Educating Decision Makers About the Need for Encryption

An Osterman Research White Paper

Published August 2010

SPONSORED BY

DATAMOTION™

OSTERMANRESEARCH

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

Executive Summary

OVERVIEW

Sensitive and confidential messages and documents – proposals, contracts, purchase orders, personnel records, discussion threads between senior managers, etc. – are sent via email, instant messaging, in unified communications systems and file transfer systems in just about every organization. This information is stored on desktop computers, laptops, smartphones, backup tapes, archives, file servers and other data repositories. However, despite the sensitivity of much of this information, the vast majority of it is never encrypted but instead left vulnerable for interception and review by virtually anyone inside or outside of an organization.

Is that a problem?

Yes. Not only does it violate best practice and common sense to make sensitive and confidential information available to unauthorized parties, either through inadvertent discovery or malicious intent, doing so also violates a growing number of local, national and international statutes focused on data privacy and content protection. For example, 46 US states and one Canadian province now have data breach notification laws, obligating those who lose or expose data to expensive remediation procedures. The US government imposes similar penalties on those who lose even a small number of patient health or financial records. Add to this a growing number of nations that are considering or have passed data breach notification requirements.

However, encrypting sensitive and confidential content is not just about avoiding negative consequences. Encryption can also provide distinct competitive advantage, allowing companies to win new customers and boost retention rates for existing customers. It can reduce the cost of communicating with customers and prospects. It can enable faster and better ways of improving customer outcomes. And, it can enable new business opportunities that would not exist in the absence of good encryption capabilities.

KEY TAKEAWAYS

The bottom line is that:

- The use of good encryption technology can reduce an organization's risk of non-compliance, and

- It can produce new opportunities for revenue generation and competitive advantage that would not otherwise be available.

ABOUT THIS WHITE PAPER

The purpose of this white paper is to educate decision makers on the merits of encryption, both from the perspective of avoiding negative consequences and from the benefits it can offer in generating new business. This paper also provides a brief overview of a leading vendor of encryption and related technologies and the sponsor of this white paper, DataMotion.

Email is Absolutely Essential in the Workplace

EMAIL'S DOMINANT ROLE IN THE WORKPLACE

Although there are a growing number of communication and information delivery tools used in the workplace – including the desktop telephone, mobile and smartphones, Twitter, Facebook, unified communications, instant messaging, etc. – email continues to reign as the primary mode of communication for most users. For example, in a study conducted by Osterman Research in May 2010[1], we found that:

- The typical user works in email 146 minutes each day, or 30% of an eight-hour work day.

- Use of email is significantly greater than the combined use of the telephone (54 minutes), instant messaging (23 minutes) and social networking (18 minutes).

- Users in organizations with up to 500 employees send and receive 173 emails on a typical workday, while users in larger organizations send and receive 160 emails. This means that users create or receive an email, on average, every three minutes or less.

- Email has become the de facto file-transport mechanism in most organizations, with 20-25% of all emails (depending on the size of the organization) containing attachments. Traditional file-transfer systems also find use, but email continues to dominate file transfer because of its ubiquity and ease of use.

OTHER COMMUNICATION MODES ARE BECOMING MORE IMPORTANT

Real-time communications tools are important in the context of workplace communications and are finding increased use. These include traditional instant messaging tools – both consumer-oriented and enterprise-grade – as well as Web conferencing, chat, VoIP (e.g., Skype) and other forms of presence-enabled communications systems. Social networking tools like Twitter, Facebook, LinkedIn and a host of other Web 2.0 applications are also being used more in the workplace, although typically as additional venues for sharing information and communicating with others and generally not as a replacement for email.

It is also important to note that ad hoc communications – such as sending a single file securely through email or any of a variety of tools – are becoming more important and more common, particularly as the workforce becomes more distributed and remote. Users are employing more formalized tools, such as FTP, far less for these types of communications.

THE BOTTOM LINE

Despite the growing use of alternatives to email for sharing information, making product announcements, keeping up with colleagues and the like, Osterman Research anticipates that email will continue to dominate the communications landscape for many years to come. As corroboration of this, Osterman Research found in a survey published in February 2008 that users in smaller organizations (up to 500 employees) sent and received 129 emails on a typical day; users in larger organizations sent and received 140 emails[2]. That translates to email use in smaller organizations increasing by 34% in just over two years, while email use in larger organizations has increased by 14% during the same period. And, this increase occurred during a period of enormous growth in the use of social networking tools and continued strong growth in real-time communications.

Most Messages are Sent in the Clear

CLEAR TEXT EMAIL IS EASILY INTERCEPTED

Somewhat surprisingly, the vast majority of emails are sent without any form of encryption to prevent their unauthorized access. This occurs despite the fact that a large proportion of emails contain sensitive or confidential information, such as purchase orders, contracts, proposals, embargoed press releases, login credentials and the like.

Quite often, unauthorized access to sensitive or confidential information in email occurs as a result of a mistake. For example, the type-ahead feature in many email clients will often result in senders clicking on the wrong name in an address list. Users will often include unauthorized individuals or former employees on distribution lists for some types of email communications or attachments. To be sure, there are situations in which someone will intercept email communications with malicious intent, but these tend to be the exception and not the rule.

THE PROBLEM IS NOT A THEORETICAL ONE

That said, the problem with unencrypted, sensitive email being lost or intercepted by third parties is not something that could happen, but one that happens all too often. Here are just a few examples that illustrate the seriousness of the problem:

- In May 2010, Aramark Healthcare Support Services and Sinai Hospital of Baltimore were involved in an email data breach of 937 individuals' records[3].

- Also in May 2010, an error in the use of a mail merge program by the Tralee Town Council in Ireland resulted in bank details of companies who do business with the council being exposed to other companies[4].

- In April 2010, the Children's Medical Center of Dayton, Ohio, was involved in an email data breach of 1,001 individuals' records[5].

- In February 2010, Computer Program and Systems and Reliant Rehabilitation Hospital of North Houston were involved in an email data breach of 763 individuals' records[6].

- In October 2009, the Public Employee Health Insurance Plan (Kentucky Employees' Health Plan) was involved in a breach in which a misdirected email breached the records of 676 individuals[7].

- Also in October 2009, a political party in Canada sent an email to one of their members, a Minister of Parliament (MP), with the login credentials necessary to gain access to a conference call. However, the actual recipient of the email, an MP with a very similar name in a rival political party, logged into the call, recorded it and then released the recording to media outlets[8].

- In September 2009, the University of California, San Francisco was the victim of a phishing scam in which the records for 610 individuals were breached by email[9].

- That same month, an employee of Rocky Mountain Bank of Wyoming sent an email to a representative of a customer at the latter's request. However, the employee sent the email to the wrong address and mistakenly included an attachment with account information and Social Security numbers for 1,325 bank customers[10].

- In January 2009, an office at Missouri State University in Springfield sent an email containing the names and Social Security numbers of 565 foreign students in an attached spreadsheet[11].

THE PROBLEM IS NOT LIMITED TO EMAIL

While most electronic communication data breaches occur via email given the dominance of that platform for sending communications and attachments, other tools can be used to commit data breaches, as well. For example, there have been numerous cases in which unencrypted data on USB sticks, backup tapes and other portable media has been lost or stolen. Instant messaging systems can be used to share files and other data as easily as can be accomplished using email. FTP systems can also be the source of data breaches, either by sending data improperly or by leaving content on servers unattended and unmanaged. Social networking tools can also be used easily to breach sensitive or confidential data given that few organizations today monitor content sent or received with Twitter, Facebook, etc.

FOUR TRENDS IN INFORMATION MANAGEMENT

The future of communications, particularly in the context of potential sources of data breaches, can be summarized as follows:

- **The number of communication tools will increase**
  Despite the continued dominance of email, there will be a growing number of tools through which unencrypted communications and data breaches will occur.

- **Tools will be more consumer-focused**
  The workplace will be the venue in which tools that were originally consumer-oriented find a home. This includes tools like Facebook, Skype and other tools that users employ at home and then bring with them to work.

- **Migration to the cloud**
  More organizations are moving important parts of their infrastructure to the cloud, resulting in customers dependent on these providers to react appropriately to the problem of encrypting communications and ensuring that data breaches do not occur.

- **The IT department will have less control**
  The number of employees who work from home or remotely will continue to

increase, as will the number of younger employees. This means that IT will not be able to dictate the use of only "approved" tools – younger and/or more independent employees, assisted by their lack of proximity to IT staff, will simply use what they want, resulting in at least the potential for more data breaches.

Why is Unencrypted Communications So Dangerous?

The question of why unencrypted communications is dangerous is a bit like asking why it's unsafe to leave the front door of a house unlocked when the owner is on vacation. While the latter question may seem trite, in reality it is not. Just like leaving a front door unlocked when the owners are absent will probably not result in the home being burglarized, sending an unencrypted email will probably not result in its content being intercepted and used for nefarious purposes. In fact, most data breaches do not actually result in harm to the affected parties.

However, because of the potential for serious harm that can result from data breaches, governments and other organizations have created a number of laws that dictate remedies when data breaches occur, even if they do not result in unauthorized use of the breached information. Further, violations can result in large fines or costly litigation – something that companies should be diligent to avoid.

ORGANIZATIONS CAN VIOLATE DATA BREACH AND OTHER LAWS

- **US federal requirements**
  There are numerous US federal requirements focused on addressing data breaches, but among the most notable is 16 CFR Part 314 (Standards for Safeguarding Customer Information). This statute implements Gramm-Leach-Bliley Act sections 501 and 505(b)(2) and applies to banking and other financial institutions. It requires organizations to implement employee-training programs, design networks appropriately to minimize intrusions and attacks, and provide oversight of any service providers that are used by financial institutions.

  Regulation S-P has been adopted by the US Securities and Exchange Commission (SEC) in accordance with Section 504 of the GLBA. This section 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. The rule applies to brokers, dealers, investment firms and investment advisers.

  Part of the Safeguards Rule, the Red Flag Rules requires financial institutions and creditors to implement a program to detect, prevent, and mitigate instances of identity theft. Affected businesses must develop and implement written identity theft prevention programs, which were required to be in place by Nov. 1, 2008. The programs "must provide for the identification, detection, and response to patterns, practices, or specific activities – known as 'red flags' – that could indicate identity theft."

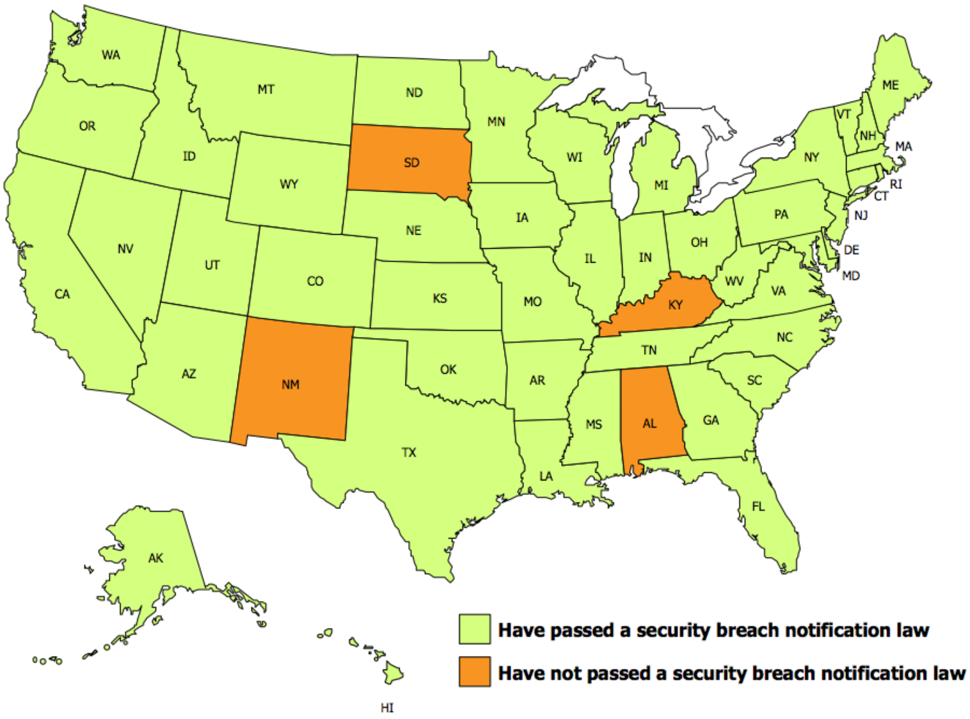
  Penalties for violations of the Health Insurance Portability and Accountability Act

(HIPAA) have been expanded dramatically. For example, the US Department of Health and Human Services (HHS) issued *Breach Notification for Unsecured Protected Health Information* that became effective on September 23, 2009[12]. Health and Human Services requires individuals to be notified of breaches of their protected health information (PHI), logging of all such breaches with notification to HHS annually, and notification of breaches of more than 500 individuals in one state to a prominent media outlet. Fines for violations can now reach as high as $1.5 million per calendar year.

The Family Educational Rights and Privacy Act of 1974, which focuses on protecting the privacy of students' education records, includes provisions for how states can transmit data to federal entities.

- **State and provincial encryption requirements**
  At present and as shown in the following figure, 46 of the 50 US states have passed data breach notification laws, requiring those who breach sensitive, confidential or otherwise protected data to notify the affected parties of the incident. The impetus for data breach notification laws began with California's SB 1386 back in 2003.

Status of Data Breach Notification Laws in the United States


WA
MT
ND
ME
OR
MN
VT
NH
MA
ID
SD
WI
NY
WY
MI
RI
CT
PA
IA
NE
NJ
NV
OH
IL
IN
UT
DE
CO
MD
WV
VA
CA
KS
MO
KY
NC
TN
OK
AR
SC
AZ
NM
GA
AL
MS
TX
LA
FL
AK
HI
🟩 Have passed a security breach notification law
🟧 Have not passed a security breach notification law

Data Source: National Conference of State Legislatures

The penalties for breaching confidential data vary from state to state but normally include some fairly significant penalties for non-disclosure, as well as often-rigorous requirements to notify the affected individuals. For example, Florida's data breach notification law (Florida Statute 817.5681) requires that if unencrypted personal information is breached, notification to the affected parties is required within 45 days; if notification is not made within this 45-day period, an administrative fine of up to $500,000 can be levied. Any business that holds information on behalf of another business must provide notification within 10 days.

Alberta is the only Canadian province that has enacted a data breach notification law (effective May 1, 2010), which it added to the province's Personal Information Protection Act that was first implemented on January 1, 2004. However, the Albertan law is not as rigorous as many US data breach notification laws, since notifications are not mandatory but instead determined on a case-by-case basis by the Office of the Information and Privacy Commissioner of Alberta.

- **More rigorous state obligations**
  On Oct. 1, 2008, a Nevada law (Nev. Rev. Stat. § 597.970 [2005]) went into effect stating that: "A business in this State shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission." Such personal information includes an individual's first name or first initial and last name, along with details like a Social Security number, driver's license number or credit card number with security code. Law experts say that since the Nevada law doesn't define a "customer", the rules could be interpreted as applying to customers regardless of where they reside.

  Standards for the Protection of Personal Information of Residents of the Commonwealth (201 CMR 17.00), took effect in Massachusetts on March 1, 2010. The law mandates that personal information – a combination of a name along with a Social Security number, bank account number or credit card number – be encrypted when stored on portable devices, when transmitted wirelessly or when transmitted on public networks. The law affects "persons who own, license, store or maintain personal information" about Massachusetts residents.

  The impact of these types of laws can be felt worldwide – if an organization has a customer in a state with a data breach notification law, they are obligated to carry out the provisions of the law in the event of a data breach. The good news, however, is that many data breach notification laws exempt breaches in which the lost data was encrypted.

- **Other requirements**
  The Payment Card Industry Data Security Standard is 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.

  The Personal Information Protection and Electronic Documents Act is a Canadian privacy law that applies to all private companies operating in Canada. Like many other privacy laws, it requires that personal information be stored and transmitted securely. Canada's Privacy Act, in place since 1983, protects the personal information collected by government institutions.

The United Kingdom (UK) Data Protection Act imposes requirements on businesses operating in the UK to protect the security of personal information and to preserve information only as long as it necessary to do so. The act requires, at least by implication, encrypted transmission of personal information and its secure retention.

Germany passed amendments to the nation's Federal Data Protection Act (the Bundesdatenschutzgesetz). Among these provisions is a relatively weak (by many US state standards) provision that individuals be notified if an information holder determines that a breach could cause "significant harm."

ENCRYPTION CAN PROVIDE COMPETITIVE DIFFERENTIATION

Encryption is not just about avoiding negative consequences like data breaches. On the contrary, there are a number of benefits that can be realized by companies that deploy encryption capabilities. For example:

- Businesses that can demonstrate secure communications capabilities for their customers' personally identifiable information are more likely to win and keep customers. In a *Dark Reading* article in 2007, secure email system user Intego Insurance attributed a $500,000 deal with a New York investment bank to its email encryption capabilities.

- There are many well-known banks that use encrypted email capabilities as a selling point for new customers. The key is to provide a service that is easy for bank employees to use and that does not require customers to install new software or go through numerous steps before communicating electronically with the bank.

- Similarly, physicians can also offer encrypted email for patients using any of a number of secure messaging services. Despite the availability of these services, only one-third of physicians surveyed by Manhattan Research for its 2008 report communicate with their patients online. The researchers concluded that although the number of doctors that email patients is growing, that number lags behind consumer interest in such communication methods.

- More strategically, encryption can be integrated with portals via Web service APIs; electronic forms capabilities can be developed to allow a wide range of interaction capabilities with customers, prospects and others; and connectors can be developed into backend systems to encryption-enable a wide and growing variety of processes, allowing businesses to run more efficiently by making their processes more secure.

SOME CONSEQUENCES ARE DIFFICULT TO QUANTIFY

Aside from the obvious threat that a data breach puts customers at risk of having their identities stolen, consumers who receive a data breach notification often struggle to understand what it means and how it could be relevant to them. According to Javeline Strategy & Research's 2009 Identity Fraud Survey Report, the mean consumer cost of identity fraud is at its lowest level since 2005 at $496 per incident, but fraudsters are moving much more quickly. A full 71% of the fraud incidents began less than one week after the data was first stolen, according to the researcher[13].

In addition to the penalties with which a business may be charged by regulatory bodies, the Federal Trade Commission (FTC) has the authority to impose an annual 20-year audit requirement on firms that were subject to a breach and found to have failed to adequately secure customer data. Audits can be rigorous, and complying with them for 20 years can be very costly.

A security breach also forces organizations to review their security processes. A security failure at SAIC, for example, forced the company to undergo a complete employee training and investigation program, again adding significant costs across the enterprise.

Justifying Encryption to Decision Makers

TIPS FOR APPROACHING DECISION MAKERS ABOUT ENCRYPTION

Aside from the fact that all organizations should encrypt sensitive communications, data stores and other repositories of important information simply as a best practice, there are a variety of ways to justify the deployment of encryption technologies to decision makers who might resist the use of encryption, or at least the expense of deploying the technology. Among these are the following examples:

- **Avoiding a major data breach**
  As discussed earlier, there are numerous examples of data breaches, some involving hundreds of records and some involving millions. Let's say, for example, that a 500-employee company has the potential for experiencing a data breach in which 5,000 customer records are exposed and each of these customers generates an average profit of $250 annually. The following assumptions will be used in calculating the actual cost of a data breach on a per customer basis:

  - Cost of notification (staff time, postage, etc.): $50[14]
  - Cost of providing credit reporting services for one year: $10
  - Percentage of customers that will be lost as a result of the breach: 4%

  Based on these assumptions, the total cost of a single breach of 5,000 customer records will be $350,000. That means that if an organization invested $200 per employee in technology, training, etc. to avoid a single data breach, the cost would be $100,000, and the net savings would be $250,000.

  Viewed in this context, the deployment of encryption technology only to avoid data breaches is akin to preventive health care: a relatively small expense incurred proactively can dramatically reduce the potential for a much more expensive consequence in the future.

- **Winning new customers**
  Another justification for deploying encryption technology is the ability to win new customers. This is particularly important in industries in which sensitive information must be sent, such as healthcare, insurance and financial services. For example, if an organization with 5,000 customers, each generating a net profit of $250 annually, could add just 2% to its client-base each year by offering the ability to communicate

with customers via encrypted email, that would result in additional profit of $25,000 in the first year and $76,510 over three years.

The potential for adding new customers because of the ability to communicate with them in a secure manner is not simply theoretical. Osterman Research conducted a study in June and July 2010 in which end users were asked about their likelihood of switching to providers if they could communicate with them via email and other forms of communication. For example, we found that 9.4% of end users would definitely switch to a new physician/clinic that allowed communication via email assuming that their current physician/clinic did not. Similarly we found that 4.9% would definitely switch to a new physician/clinic that allowed communication via instant messaging or chat if their current provider did not.

- **Cost savings from eliminating paper documents and faxes**
  Another justification for the use of encrypted communications is the ability to replace some or all of an organization's paper-based and faxed documents. This is particularly important in the banking, securities trading, healthcare and mortgage industries, although many other industries can also benefit from the use of encrypted communications.

  For example, if we assume that an organization sends out 50,000 statements each month via postal mail, and that the direct cost (postage, paper, printing, etc.) is $0.50 per statement, then the total annual savings will be $300,000 annually. Encrypted communications can create more efficient, less expensive processes that result in resources being freed up and assigned to other initiatives.

- **Considering the difficult-to-quantify issues**
  There are other issues more difficult to quantify that decision makers should consider when deciding whether or not to deploy encrypted communications systems in their organization. For example:

  - How many prospective customers will not consider doing business with a firm that has experienced a data breach as a result of not encrypting its communications?

  - What are the long-term costs of additional regulatory oversight or additional audits that result from a single data breach?

  - What is the long-term damage to a company's reputation, its brand(s) or its ability to work with new business partners as the result of a data breach?

  - What internal damage might follow a data breach, such as lower employee morale, finger pointing between groups responsible for managing customer data, etc.?

While these issues are, admittedly, difficult or impossible to quantify, they represent actual harm that can arise from the inability to adequately protect sensitive data.

HOW SHOULD CONTENT BE ENCRYPTED?

There are many ways that email can be encrypted, from deploying systems that automatically encrypt messages with sensitive information based on company-defined policies to manual options. These options, discussed below, all have various advantages and disadvantages.

- **Policy-Based Encryption**
  Some email security solutions allow organizations to automatically apply encryption or decryption based on their policies and with varying degrees of granularity. For example, a policy-based encryption system can scan emails or files for particular keywords, company names or strings of numbers that look like Social Security numbers or credit card numbers and automatically encrypt this content before it is sent. Using policy-based encryption ensures consistent application of security policies without user intervention, and it saves IT having to monitor email traffic manually.

- **TLS (Transport Layer Security)**
  TLS is an Internet Engineering Task Force (IETF) standard and provides gateway-to-gateway encryption, and it is the successor to Secure Sockets Layer. It provides encryption of message transmission over TCP/IP connections. If both the sender's and recipient's email environment supports TLS, all transmissions traveling to and from both parties' mail programs and mail servers are automatically encrypted. If a recipient's email environment does not support TLS, the transmission is sent anyway but unencrypted.

- **S/MIME (Secure Multipurpose Internet Mail Extensions)**
  S/MIME is an IETF standard for public key encryption and signing of email encapsulated in MIME. An individual can send and receive S/MIME-protected emails once he or she has acquired a public key and a private key from a certification authority and exchanged the public key with his or her contact. Public keys can be exchanged by sending digitally signed messages, and individuals store a contact's key in the contact's entry in an address book. To send an encrypted message, the sender composes the message in his or her S/MIME-enabled email software then locates the recipient's public key, using it to encrypt the message. The recipient's email system in turn decrypts the message using the recipient's private key.

- **OpenPGP**
  OpenPGP (using keys) and S/MIME (using certificates) are encryption standards (similar to how gif and jpeg are standards for photos). OpenPGP can encrypt any type of content (email, email attachments, data, files, folders, pictures, PowerPoint presentations, documents, PDFs, etc.). OpenPGP uses asymmetric (public and private) encryption keys that are discoverable via open source and commercial global directories. Companies like PGP Corporation are in business to create solutions to make the underlying mechanics transparent to users and IT departments. For example, keys are automatically, transparently looked up once messages are sent.

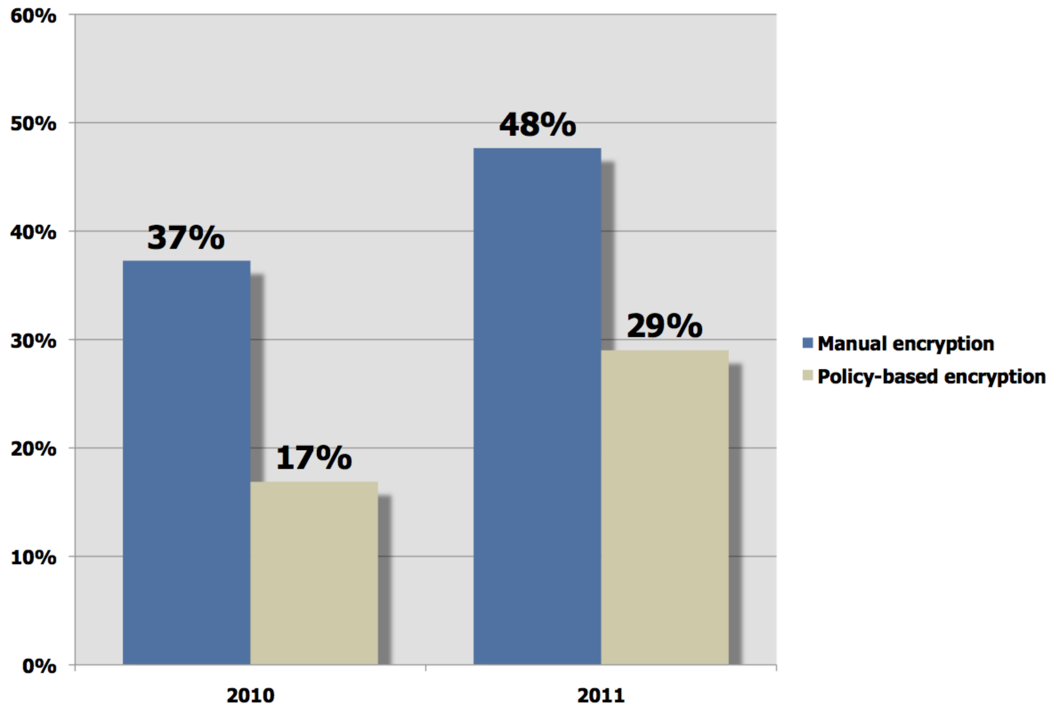
- **Manual Encryption Methods**
  Some email security software enables users to manually encrypt messages by adding a prefix, such as "[encrypt]" in the subject line, telling the software to encrypt the message and save it as an attachment. The recipient will need to go through a series of processes in order to view the message. One process would be for the recipient to save the attachment and open it in a Web browser, but some vendors also allow TLS delivery, PDF push, POP3/S pickup and also Web service APIs. But first they would need to register and activate an account with the sender's email security software provider. To reply to an encrypted email, the recipient would need to respond via the same user interface provided by the email security software provider.

  Encryption solutions using PDF documents have the advantage of not requiring special encryption software for the recipient, instead using only freely available Acrobat Reader software. PDF-based encryption solutions also have the advantage that the recipient does not need to visit a Web site to view the encrypted message. Another advantage of PDF-based solutions is that attachments are embedded into the push, so unlike JavaScript-based push solutions, the recipient does not need to visit a Web site to download the message attachments.

WHERE THE MARKET IS GOING

Encryption, while not widely used for most communications, is becoming more common. For example, an Osterman Research survey conducted with mid-sized and large organizations during Spring 2010 found that both manual and policy-based encryption are becoming more common, as shown in the following figure.

Email Encryption Methods in Use



Three Steps to Creating an Encryption Strategy

FIRST: TAKE AN ALL-ENCOMPASSING VIEW OF SECURITY

Osterman Research recommends that organizations of all sizes and serving any industry take a broad view of their encryption requirements by viewing it as part of their overall security infrastructure. This means that encryption should not be viewed as a standalone technology or activity, but part-and-parcel with an organization's control of malware, spam, data leak prevention, Web monitoring and the like.

Part of this effort should identify who in an organization has the greatest need for encryption and where the deployment of encryption would enable the creation of business processes not currently available to them. The roles that could benefit most might include legal counsel, human resources, finance and other groups that regularly send sensitive or confidential information to others inside and outside the organization. However, Osterman Research has found that users who might not consider themselves as users of encryption technology quite often could make good use of it. For example, some roles/applications that could make good use of encryption include marketing managers when sharing new logo or product designs, analyst relations staff when sharing embargoed presentations, or public relations staff when distributing announcements to the press. Most often, these roles do not use make regular use of encryption technology despite the fact that they share sensitive data on at least a somewhat regular basis.

SECOND: CONSIDER OBLIGATIONS TO PROTECT DATA

The next step is to examine the strictly codified obligations to encrypt sensitive communications and data at the state/provincial, federal and international levels, as well as other requirements that may not be regulatory in nature. For example, as noted above, there are a variety of regulatory obligations to protect customer and other sensitive information in transit and at rest; each of which carries with it penalties for breaching this data. There may also be business partner requirements and generally accepted industry standards to protect data to which an organization must adhere.

It is also important to examine the reach of obligations that may not necessarily apply to an organization today but that could impact it in the future. For example, the "new" HIPAA expands the obligations that used to apply only to covered entities to all of those entities' business partners. That means that attorneys, benefits administrators, accountants and others that work with healthcare-related organizations and have in their possession PHI are now subject to the same obligations for data privacy.

THIRD: EVALUATE YOUR DEPLOYMENT OPTIONS

The next step is to evaluate the various deployment options and scenarios that are available and that might have applicability for a particular organization's requirements. For example, deployment models range from completely on-premise solutions using servers or appliances to completely hosted/SaaS-based solutions. An organization may opt for policy-based encryption that takes the decision about encrypting individual emails out of the hands of users, or they may opt to allow only manual encryption that is completely under the control of users. Encryption could occur at the gateway so that content remains unencrypted behind the firewall, or an organization could opt for desktop-to-desktop encryption.

Another consideration when choosing an encryption capability is its impact on email and other electronic content archiving. Because organizations are obligated to preserve electronic business records for legal and regulatory purposes, the decision about encryption technologies will have an impact on how content is archived and how it is searched and accessed in the future.

Also, content encryption should be viewed holistically in the context of every venue in which it should be used: for email, real-time communications, backup tapes, USB sticks, laptops, smartphones, etc.

Finally, it is useful for an organization to focus on as few "platforms" as possible to eliminate complexity for end users and administration requirements for IT.

Sponsor of this White Paper

DataMotion
35 Airport Road
Suite 120
Morristown, NJ 07960
+1 800 672 7233
www.datamotion.com

DataMotion™, Inc. is a leading provider of information delivery solutions that enable businesses to safely and easily transact with partners and customers. DataMotion solutions leverage your existing IT infrastructure resulting in rapid deployment and a quick return on investment, saving as much as $5 for every $1 spent. Core applications of the DataMotion suite include encrypted e-mail, file transfers, electronic forms and programmatic APIs for integration. Solutions are available as hosted services or on-premise software. DataMotion's unified platform provides visibility, security, management and reporting to all data exchanges - helping customers streamline business workflow and achieve regulatory compliance. For more than ten years leading healthcare, insurance, pharmaceutical, financial services and government agencies have trusted DataMotion for safe data delivery.

For additional information and a free trial account, visit www.datamotion.com.

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, statue, 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.

[1] Unpublished research from Osterman Research, Inc.

[2] Source: *Results of an End-User Survey on Messaging Issues*; Osterman Research, Inc.; published February 2008

[3] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html

[4] http://www.irishexaminer.com/ireland/probe-after-bank-details-of-firms-sent-by-email-to-rivals-121183.html

[5] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html

[6] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html

[7] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html

[8] http://lawiscool.com/2009/10/12/rcmp-takes-heat-for-failing-to-probe-wire-tapping-allegations/

[9] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html

[10] http://commonlaw.findlaw.com/2009/09/personal-data-an-email-error-security-breach-notification-laws.html

[11] http://www.privacyrights.org/data-breach

[12] http://www.aad.org/pm/compliance/hipaa/documents/BreachNotificationFactSheet.pdf

[13] http://tinyurl.com/m9avas

[14] Source: Ponemon Institute