry. Preservation of important records within email or other content stores is a business necessity, one that decision makers are beginning to take more seriously over time. As a result, the email archiving market is growing – Osterman Research expects the installed base of corporate archiving seats in North America to grow from its current 56 million seats to 113 million seats by 2012.

COST

Email systems are expensive to deploy, manage and upgrade. For example, Osterman Research has developed a number of cost models focused on the total cost of ownership for email systems and found that the cost for managing leading systems like Microsoft Exchange or Lotus Notes/Domino can range from \$27 to \$30 per seat per month for a 1,000-user organization. While many decision makers focus on the hardware acquisition and software licensing costs, labor typically constitutes anywhere from 47% to 53% of the total three-year cost of ownership, while downtime runs anywhere from 14% to 19% of the total.

The high cost of email management is driven by a number of factors, not least of which is the fact that larger organizations simply have a great deal of infrastructure to maintain, coupled with the fact that IT staff have a number of different point solutions to maintain that can add significantly to their total workload.

What Should Organizations Do?

There are a variety of things that organizations should do to more effectively and efficiently manage their email infrastructure. We have condensed these action items into the following four key focus areas.

DEVELOP POLICIES FOCUSED ON COMPLIANCE

Any organization – regardless of its size or the industry in which it operates – should develop policies to comply with the growing set of regulatory and legal obligations surrounding email and other types of messaging and collaboration. These policies should be focused on:

- **Archiving**
Every organization should establish policies focused on data retention and deletion, including the specific types of data that should be retained, the time periods for retention, and when data can safely be deleted. Policy development will focus on legal counsel's opinions and court precedents and must continually be updated.
- **E-discovery**
Closely related to archiving is the impact of e-discovery and the critical need to develop policies that are focused on helping an organization to comply with its discovery and legal obligations. Because the cost of just one e-discovery effort using backup tapes can total in the millions of dollars, a sound e-discovery policy and deployment of the right technologies to enforce it can have a dramatic and positive impact on an organization's bottom line.
- **Encryption**
The ability to encrypt sensitive content during transmission and at rest is already a requirement under HIPAA, GLBA, S.B 1386 and a growing number of other state and federal requirements. If an organization suffers a data breach and the data was not encrypted, remediation costs can total in the millions of dollars, not to mention the loss of reputation, lost sales and other consequences that can arise from even a single breach of data.
- **Other capabilities**
Decision makers must also focus on other policies dealing with capabilities like Twitter, Facebook, other social networking tools, personal Webmail accounts and other systems that can have an impact on an organization's network infrastructure.

MANAGING CAPABILITIES HOLISTICALLY

Holistic messaging management is a key requirement, but never more so than during periods of economic difficulty. To the extent possible, organizations should use a single management console to manage all of their various platforms and policies. They should also integrate and consolidate platforms as much as they can to eliminate the number of point solutions in their infrastructure and to reduce the number of different vendors in use. Doing so will allow an organization to lower its costs, improve the efficiency of its IT staff and achieve economies of scale that are not available in environments in which a large number of point solutions are used.

DEPLOY MIGRATION-FRIENDLY CAPABILITIES

Another key consideration is to deploy capabilities that will permit migration from one platform to another with as little pain as possible. While migration is not a frequent occurrence (nor does it need to be) the availability of an infrastructure that makes migration as painless as possible will allow an organization to move from one system to another in order to achieve new functionality and/or lower the cost of email management.

DRIVE AS MUCH COST OUT OF THE SYSTEM AS POSSIBLE

Email is critically important and has achieved “utility-like” status in most organizations, but it is expensive to manage. One of the key drivers for improved messaging management, therefore, is to drive as much cost out of the infrastructure as possible. This is important anytime, but particularly during economic slowdowns when most IT budgets are either static or are being cut. There are various ways of cutting email-related costs as discussed above. Most organizations will realize significant IT labor savings from consolidation of their various point solutions, and they will avoid extremely costly e-discovery and regulatory compliance efforts if they archive and manage their content properly. Longer term, significant cost savings can also be realized through the ability to more easily migrate from one system to another, even if an organization migrates only to the newest version of the same vendor’s platform.

IT SOUNDS SIMPLE, BUT...

While most would agree that these are things that organizations should do, actually implementing these changes doesn’t just happen. It takes the right mix of technology, appreciation of the issues and problems imposed by the status quo, and the willingness to make changes that will dramatically improve performance throughput.

Who is ColdSpark?

CORPORATE OVERVIEW AND OWNERSHIP

ColdSpark, acquired by BakBone Software in 2009, is a leading provider of email infrastructure solutions focused on the enterprise market. The company is focused on streamlining the flow of email in large organizations by eliminating the sometimes thousands of MTAs used to send email, replacing them with its SparkEngine Email Transport Platform.

Although ColdSpark is focused heavily on the financial services industry, serving many of the world's largest financial services companies such as JP Morgan, the company is staking a claim in the healthcare industry with solutions tailored to this vertical. Their customer roster also includes many of the top global investment and retail banks, healthcare payors like Blue Cross Blue Shield of Tennessee and many other companies in the entertainment and hospitality industries such as Fairmont Hotels.

WHAT COLDSPARK IS NOT

ColdSpark is an interesting company because its offerings cut across a variety of capabilities, including email delivery, archiving, customer relationship management and other focus

areas. It is important to note that aside from ColdSpark not being “that email blast company”, the company does not offer:

- **A replacement for Microsoft Exchange**
ColdSpark solutions replace the vast array of MTAs that are used by many companies for high volume message delivery, but they do not replace Exchange servers or other groupware functionality.
- **An archiving solution**
While ColdSpark technology facilitates the archival of business records in email, the company does not provide the underlying email archiving or discovery technology.
- **An email blast provider**
Here again, ColdSpark facilitates the high volume delivery of email for providers that must send multiple millions of email messages in a short amount of time, but they are much more than an email delivery provider.

WHAT SOLUTIONS DOES COLDSPARK ENABLE?

ColdSpark offers a variety of solution sets designed to streamline email processes and reduce their cost. These solution sets include:

- **IT Governance and Compliance**
ColdSpark’s IT Governance and Compliance solutions integrate with, not replace, existing systems, such as email archiving, to improve their performance and enhance an organization’s overall compliance readiness. These solutions improve an organization’s overall compliance and litigation support by providing an automated, policy-based approach to email archiving. These solutions also allow organizations to integrate email from applications, such as CRM and marketing applications, into their existing email archiving solution regardless of whether this email travels through host-based email systems, such as Exchange. Finally, these solutions allow organizations to completely leverage their email channel to improve customer retention, acquire new customers and reduce operational costs in a compliant fashion.
- **Customer Care**
ColdSpark’s Customer Care solutions provide organizations with a 360 view into all email communications with customers, prospects and partners. This allows organizations to more effectively leverage email communications as a vehicle to attain new customers, improve existing customer loyalty and improve partner efficiencies. For example, Customer Care solutions can be deployed to help a brokerage distribute large volumes of research publications to its clients within a tight time window each weekday, or to provide secure emails to healthcare patients in lieu of paper-based billing statements. Ultimately these solutions increase revenues through improved targeting and relevance to customers while providing reports, analysis and forensic tools to evaluate the overall effectiveness of individual campaigns or communications or overall effectiveness of email as a communication channel.

- **Archiving Management**
ColdSpark's Archiving Management solutions provide unmatched flexibility for existing email archiving solutions and infrastructure. By centrally managing email archiving policies, these solutions allow organizations to manage multiple archiving solutions from a single location and with a single set of policies. Organizations can future proof their existing email archiving solution by eliminating MAPI based archiving requirements, eliminating unnecessary future upgrades and costs without costly upgrade or infrastructure changes. They can also automate the migration between email archiving solutions, allowing organizations to select the appropriate solution given current requirements.
- **Services-Oriented Messaging**
ColdSpark provides organizations with a powerful messaging foundation from which they can control and monitor the flow of email, ensuring that compliance and SLA requirements are achieved. ColdSpark refers to this as Services Oriented Messaging and has solution sets to help organizations centralize the creation and monitoring of all email policies while integrating with existing email solutions, such as anti-virus, anti-spam and data loss prevention solutions, extending the capabilities of these solutions. Services Oriented Messaging solutions increase the performance, availability and scalability of existing email infrastructure and allows organizations to support policies, SLAs and services by business unit or geographical business operations.
- **SalesForce.com Integration**
ColdSpark's SalesForce.com Integration solution allows organizations to use the native email capabilities in their SalesForce.com solution, while efficiently capturing all inbound and outbound messages to the system and directly injecting them into existing email archiving solutions. This allows organizations to gain the full benefits and efficiencies of their SalesForce.com implementation while ensuring regulatory compliance objectives are achieved on all inbound and outbound SalesForce.com emails.

COLDSPARK'S TECHNOLOGIES

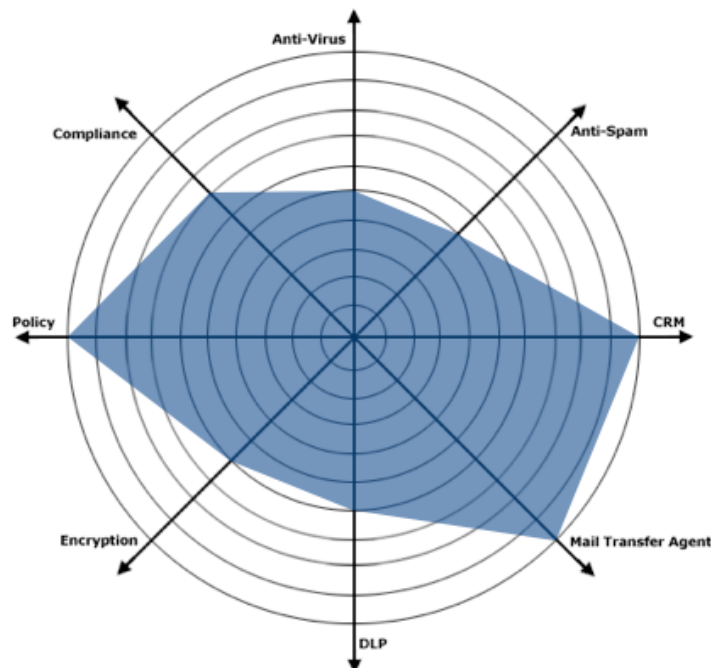
ColdSpark has five basic product offerings that deliver their broad range of solutions:

- **SparkEngine Mail Transport Platform**
Provides a scalable, extensible and powerful platform for bi-directional delivery and all SMTP mail processes plus policy control for routing and message management for all mail services, including application support, content interrogation, security, archiving, and encryption.
- **MailFusion Email Automation System**
Offers next-generation capabilities for data-driven email content and delivery, supporting the new generation of highly relevant, personalized correspondence with customers. It also includes feature-rich email marketing tools, comprehensive data management, tracking and analytics, and flexible integration points with critical business applications for customer contact management, publication control and delivery, transactions, and other operational systems.

- **Compliance Catalyst**
Allows organizations to capture, classify and insert messages from any source systems, such as the corporate mail host like Microsoft Exchange, or any of the widely deployed automated systems in an enterprise, such as CRM and custom applications, into any existing archive. By leveraging direct integration with many of the top enterprise archiving products, it can be implemented without requiring changes to existing email and compliance infrastructure.
- **SparkEngine Inbound Processing Manager**
An in-process API application that classifies and acts upon inbound email messages. It can be used with the ColdSpark MailFusion application, or any other automated email or CRM application that requires inbound message handling.
- **Third Party Modules**
While the ColdSpark platform will support integration with any open-source or commercial messaging application, through the ColdSpark Technology Partner Program, organizations can use best-of-breed vendor products and services certified to work with the SparkEngine platform to deploy the best solutions available that adapt to local requirements. Available certified applications include security (anti-spam, anti-virus and reputation), compliance (encryption and archiving) and business automation (CRM and transaction systems).

COLDSPARK'S PLATFORM APPROACH

ColdSpark has approached the broad messaging space in a unique way. Rather than focusing on point solutions, the company has built and deployed a sophisticated platform for messaging suitable to the enterprise. Based on technology capabilities, the figure below shows ColdSpark's breadth and depth of capabilities across the variety of messaging technologies it can manage.



Summary

Email is absolutely vital to the way that most organizations work: it is the primary communications tool, it is the primary file transport tool and, for a growing number of companies, it is the fastest and most efficient way to send vital and timely information. However, email systems are typically not optimized, instead built on a collection of point solutions from multiple vendors for message transfer, security, archiving and other vital functions. This results in less than optimum throughput, higher hardware and software infrastructure costs, and excessive requirements for IT labor.

ColdSpark's solutions are designed to address these problems by eliminating the bottlenecks and costs associated with sometimes thousands of MTAs in an organization. The solutions are designed to integrate various email and other messaging systems so that policies can be managed in a unified way. And, they are focused on streamlining the overall email management process so that costs can be minimized and throughput maximized.

© 2009 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.