

Cloud Email Encryption & DLP

The Critical Need for Encrypted Email and File Transfer Solutions

WHY THIS WHITE PAPER WILL BE WORTH YOUR TIME

WE'VE ALL HEARD "AN EMAIL IS LIKE A POSTCARD"...

Among the more common analogies used to describe an email sent across the Internet is that it is like a message on a postcard that anyone can read along the way. However, an email or file sent in clear text offers much more exposure than a postcard because of the nature of transmission itself. When an email or file is sent, it is copied to at least two servers, but often many more than that. These copies are sometimes included on backups at various points between the sender and recipient. Content is inspected by various firewalls through which the email passes, exposing it to copying and interception. IT staff members at any of the points at which an email might be stored or through which it transits have access to these emails, perhaps using traffic monitors or packet sniffers that look for particular keywords or other content.

It is important to note that the email message itself is not the only information at risk. An Osterman Research survey found that 29% of the emails sent through corporate email systems contain attachments, and that emails with attachments account for just under 96% of the total volume of content sent through email systems. Clearly, protecting the integrity of files sent through email is just as important as protecting the messages themselves.

The problem, however, is not limited just to email systems. A growing number of organizations are turning to dedicated file transfer systems to address the growing number of files they send, to manage larger attachments that cannot be sent through email, and to alleviate the load on email servers. Increasingly, these systems are a critical component of essential business processes in their own right, and content sent through these systems must also be encrypted to ensure the integrity of the information sent through them.

....BUT THE PROBLEM IS NOT A THEORETICAL ONE

The problem of clear-text email being intercepted is not a theoretical one:

The US National Security Agency's (NSA) Pinwale database contains millions of emails, including those of former President Clinton. Surveillance of email by the NSA was made legal in 2008 under the FISA Amendments Act¹.

Interloc, an online bookstore offered Internet access and email services to several of its clients. However, the company configured its mail server to copy these clients' emails sent to Amazon.com without the permission of the affected parties.

SAIC, a defense contractor that handles sensitive health information for more than 850,000 US service members and their families, acknowledged in July 2007 that it sent medical appointments, treatments and diagnoses unencrypted over the Internet².

Confidential emails sent by two US governors were made public in June 2009. In one case, a governor's emails were "obtained exclusively"³, implying that the emails were not public knowledge or made available through some sort of freedom of information request; while in the other a newspaper reports that it received the emails "from the governor's personal email account by an anonymous person"⁴.

Utegate is a current scandal in Australia that threatened their Prime Minister and head of the opposition party⁵. The focus of the controversy was an email supposedly sent by PM Kevin Rudd to the Australian Treasury Department asking Treasury to give special financial favors to a car dealership associated with Mr. Rudd. The opposition leader, Malcolm Turnbull, used the email to confront the Prime Minister, going so far as asking him to resign. However, it turned out that the email was forged, and instead of the Prime Minister being asked to step down, he then pushed for Turnbull to resign. All of this happened since the highest levels of government in Australia use standard email in the normal course of their business using a system that does not allow message identity to be based on a user's credentials.

The bottom line is that unencrypted emails can be intercepted by unauthorized parties, sometimes with malicious intent, but most often inadvertently. Even so, the consequences for not encrypting email and other content when required to do so by statute or best practice can result in significant fines, loss of reputation, loss of customers and, possibly, business failure.

ABOUT THIS WHITE PAPER

This white paper discusses key issues around encryption for both email and file transfer systems, some of the leading statutes that require sensitive content to be encrypted, and suggestions for moving forward with encryption.

EMAIL AND FILE TRANSFER OFFER BENEFITS AND LIABILITIES

EMAIL IS THE SINGLE MOST IMPORTANT COMMUNICATIONS TOOL

Twitter is growing by leaps and bounds among business users. Tens of million of business users communicate on Facebook. LinkedIn users number in the multiple millions. Instant messaging clients – both consumer and enterprise-grade – are used widely. Text messaging/SMS has become the default mode for personal communications for many younger workers.

All of that said, email continues to be the dominant communications and file transport mechanism used in business today. To back up that claim, consider the following from an Osterman Research study published in May 2009:

Email users spend a mean of 152 minutes on a typical day working in their email client, or 28% of their nine hour nine minute workday. Contrast this with their use of the Web at 138 minutes per day (23%), attending in-person meetings (13%) and talking on the phone (12%).

Further, email users spend only 13% of their time on a typical day not working on a computing platform of any kind, whether it's a desktop computer, laptop computer, smartphone, etc.

55% of email users report that more than one-quarter of the information they need to do their work is to be found somewhere in their email system.

EMAIL WILL BECOME MORE IMPORTANT OVER TIME

Clearly, email is a critical communications tool for virtually any organization or user, even those that make use of social networking and other communications tools. While social networking tools, wikis, blogs and other tools are becoming important components in the mix of communications modes employed by users in the workplace, email use will continue to grow for many years to come.

EMAIL IS THE DEFAULT FILE TRANSPORT MECHANISM

Although email is a critical communications tool, it also has become the primary method for transferring files both within and outside of the organization. Email's ease of use, its ubiquity, and the high level of confidence that individuals have that attachments will actually arrive intact have allowed email to become the most important single file transport system in most organizations.

DEDICATED FILE TRANSFER SYSTEMS OFFER MANY BENEFITS

That said, there is growing interest and dependence upon dedicated file transfer systems that can securely transmit files independently of email. Although email has become the de facto file transport system in most organizations, a growing proportion of decision makers are realizing that it is critical to have a dedicated capability that can encrypt, send, track and audit the transfer of files. This is particularly important as attachments continue to increase in size, as the transfer of files becomes more engrained in various business processes (about one in five organizations has seen overall file transfer growth in excess of 20% during the past year), as regulations (e.g., HIPAA, discussed later in this report) require that senders ensure that content is protected during transit, and as email managers seek to minimize the impact of large file transfers on the email infrastructure.

A dedicated file transfer system can address many of the issues associated with sending attachments through email, and can provide a number of important benefits for end users and IT staff:

File transfer systems ease the burden on email servers

Managed file transfer systems can dramatically reduce the load on email servers, allowing them to operate at improved performance levels so message delivery times can be minimized and overall efficiency improved. Ultimately, this can result in organizations deploying fewer email servers and deploying more mailboxes per server, resulting in lower TCO for email.

Users benefit by eliminating the impact of file-size limits

Many organizations impose limits on the size of files that can be sent through email. For example, an Osterman Research survey found that 35% of users cannot send files larger than 10 megabytes through their corporate email system, while only 4% of users have no limit.

Lower email-related costs for storage

As email storage is reduced, storage costs are also reduced. For example, even a 10% reduction in email storage can result in savings of tens of thousands of dollars per year in storage-related costs.

Email-related storage is reduced

Reductions in email server storage can be achieved through the use of managed file transfer systems because attachments are offloaded from "live" email storage. This results in less IT time spent managing storage, improved email server efficiency, shorter backup times and faster restoration after a server disruption.

Reduce impact on network bandwidth

Managed file transfer systems also reduce the impact on overall network bandwidth because most of the content that would normally be sent through email is sent in a more efficient way. This is because the actual download of the attachment occurs only on demand and is spread out over time, resulting in fewer spikes in network bandwidth demand and less overall traffic.

However, it is very important to note that many file transfer systems currently in use do not adequately protect content. For example, many files sent via FTP systems are not sent encrypted, many users share passwords to gain access to FTP systems, and older content is allowed to remain in storage for indefinite periods. What organizations need, therefore, is a way not only to encrypt content sent through file transfer systems, but also to manage it much more effectively.

THE PERILS OF CLEAR TEXT EMAIL AND FILE TRANSFER

CONTENT IS EASY TO INTERCEPT

Email messages and files that are not encrypted are sent in clear text or some other easily readable form, which allows them to be intercepted – either with malicious intent or accidentally – when, for example, an email or file is sent to the wrong person. This is akin to writing and mailing a postcard with the contents exposed to everyone handling the card during its journey to the recipient. Hackers and others with malicious intent can intercept email messages and read them simply by placing packet sniffers on the network.

As businesses use email as a standard form of communication, clear text email messages can often contain information that businesses would not like to become public or fall into the wrong hands. But all too often this is exactly what happens. It is easy to rely on the auto-fill feature of many email clients that completes a recipient's name when the sender types the first few letters, but this could result in the email being sent to the wrong person.

Also, it is easy to email attachments and other files that contain sensitive information to contacts mistakenly, or for other users to mistakenly forward such attachments to unauthorized recipients. Further, an email can be forwarded that might contain sensitive information far down in a discussion thread, often unbeknownst to the sender who might not have read the entire message.

EXAMPLES OF CONTENT INTERCEPTION

There have been many cases in which large numbers of emails have been sent to unauthorized parties or otherwise leaked because of the lack of encryption, as the following examples will illustrate:

Office of the State Superintendent of Education, DC

Someone at this agency, which manages requests for college financial aid, mistakenly emailed personal information about 2,400 applicants to more than 1,000 of these applicants in May 2009. The sensitive content was contained in a Microsoft Excel spreadsheet that was mistakenly attached to the email.

Government of Cameron County, Texas

An email containing the names of all Cameron County employees and officials – including their Social Security numbers and salary information – was mistakenly sent in an email by a County employee.

Walgreens Health Initiative

Walgreens Health Initiative (WHI) manages the pharmacy benefit of the Kentucky Retirement Systems (KRS). In March 2009, the pharmacy provider emailed 28,000 KRS members' records to the KRS benefits office without applying WHI's usual encryption process. In its disclosure letter, which is posted on the KRS website, WHI says the file was addressed only to a single and proper contact at KRS, and that the receipt of the file had been confirmed. The letter adds: "While there is a remote possibility that these records, containing limited personal information (name, date of birth, Health Insurance Claim [HIC] Number and Social Security number), were accessible while being transmitted, we believe the likelihood of any harm from this transmission to be very minimal."

Science Applications International Corp.

Defense contractor SAIC, which handles sensitive health information for 867,000 U.S. service members and their families, acknowledged in July 2007 that it sent medical appointments, treatments and diagnoses unencrypted over the Internet. The information was stored on a single, SAIC-owned, non-secure server at a small SAIC location; the security hole was detected during a routine network security check.

Royal Air Force Mildenhall

A British man in 2008 was forced to relinquish the mildenhall.com domain because he was constantly receiving sensitive emails that were mistakenly sent to his domain instead of to mildenhall.af.mil, the correct domain of the UK's Royal Air Force base at Mildenhall. The man had purchased the domain to promote the town, but told reporters that he had received numerous emails intended for the military base. These emails included the flight paths of Air Force One and President Bush, military tactics and passwords. The man worked with military officials to try to stop these emails, including blocking unrecognizable addresses, but the actions were unsuccessful.

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.

▪ TLS (Transport Layer Security)

TLS is an Internet Engineering Task Force (IETF) standard and provides gateway-to gateway encryption, and 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.

Advantages: If both sender and receiver are using TLS, messages are encrypted automatically without requiring additional steps by either party.

Disadvantages: Requires the purchase and maintenance of an X.509 Public Key Infrastructure certificate, requires all recipients to have TLS enabled, does not provide sender or receiver notification, message is sent unencrypted if the recipient's server isn't TLS-enabled, and can slow email processing if sending and receiving large emails. TLS protects the transport layer/channel itself, but not the data, email or backups, nor does it protect the data at rest.

- 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.

Advantages: Messages can be sent to multiple recipients at the same time, while allowing each of them to use their private key to decrypt the message, users can sign clear messages with their PGP encrypted signatures which other PGP users can verify, asymmetric keys are extremely difficult to crack, works with data at rest and in motion, and users can use their private keys to encrypt personal folders and documents.

Disadvantages: This protocol is not built in to email systems and users need keys and software to use OpenPGP. Although users can forget the passphrase for their keys (which is similar to a person losing their car keys), IT departments can easily and securely remedy the situation.

- S/MIME (Secure Multipurpose Internet Mail Extensions)

S/MIME is an IETF standard for public key encryption and signing of email encapsulated in MIME. Individuals can send and receive S/MIME-protected emails once they have acquired a public key and a private key from a Certification Authority (CA) and have exchanged their public key with their 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 and his or her S/MIME-enabled email software then locates the recipient's public key and uses it to encrypt the message. The recipient's email system in turn decrypts the message using the recipient's private key.

Advantages: As the sender and recipient need to have exchanged keys before exchanging encrypted messages, S/MIME is best suited for situations that call for a high level of security, such as regulatory compliance. S/MIME can be used to confirm the identity of the sender, message data cannot be modified or changed on sending, and support for S/MIME is built into Microsoft Outlook, Outlook Express, Mozilla and Netscape.

Disadvantages: Can only send and receive encrypted emails from individuals with S/MIME-enabled email systems, requires sender and recipient to have exchanged public keys ahead of time, there is a risk of individuals losing their private keys if a hard disk becomes corrupted or a device is lost, and keys are specific to email accounts so that individuals with multiple accounts must request keys for each account.

- 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. Manual encryption includes solutions like DataMotion's Send Secure offering.

Encryption solutions using PDF documents, such as those offered by PGP Corporation and DataMotion, among others, 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.

Advantage: Allows users the flexibility to choose which messages to encrypt.

Disadvantages: Requires sender and recipient to take extra steps to encrypt a message, requires training of staff in proper use, recipient must read and respond using the user interface provided by the security software provider and not their own email program.

- 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.

Advantages: Ensures consistent application of security policies without user intervention. Saves IT having to monitor email traffic manually.

Disadvantages: Depending on configuration, there is potentially less individual control over the encryption of individual messages (although a policy can be created to allow users to decide on encryption of individual messages), but arguably more control over corporate-wide encryption. Policies must be kept up-to-date to ensure compliance, and a discretionary policy must be established to permit instances of manual encryption.

WHAT DOES ENCRYPTION MEAN FOR OTHER CAPABILITIES?

Encryption does not operate in a vacuum, but instead must be deployed in light of other technologies that are currently in an organization's infrastructure or that might be in the foreseeable future. Two of the key areas that encryption impacts most are virus scanning and email archiving:

- Virus scanning

If an encryption capability does not provide virus-scanning functionality, some encryption methods, as noted below, prevent emails from being virus scanned. For example, a SANS Institute paper "Encrypted E-mail: Close One Door, Open Another" warns that any malicious code in email messages is encrypted along with the entire message and thus cannot be scanned by antivirus software. But the paper notes that this vulnerability applies only to S/MIME and OpenPGP where email remains encrypted until the recipient decrypts it at the desktop (unless a gateway solution decrypts the email at the mail server). This does not apply to SSL or TLS technology, since these technologies decrypt the data at the Web server, not at the end user's desktop. However, since most users have anti-virus software on their desktop or laptop platform, this is often not a critical issue.

- Email archiving

Federal and regulatory rules, such as the Federal Rules of Civil Procedure, the Sarbanes-Oxley Act of 2002, and the Securities and Exchange Commission Rules, require organizations to retain email messages for e-discovery purposes. Organizations in certain industries, such as healthcare, are required to encrypt emails containing protected information. Traditionally, organizations have been limited to gateway deployments, but some email security software vendors allow organizations to encrypt all email, including desktop-to-desktop while preserving e-discovery. Messages are decrypted automatically before archiving so that messages can still be indexed and searched for e-discovery purposes.

THERE ARE REQUIREMENTS TO ENCRYPT SENSITIVE CONTENT

WHAT HAPPENS IF CONTENT IS SENT WITHOUT ENCRYPTION?

Some laws, such as the California Security Breach Information Act (S.B. 1386), applicable to organizations that do business or have customers in that state, require organizations to notify individuals whenever their personal information is at risk of being compromised. Notifying customers includes sending letters to affected individuals and setting up helplines. Notifications could also expose the company to negative media attention, causing damage to the company's reputation and potential loss of customers.

A study by the Ponemon Institute of 43 organizations that reported a data breach in 2008 found that some \$202 was spent on each consumer record compromised, with the average number of consumer records at risk at about 33,000. This cost included hiring forensic experts, notifying customers, setting up telephone hotlines, and offering free credit monitoring services.

A separate Ponemon study of consumers in 2008 who received a notification letter found that consumers were dissatisfied with the notification process and said the letters offered no direction on the steps the consumer should take to protect their personal information¹¹.

As a result, 31% said they terminated their relationship with the organization, and 57% said they lost trust and confidence in the organization. To prevent customer loss, some companies also offer added incentives. For example, TJX, which in 2005 suffered a security breach that laid bare 45.7 million credit card numbers, held a three-day customer appreciation event giving a 5% discount to affected customers. After the security failure at SAIC, the company took a number of steps to mitigate damage, including setting up a Web site with information for those affected, including an open letter from the chairman and CEO; and notifying some 580,000 households of possible compromise to individual's personal information. SAIC also provided affected individuals a free, one-year membership to an identity restoration service, which was also backed up by SAIC resources if the service failed to provide adequate assistance. It also extended the hours of its call center. Internally, SAIC initiated an investigation and placed a number of employees on administrative leave pending the outcome of the investigation. The bottom line here is that a lack of encryption or other protection of confidential information can lead to enormously damaging and expensive mitigation efforts.

US STATE REQUIREMENTS TO PROTECT DATA

California, with S.B. 1386, led the way for many states and some countries to pass data breach notification and disclosure acts. By the end of 2008, 44 U.S. states had enacted data breach notification laws and 25 countries, to varying degrees, have similar rules. A paper published in 2009 by the University of New South Wales ("Data Breach Notification Law Across the World from California to Australia"¹²) notes that the European Union and Australia have tabled data breach disclosure bills or passed acts. It also found that many of the laws and proposals from the 25 countries it examined are modeled on the California law.

The California law took effect in 2003 and is the basis of many of the laws of the other states. This law states that companies must immediately disclose a data breach to customers. However, it is important to note that a key exemption to the law is for data that is lost if encrypted. Some states differ on the penalties that businesses running afoul of the laws could face. In California, there is no civil or criminal penalty for failure to promptly disclose, but in Arizona, Florida, Texas and Colorado, businesses could face civil or criminal penalty. Arizona and Arkansas laws allow a civil penalty not exceeding \$10,000, whereas the limit is \$25,000 in Connecticut and Idaho, and \$500,000 in Florida. But Nevada and Massachusetts are leading the way in developing laws that require organizations and individuals to proactively protect customers' personal information. Legal experts believe that similar rules will soon be enforced in Michigan and Washington State.

FEDERAL AND NATIONAL REQUIREMENTS TO PROTECT DATA

There are a growing number of US federal requirements to protect sensitive data, as well as requirements in a number of other countries, some of which are discussed below.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

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]). It is also important to note that if an unencrypted email that contains PHI is sent across the Internet, a violation of HIPAA may have occurred even if the email was not intercepted. The mere fact that this content is available for review by an Internet service provider or another third party can expose an organization to penalties under HIPAA.

GRAMM-LEACH-BLILEY ACT (GLBA)

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.

PRIVACY OF CONSUMER FINANCIAL INFORMATION (REGULATION S-P)

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.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

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.

PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA)

The Personal Information Protection and Electronic Documents Act (PIPEDA) is a Canadian privacy law that applies to all companies operating in Canada. Like many other privacy laws, it requires that personal information be stored and transmitted securely.

UK DATA PROTECTION ACT

The UK Data Protection Act imposes requirements on businesses operating in the United Kingdom 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, requirements for encrypted transmission of personal information and its secure retention.

OTHER REQUIREMENTS

There are a number of other requirements that impact the decision for encryption, some of which are discussed below:

[Red Flag Rules 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."

[Federal Trade Commission's proposed security breach notification law](#)

In April 2009, the Federal Trade Commission proposed a security breach notification law focused on electronic health information. The rules, covering notification to individuals and federal regulators, would apply to vendors of personal health records and entities that offer products or services through Web sites of such vendors.

[American Recovery and Reinvestment Act of 2009](#) There are provisions in the current US economic stimulus legislation (American Recovery and Reinvestment Act of 2009) that require certain entities to notify affected individuals, regulatory bodies and the media of "unsecured protected health information". The new breach provisions affect all entities that deal with protected health information, whether previously covered by HIPAA or not.

The wide-ranging provisions include the appointment of a National Coordinator for Health Information Technology, who will "[ensure] security methods to ensure appropriate authorization and electronic authentication of health information and specifying technologies or methodologies for rendering health information unusable, unreadable or indecipherable." (H.R.1-116 SEC. 3001. (a)(iv))

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 the following:

- The reach of HIPAA has now been expanded 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.
- Now for the really serious part if you're subject to HIPAA requirements: one provision of HITECH is that the proceeds from HIPAA civil penalties will now be given directly to the Office of Civil Rights Enforcement within the US Department of Health and Human Services (HHS). What that means is that those who enforce HIPAA now have a direct financial incentive to levy fines and make them as large as possible, since these fines go directly into their budget. Further, individuals and lawyers can now collect fines for violations of the HIPAA Security Rule, dramatically increasing the incentive to sue privately when data is breached.
- Related to the point above is that 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. What this means for organizations that choose to remain in the healthcare industry or do business with them is that encryption and archiving become of paramount importance to a much larger group of companies. All of these organizations will need to appoint individuals to manage security policies, they will need to deploy appropriate technologies to protect data at rest and during transmission, and they will need to dramatically beef up their security posture for messaging, managed file transfer, realtime communications, data preservation and other parts of their infrastructure.

Family Educational Rights and Privacy Act of 1974 (FERPA)

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.

WHAT ABOUT THE HARDER-TO-QUANTIFY CONSEQUENCES?

Hardship on consumers

Aside from the obvious threat that a data breach causes by putting 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 started occurring in less than one week after the data was first stolen, according to the researcher.

Hardship on affected businesses

In addition to the penalties that business may be charged with by regulatory bodies, the FTC has the authority to impose an annual 20-year audit requirement on firms that were subject to a breach and that were found to have failed to adequately secure customer data. According to an FTC representative at the 2006 Information Security, Data Breaches, and Protecting Cardholder Information conference organized by the Federal Reserve Bank of Philadelphia and the electronic Funds Transfer Association, audits can be rigorous and complying with them for 20 years can be very costly.

A security breach also forces organizations to review its security processes. The 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.

ENCRYPTION AS AN ENABLER OF NEW BUSINESS OPPORTUNITIES

It is also important to note that not only are there negative business consequences from not using encryption, but there are a number of business benefits that can be realized by organizations that proactively deploy encryption capabilities. For example, businesses that can demonstrate a secure infrastructure for their customers' personal information are more likely to win and maintain 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 capabilities¹⁴.

In addition, 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 staff to use and does not require customers to have to install new software or go through complicated steps before communicating electronically with the bank. Similarly, physicians can also offer secure email messaging with 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 methods¹⁵.

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.

How Do You Solve the Problems?

Step one: focus on encryption across applications

Encryption is a critical – albeit just one – component of any messaging management system. Decision makers, therefore, must evaluate encryption solutions in the light of other systems, including archiving, malware scanning and the like. For example, while encryption should be a high priority for virtually any organization, organizations should not focus on it to the exclusion of other current or anticipated, non-email encryption requirements. With so many possible applications of encryption, an organization is likely to want interoperability (or at least non-interfering co-existence) among these applications so that a user will have a single keypair to encrypt and decrypt sensitive data with all devices, regardless of the application that is transporting the data. There are many emerging applications for encryption and it will be advantageous to leverage an enterprise architecture across all of them. Most important, the architecture needs to logically support expansion into new areas.

Step two: focus on obligations to protect data

As discussed earlier, there are a growing number of obligations to protect sensitive data sent in email or via other communication systems, necessitating the availability of encryption for all of these systems. Therefore, it is critical to understand the current and anticipated obligations that an organization might face, such as statutory obligations that are imposed by local, state/provincial, Federal and international requirements. In an era of increased corporate oversight and corporate governance, expect a growing number of obligations for data encryption (among other things) imposed on organizations in just about every industry.

However, it is important for organizations to anticipate future, internal obligations even in the absence of statutes, industry standards or other codified obligations to protect data beyond the confines of email and file encryption. These considerations might include the use of encryption to secure all of the information on laptops, mobile device or USB sticks. For example, full disk encryption is needed to protect duplicate data in temporary files, swap files, and hibernation files. To complement local full disk encryption, emerging applications such as network or shared storage encryption are becoming important. There has been a growing demand for shared storage encryption, where administrators can easily assign group rights to encrypt/decrypt data.

STEP THREE: FOCUS ON HOW BEST TO DEPLOY ENCRYPTION

There are a variety of encryption and management capabilities available:

Endpoint-to-endpoint

Encrypts email from sender to recipient, allowing email to be protected at every point between the sender and recipient. At no point is an email unencrypted during the transmission of the message.

Gateway-to-gateway

This mode is similar to the gateway-to-endpoint mode discussed below, but substitutes an encryption gateway for an endpoint on the recipient's side, eliminating desktop software and administrative costs on that end as well. Email is encrypted between gateways, but not within the sender's or recipient's organizations.

Gateway-to-Web

The encryption gateway provides access to sensitive data via a Web server, possibly co-located on the gateway itself. The data is typically protected via transport layer encryption, such as Secure Sockets Layer (SSL), allowing secure communication to occur with any recipient, regardless of its architecture or level of sophistication. Email is encrypted between the gateway and Web portal, but not within the sender's or recipient's organizations.

Gateway-to-endpoint

Provides encryption from a gateway system within the sender's network to the recipient's endpoint. In this scenario, the message leaves the sender's desktop in plain text and is encrypted by a gateway solution located near the email server, but still behind the corporate firewall. Email is not encrypted between the sender and the gateway used to encrypt the content.

ON-PREMISE OR IN THE CLOUD?

Further, organizations need to determine if their encryption capabilities will be managed on-premise via dedicated hardware and software managed by internal IT staff, or if a hosted encryption service will be used. There are benefits that can be realized from both approaches:

On-premises solutions

This approach offers the greatest level of flexibility in terms of deployment, ongoing management and choice of encryption modes. It may also be less expensive than the hosted model in some instances.

Hosted solutions

This approach offers very low initial costs and a shift from a focus on capital expenditures to operating expenditures. Hosted solutions also offer more granularity in terms of who is given access to encryption capabilities and can be less expensive than on-premise solutions. If data is not protected while at rest, outside parties may have access to sensitive customer data. In short, there are multiple points at which content can be encrypted and multiple models for deploying encryption capabilities.

SUMMARY

Email and file encryption are absolutely critical for a variety of reasons, including compliance with regulatory obligations to protect the integrity of sensitive data and best practices focused on maintaining the confidentiality of corporate data. However, most emails sent today – including those that contain highly sensitive content – are sent in clear text email. Similarly, most use of file transfer systems does not include encryption, leaving organizations exposed to a variety of negative consequences.

However, the status quo must change. Because of increasing amounts of sensitive content that organizations are sending and storing in email, increasing corporate governance requirements, and the growing number of consequences associated with not encrypting email and other content, encryption has become a business and legal necessity. Decision makers faced with the prospect of deploying encryption capabilities or living with the consequences will increasingly opt for the former.

CONTRIBUTORS TO THIS WHITE PAPER

This white paper was written by Michael Osterman, principal of Osterman Research, Inc. and Linda Leung.

Mr. Osterman is the president and founder of Osterman Research. He has more than 27 years experience in the high-tech research industry and has spent nearly 16 years following the messaging and collaboration industries. Prior to founding Osterman Research in 2001, he was Vice President of Market Research for Creative Networks, and has held senior analyst positions with SRI International, Ryan Hankin Kent and other research firms. Ms. Leung is an independent technology writer with 20 years of experience reporting on the high-tech sector. She has held senior editorial roles in print and online publications in the United Kingdom and the United States, including Computing and Network World. She is based in the San Francisco Bay Area and can be contacted at leunglh@gmail.com.