WHITE PAPER

Three Steps to Get Started With Email DLP

An Osterman Research White Paper

Published July 2013

SPONSORED BY

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

EXECUTIVE SUMMARY

A February 2013 study found that victims of cybercrime and data breaches not only lose current and potential customers, but are very likely to lose potential investors, as well. The study found that 69% of investors would be "somewhat or very unlikely" to invest in a company that had suffered one or more data breaches. The bottom line is that even a single data breach can carry with it disastrous consequences for any organization.

OVERVIEW

Email is the most commonly used communication channel in most organizations, and it is the primary method by which organizations send files and other sensitive content. This data might include information on employees' health issues or medications; customers' Social Security numbers, addresses or account numbers; students' education records; intellectual property; financial records; embargoed product announcements and the like. Even with detailed policies in place to instruct employees on how to manage this sensitive information in email, mistakes happen and costly data breaches occur.

There is also the potential for intentional misuse of email, such as an employee who sends confidential information to his or her personal email account when planning to leave for a competitor, or an employee who sends sexually harassing or other offensive content to a business partner. Add to this the likelihood that malware will enter an organization and allow cybercriminals to exfiltrate sensitive data or use corporate resources to transmit malware, spam or other content.

Consequently, outbound email must be managed in compliance with corporate policies so that risk is mitigated to the greatest extent possible. What this means is that outbound email must be scanned and its content identified so that appropriate actions can be taken on it. This might mean encrypting some sensitive content automatically, preventing some messages from leaving the organization whether encrypted or not, routing some messages to a supervisor for review before they are sent, scanning outbound content for malware, or doing nothing at all.

In short, outbound email content needs to be properly identified and processed so that corporate policies are followed.

THE PROBLEM WITH TRADITIONAL DLP

Traditional data loss prevention (DLP) solutions created challenges that were difficult to address: high costs, a significant level of configuration and management effort, and a requirement for broad enterprise adoption and commitment. However, leading vendors have now embedded robust capabilities as a built-in component of their email security solutions, making them easily available to enterprises to take their first steps where the risk is greatest. In short, email DLP can be considered the next generation of DLP, but one that is much easier to implement and more integrated with other security tools.

KEY TAKEAWAYS

- Deployment of email DLP is a best practice for any organization to minimize the risk from content leaving an organization in a manner that could be harmful. It is critical to understand that email security is not simply about inbound protection, but also about protecting content that leaves an organization.

- The consequences associated with unidentified and unmanaged content leaving an organization are data breaches of various types that can be very damaging to any organization, both financially and to its long-term reputation.

- Traditional DLP solutions have been expensive and difficult to implement, but this is no longer the case with the new crop of offerings from leading providers that have built DLP directly into the email solution (i.e., no separate deployment

A February 2013 study found that victims of cyber-crime and data breaches not only lose current and potential customers, but are very likely to lose potential investors.

or integration is required, pre-built compliance templates can be leveraged right out-of-the-box, deep content scanning capabilities are included for specialty and legacy formats, identification of both structured and unstructured data, etc.).

- When considering email DLP, it is essential to consider how this can integrate with whatever broader DLP strategy the organization needs to implement as part of a long-term initiative. A failure to do so may require scrapping key elements of a DLP solution that cannot meet all organizational requirements.

- Organizations of all sizes and in all industries should implement a program to manage all of their relevant content sent through email. The ultimate goal should be to accurately identify outbound information and take appropriate actions upon it.

ABOUT THIS WHITE PAPER

This white paper discusses the need to identify and manage outbound content and the steps that organizations should consider in doing so. This white paper also discusses the relevant offerings from McAfee, the sponsor of this document.

WHAT DRIVES THE NEED FOR DLP?

Email data loss prevention (DLP) is the set of software, services and processes focused on managing information that is sent out of an organization through email. Through the use of automated scanning of outbound content, the goal of DLP is to prevent information from leaving an email system in an unmanaged state that could in some way be harmful to the organization. Management of data in this context means identification of each email's content and application of applicable policies to ensure that the information will not violate a corporate policy. This might include automatic encryption of sensitive content before it is sent, outright blocking of content, routing of particular messages to a supervisor for review before being sent, or simply passing through messages that contain no violations of policy.

Data Loss Prevention (DLP) has traditionally been driven by the need to manage outbound content for compliance purposes. While the same need continues, the need for DLP is growing by leaps and bounds as a result of several critical factors that are discussed throughout the rest of this paper:

- The explosion of ingress and egress points for content: the traditional ones that include desktop and laptop computers; but also smartphones, tablets, cloud-based storage and collaboration applications, social media, employees' home computers and other applications and tools.

- The compliance obligation that is becoming more difficult to address as a result of tighter corporate governance requirements, new regulations and the like.

- The need to more carefully manage what is sent through email systems in light of the increasing level of telework and remote work, as well as the greater number of devices employed by these remote employees for sending email.

- The increasingly high cost of data loss.

WHY FOCUS ON EMAIL DLP?

There are a number of reasons to focus on email DLP as a critical best practice in any organization:

- Despite the fact that collaboration systems, file-sharing tools and other non-email systems are used to send information, email remains the dominant channel for corporate communications. For example, an Osterman Research survey conducted in January 2013[i] found that the average corporate email user sends a median of 30 emails per day, or 7,500 emails during a typical workyear.

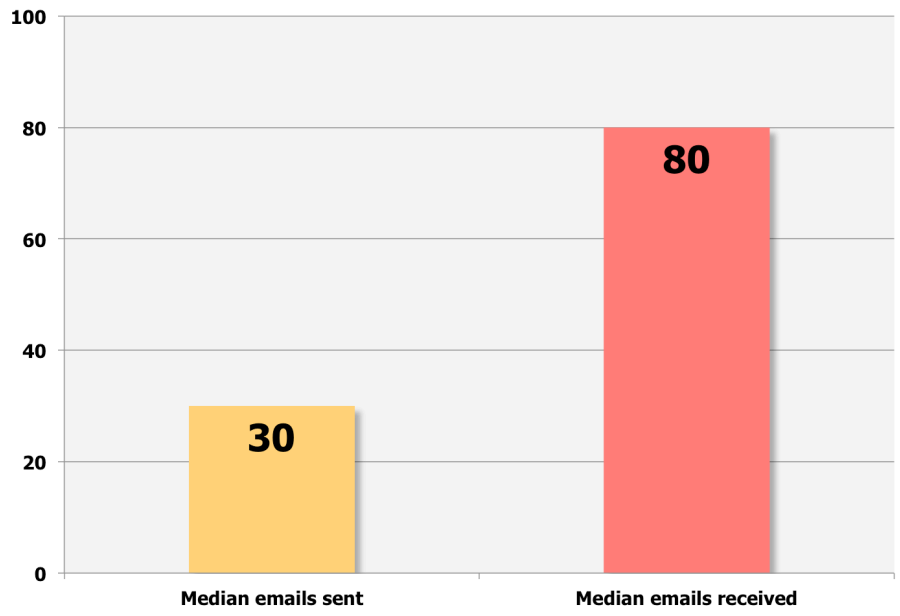
There are a number of reasons to focus on email DLP as a critical best practice in any organization.

Moreover, the same survey found that 90% of email users are using email as much or more today than they were 12 months ago, despite the increasing use of alternative forms of communication and collaboration.

- The trend toward telework is creating more geographically distributed teams, meaning that email is sent increasingly outside of corporate networks, thereby creating more opportunity for data breaches as information traverses the Internet. Several studies have found that employers are increasingly open to having their employees telecommute. For example, a study from IDC found that more than three million corporate home offices will be added to the base of US teleworking households through 2015[ii].

- The growing number of devices used to send sensitive and confidential information – company-owned and personally-owned desktop computers, laptops, smartphones, tablets, etc. – is creating more opportunities for data breaches to occur. The Bring Your Own Device (BYOD) trend, in particular, is fueling much of this – an Osterman Research study conducted during Q1/2013 found that most of the iPhone, Android smartphones and tablets in use in corporate environments are personally owned[iii]. The same study found that personally deployed applications are also in common use, exacerbating the problem by creating more egress points for corporate content. The result is that because these devices and applications are under the primary control of the user and not IT, the potential for violations of corporate policy are greater than if these devices were purchased and provisioned by IT.

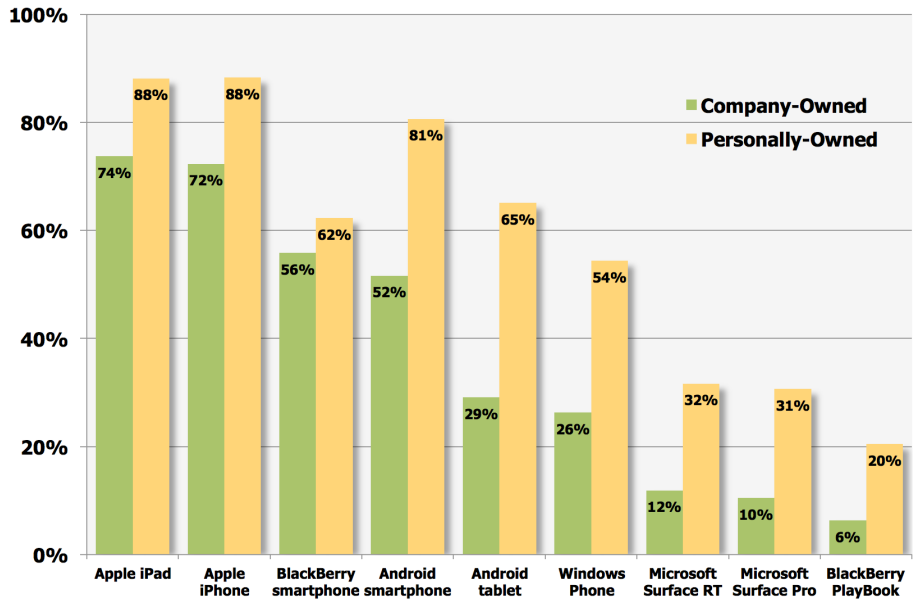
Median Email Volume per User per Workday



Source: Osterman Research, Inc.

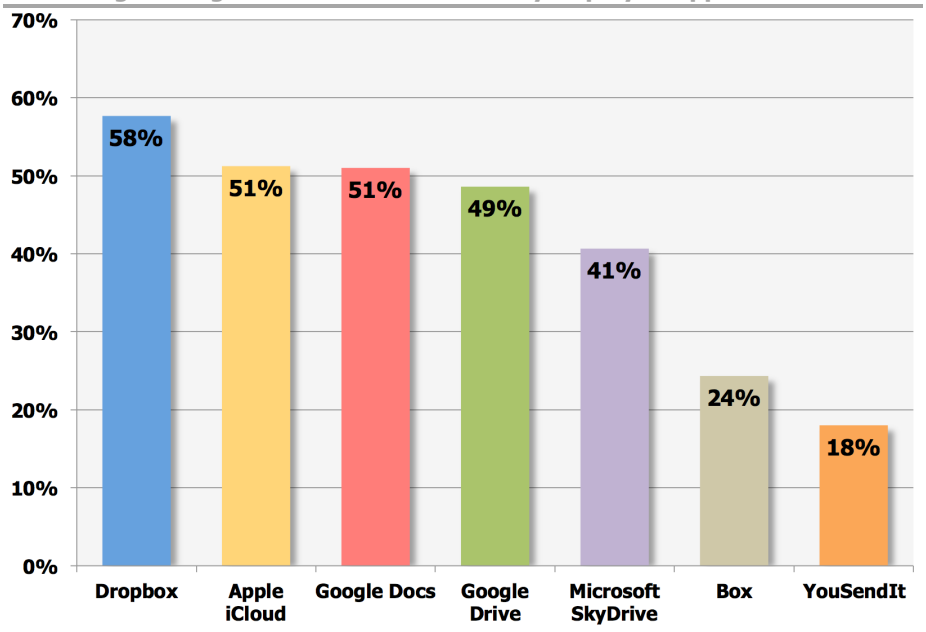
The growing number of devices used to send sensitive and confidential information – company-owned and personally-owned desktop computers, laptops, smart-phones, tablets, etc. – is creating more oppor-tunities for data breaches to occur.

Percentage of Organizations With Mobile Devices in Use



Source: Osterman Research, Inc.

Percentage of Organizations With Personally Deployed Applications



Source: Osterman Research, Inc.

THE TRADITIONAL FOCUS HAS BEEN ON COMPLIANCE

The traditional focus of DLP has been on compliance with statutory obligations to protect data in transit. Among the many such obligations are:

- The **Payment Card Industry Data Security Standard (PCI-DSS)** is a set of strict requirements for protecting the security of consumers' and others' payment account information. PCI-DSS includes requirements for creating and

The traditional focus of DLP has been on compliance with statutory obligations to protect data in transit.

maintaining a secure network and encrypting cardholder data when it is sent over public networks, among other provisions.

- The **Health Insurance Portability and Accountability Act (HIPAA)** mandates that healthcare and other organizations protect sensitive health records of patients and others. Although HIPAA was enacted in 1996, it was generally considered a poorly enforced requirement. However, the Health Information Technology for Economic and Clinical Health (HITECH) Act, followed by the HIPAA Omnibus Rule that became effective as of late March 2013, significantly increased both the scope of HIPAA and the consequences for its violation. For example:

  - The definition of which types of organizations are now subject to HIPAA compliance has been expanded. For example, a cloud provider that stores Protected Health Information (PHI) is now considered a "Business Associate" and must adhere to various HIPAA requirements.

  - Any subcontractor that "creates, receives, maintains or transmits PHI on behalf of a Business Associate, is a HIPAA Business Associate" and so must comply with the HIPAA Privacy Rule, Breach Notification Rule, Security Rule and other requirements.

  - Covered entities must receive "satisfactory assurances" from their Business Associates that PHI is being protected. Business Associates must also receive this from their subcontractors.

  - The HIPAA Security Rule Section 164.306(c) has been clarified with regard to Covered Entities' and Business Associates' requirements to provide "reasonable and appropriate" protection of electronic PHI.

  The US Department of Health and Human Services (HHS) has increased the requirements for protection of confidential and sensitive information, expanded the number of organizations that are subject to HIPAA, and can be expected to levy fines and penalties more frequently than has been the case in the past. For example, the Omnibus rule allows HHS to impose fines ranging from $100 for a "Did Not Know" breach of PHI to $50,000 for a single, uncorrected and willful violation. Fines can reach $1.5 million per year or more.

  Violations of HIPAA rules can be expensive. For example, Phoenix Cardiac Surgery committed several HIPAA violations, including their doctors emailing one another from unprotected personal accounts. The result was a $100,000 fine and a requirement to adhere to a Corrective Action Plan for one year. In another example of high cost of a HIPAA violation, Hospice of North Idaho was fined $50,000 for the loss of a single, unencrypted laptop that contained the records of 441 patients.

- The **Gramm-Leach-Bliley Act (GLBA)** requires financial institutions to protect sensitive and confidential information about individuals, including their names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers. GLBA requires organizations that transmit and store this information to prevent its unauthorized access.

- Forty-six of the 50 US states have data breach notification laws that, to varying degrees, require individuals whose data was lost, stolen or otherwise compromised to be notified about the breach. The only states that do not yet have such laws are Alabama, Kentucky, New Mexico and South Dakota[iv].

- The Australian federal government's Privacy Act 1988 requires that the personal information held by organizations be kept secure from unauthorized access or use.

The Omnibus rule allows HHS to impose fines ranging from $100 for a "Did Not Know" breach of PHI to $50,000 for a single, uncorrected and willful violation.

- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) states that the "nature of the [data protection] safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. The methods of protection should include "technological measures, for example, the use of passwords and encryption."

As a result, the market for DLP in the context of email has been driven largely by a need to comply with external obligations. While these obligations continue to be of critical importance, decision makers are coming to realize that email-focused DLP is important to protect corporate data assets that are not necessarily the focus of specific regulatory obligations. In fact, they are realizing that email DLP is a high priority to protect intellectual property, access to corporate systems, to prevent exfiltration of malicious or sensitive content, etc.

THE CONSEQUENCES OF NOT IMPLEMENTING DLP

There are numerous examples of not implementing email-focused DLP that have caused harm to organizations and their customers, a few of which are provided below:

- In December 2012 and February 2013, data on 818 patients of the Hope Hospice in New Braunfels, Texas was emailed without encryption, violating HIPAA requirements to protect PHI.

- A report published in February 2013 discussed how a partner at Ernst & Young allegedly snuck into the headquarters of Express Scripts Holding Co. and supposedly emailed 20,000 pages of content to a personal account. The case is now being litigated[v]. If the organization had implemented an email DLP solution, this violation could have been prevented by not allowing content to be sent to an employee's personal account and the expense and difficulty of the current litigation could likely have been avoided.

- It was reported in January 2013 that the California-based employee of Reyes Beverage Group had their names and Social Security numbers sent to the personal email account of a Reinhart Foodservice employee in violation of that state's data breach laws[vi]. Here again, an appropriately configured email DLP solution would have either encrypted the content before it was sent or routed it to a supervisor for review before sending because it contained confidential information.

- In October 2012, an employee of the Town Council of Chapel Hill, North Carolina mistakenly attached confidential information to an email that was sent to several of her colleagues on the town council. The email was made available to the public for about one week before the error was corrected[vii]. An email DLP solution would have detected that sensitive information was included in the email and could have notified the sender, routed the email to a supervisor for review, or automatically encrypted the content.

- In April 2012, the South Carolina Department of Health & Human Services suffered a data breach impacting more than 228,000 Medicaid recipients. The breach was perpetrated by an employee who stole the records via email.

The consequences from these kinds of data breaches, of which the list above is but a tiny representation, can range from inconvenience in having to delete emails all the way to multi-million dollar lawsuits. A useful analysis of the costs associated with a data breach has been published by Zurich Insurance[viii], which includes the costs of forensic examination, notification of affected parties, increase in the capacity of call centers, credit or identity monitoring, loss of corporate reputation, legal defense expenditures, fines and penalties, and ongoing audits.

In December 2012 and February 2013, data on 818 patients of the Hope Hospice in New Braunfels, Texas was emailed without encryption, violating HIPAA requirements to protect PHI.

If we assumed that the costs associated with just a single data breach were limited to the provision of credit reporting services and just 40 hours of forensic examination for a breach of 25,000 records, the cost of the data breach would be a minimum of $260,000 based on credit reporting service costs of $10 per user and $300 per hour for forensic examination.

THE NEED FOR LAYERED OUTBOUND SECURITY

In addition to data breaches and other types of data loss caused by accidental or malicious employee behavior, organizations should implement a layered outbound security system to limit the impact of malware infiltration. For example, if malware makes its way into a corporate network via an email attachment, malicious Web site, USB flash drive or some other means, it will likely want to "phone home" to a command and control system of some sort to carry out specific tasks like stealing information, sending spam or to download additional malware. An outbound DLP system can therefore be very useful in limiting the damaging impact of a malware infiltration.

MOST KNOW THEY NEED EMAIL DLP

The majority of electronic communications sent from the typical organization are not managed. This includes email, social media posts, instant messages and other external communications sent by users. Moreover, a significant proportion of application-generated content, representing content as diverse as flight schedules or payment statements, is sent unencrypted or without any other sort of review or management.

As but one example of the dissatisfaction with current email management, most decision makers are not happy with the current state of their email policies as they apply to encryption – just one aspect of email DLP. For example, Osterman Research found in a survey published in August 2012 that only about two in five mid-sized and large organizations find that their policies for encryption of confidential email and attachments meet their needs. Add to this the fact that only about one-half of organizations have automated systems in place to scan outbound content for policy violations, sensitive information, credit card numbers, and information that should be encrypted. The predominant actions with outbound email at such organizations are to automatically apply policy requirements (such as encryption or distribution through a secure channel), or to remind users of corporate policies through a pop-up message[ix]. However, as the table below reveals, while decision makers may intellectually understand the need to encrypt content, most are not taking a DLP approach to encryption of the sensitive and confidential content leaving their organization.

In addition to data breaches and other types of data loss caused by accidental or malicious employee behavior, organizations should implement a layered outbound security system to limit the impact of malware infiltration.

Actions That Occur Based on Automatic Scanning of Outbound Email

Action	%
Email with sensitive/confidential content is automatically encrypted or delivered through a secure delivery mechanism	48%
Users who send email with sensitive/confidential content are reminded of corporate policies (e.g., with a popup message) about sending this type of email encrypted before the email is sent	48%
Email that contains sensitive/confidential content is automatically routed to a compliance officer or supervisor for review before it is sent.	43%
Email that contains objectionable content is flagged, but is sent anyway	28%

Source: Osterman Research, Inc.

Email encryption is but one example of the larger problem with a lack of email management. The expense of procuring, integrating and managing separate

solutions to manage inspection, identification, encryption, blocking and other aspects of email DLP is a significant barrier for companies to implement DLP. The fact that leading vendors are now incorporating these capabilities into the base functionality of email management systems, as well as making capabilities like encryption easier to implement, is making email DLP more cost effective.

THREE STEPS TO PREVENT DATA LOSS VIA EMAIL

Osterman Research recommends a three-step approach in developing a DLP-focused email management plan:

1. **Understand the need to manage email**
   First and foremost, an organization must understand its need to manage the content sent through its email system. While that may seem obvious, not all decision makers are convinced of the seriousness of the issue. As noted earlier, there are a variety of regulatory obligations to encrypt and otherwise scan data as proscribed by HIPAA, GLBA, state data breach notification laws, etc. All organizations, but particularly those that are in heavily regulated industries like healthcare, financial services, energy and others must ensure that sensitive emails are sent securely, that confidential information is not being leaked, that employees are operating within corporate policy guidelines and that malicious content is not leaving the organization.

   Even in the absence of specific regulations, an organization should protect sensitive content from data leakage. For example, confidential financial data sent to analysts in advance of a teleconference to discuss an upcoming earnings report; an embargoed press release sent to the press before a major announcement of an acquisition; or graphics files with new logo designs sent to a marketing department for review are all examples of content that are typically sent through email, but that should be protected against accidental or malicious exposure.

   The fundamental goal for any organization is to protect all data sent via email through the application of encryption, blocking, review, file fingerprinting and other management of data. This should include a focus not only on national or international requirements, but also regional requirements, as well, such as individual states' data breach notification statutes.

2. **Identify what needs to be protected**
   An organization may decide it wants to monitor all content sent through email, or it may decide that just a subset of content is acceptable for monitoring: just the body of sent email, Microsoft Word documents, PDF files, zipped files, embedded images, Microsoft Excel spreadsheets, etc. The solution chosen must be able to protect content to meet today's requirements, as well as any future requirements that an organization might have.

3. **Take a phased approach to deployment**
   Osterman Research recommends a phased approach to the implementation of email DLP: start with the "low hanging fruit" of scanning email content and perhaps the most commonly sent document types for violations of policy. Follow this by later adding in additional content types as needs warrant, such as PDF files, images and other content.

   Alternatively, an organization may opt to implement email DLP for a specific subset of its users, such as traders, HR staff or other employees that deal with confidential information on a regular basis.

   Moreover, we recommend a phased, time-based approach to enforcement, as

First and foremost, an organization must understand its need to manage the content sent through its email system. While that may seem obvious, not all decision makers are convinced of the seriousness of the issue.

well. This might include doing nothing more than monitoring outbound email content as an initial step, followed a few months later by notification to employees when violations are discovered, then followed a few months after that by specific enforcement actions for policy violations.

SUMMARY

Email is a two-edged sword: it is incredibly useful for communications and collaboration, but its ease of use and ubiquity mean that policy violations in outbound email can occur quite easily. These violations can result in significant financial or other losses for an organization, despite the fact that most such violations are accidental in nature. Consequently, all organizations should implement an email DLP solution that will automatically scan outbound email content for policy violations and take appropriate action on those messages.

About McAfee

McAfee Email Protection delivers integrated inbound protection, outbound data protection, and flexibility of deployment models in an integrated, easy-to-use solution. Fueled by McAfee's Global Threat Intelligence, Email Protection defends organizations against inbound threats such as malware, shortened URLs, phishing, graymail and spam. Robust outbound capabilities include encryption and content policy enforcement to keep outgoing data in emails safe from innocent mistakes and bad actors. Additional capabilities include 114+ pre-built compliance templates, deep content scanning of 500+ file types, and data loss prevention technologies. Customers have the flexibility to deploy on-site (virtual appliances, hardware appliances, blade servers), in the cloud (SaaS), or as an integrated hybrid combination of the two.

For more information, please visit www.mcafee.com/emailsecurity.

---

[i] *Results of a Survey With Email Users*, April 2013; Osterman Research, Inc.

[ii] *U.S. Home Office 2011–2015 Forecast: Recovery Drives Interest in IT as Home Office Households Adjust to New Economic Realities,* International Data Corporation

[iii] *Managing BYOD in Corporate Environments*, April 2013; Osterman Research, Inc.

[iv] http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx

[v] http://www.stltoday.com/business/local/ernst-young-denies-stealing-express-scripts-data/article_5dc960d3-10c1-5c2c-95de-7eadda56e8b0.html

[vi] Source: California Attorney General

[vii] Source: PHIPrivacy.net

[viii] http://www.theatlantic.com/static/front/docs/sponsored/zurich/Data_Security_White_paper.pdf

[ix] Source: *Messaging Policy Market Trends, 2011-2014*; Osterman Research, Inc.