

This Free E-Book is brought to you by Natural-Aging.com.

100% Effective Natural Hormone Treatment
Menopause, Andropause And Other Hormone Imbalances
Impair Healthy Healing In People Over The Age Of 30!

E-mail Security Governance: E-mail Encryption and Authentication as a Business Enabler

By CipherTrust

E-mail Security Governance: E-mail Encryption and Authentication as a Business Enabler

by CipherTrust

How to Easily Secure Your E-mail System and Comply with HIPAA, Sarbanes-Oxley, and GLBA Regulations

While recent government regulations vary in scope and purpose, the need to protect and ensure the integrity of information is universal. Much of the information germane to business today is assimilated and communicated over messaging platforms such as e-mail. As a result, the need for a comprehensive approach to the secure delivery of e-mail affects almost all organizations, regardless of industry or size. As with many management challenges, the unknown is the most significant cause for concern. In the case of e-mail and messaging security, the most ominous threat is often the lack of ability to measure information flowing in and out of the corporate e-mail network.

E-mail has traditionally been sent "in-the-clear," meaning that e-mail headers and contents have been readily accessible to anyone with the ability to monitor network traffic. Traditionally, encryption technologies have been sufficiently difficult to implement that many businesses chose to sacrifice security in the name of user-friendliness given an application as mission-critical as e-mail. For example, some encryption and authentication technologies require ubiquitous adoption by each entity attempting to communicate, and few have ever agreed on which technologies are best or most efficient. Many businesses, committees and users have been attempting to standardize such use for well over a decade.

Over the last few years, however, regulations have been enacted that require the business and technology communities to generate and implement secure e-mail solutions. Easy-to-use encryption and authentication are now readily available. The new challenge for the enterprise is to determine where and how to implement these new solutions to ensure compliance with new regulations. Understanding how each regulation affects e-mail security and delivery is important to understanding the pressures all IT managers will be under in the months and years to come.

E-mail Security Issues for Sarbanes-Oxley

The Sarbanes-Oxley Act of 2002 took effect in June of 2004 and requires CEOs, CFOs, independent auditors and audit committees to certify the accuracy, confidentiality, privacy and integrity of financial statements — and the effectiveness of internal controls and procedures for financial reporting and disclosures. The most relevant sections of Sarbanes-Oxley to e-mail security are sections 404 and 802.

Section 404 deals with internal controls, and requires organizations to implement controls over the release of information to individuals or organizations outside the company's network.

Section 802 addresses records management, and how long and in what manner documents (including e-mail) should be retained.

Sarbanes-Oxley does not detail specific steps organizations should take to comply with these regulations. Rather, it requires that companies implement programs that ensure the secure flow of information, and then to be able to document the success and deficiencies of those programs. There exist some programs that are commonly used as a basis for implementation.

Corporations and business partners of companies affected by Sarbanes-Oxley, are required to ensure that sensitive information remains secure. Similar to HIPAA solutions, "Insider information" should not be accessible outside of the perimeter of a company's network. Encryption policies should be enforced whether a busy executive remembers to encrypt a message or not. Rogue employees should not be capable of transmitting sensitive financial information outside the network. Detailed reports should be available to auditors showing how the system has successfully protected the network and archived relevant communications. All of this can be handled swiftly with an e-mail governance policy and a central implementation mechanism. Without a mechanism in place, these requirements create a tangled web of complicated transactions and increased risk.

Unlike HIPAA, however, Sarbanes-Oxley often creates a need for organizations to prevent end-user encryption of information because encrypted information cannot be filtered for inappropriate content or trade secrets as it moves through the e-mail servers and onto the Internet. E-mails should be sent to the server as clear-text, and only once the content has been cleared for release should it be encrypted according to the organization's policies.

The need to enforce centralized content policies, as well as the need to provide detailed reports to audit committees, requires server-level control and administration. The servers should be flexible in terms of encryption technology in order to maximize the utility of e-mail, while at the same time the network should be defended from external attacks

E-mail Security Issues for HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) came into effect on April 21, 2003. The act is designed to protect the confidentiality, integrity, and availability of Protected Health Information (PHI) for individuals. PHI is defined as information that includes any individually identifiable health information. Healthcare organizations that must comply with HIPAA regulations are known as

Covered Entities (CEs). CE's include hospitals, insurance providers, employer health plans, physicians, business partners, and contractors working with healthcare providers.

The primary rule within HIPAA that affects e-mail is the Security Rule. Exposed PHI within e-mail is considered a risk that will surface during a HIPAA risk assessment. Covered Entities are required to perform a HIPAA risk assessment and then to adopt appropriate safeguards depending upon the outcome of the assessments they perform.

Healthcare organizations have reacted to the new rule in a variety of ways, and with varying degrees of effectiveness. The efficiency of e-mail offers an attractive means to transmit healthcare information from one organization to another; however the need to secure each transmission of PHI has created complications as secure e-mail solutions are new and not fully implemented at many sites that transmit and store PHI.

Many encryption technologies require the user to become familiar with the use of plug-ins and other specialized "client-side" encryption software. Encryption keys must be securely traded between partners, patients, providers, and other network members. More and more employees are involved in

transmitting PHI over the internet now than ever before. The increase in the number of employees transmitting PHI has caused administrative costs to increase as the need to train employees in proper use of encryption technologies also increases.

As the complexity increases, so does the probability that not all e-mail containing PHI will be encrypted. Doctors, who are always pressed for time, may not take the extra few minutes required to encrypt an e-mail. The clerk handling outbound messages for a nurse may not understand which information requires encryption and which does not. Furthermore, many healthcare administration workers have not been trained on the identification of PHI and subsequent proper handling.

The uncertainties and potential liabilities have led some organizations to go so far as to outlaw all PHI in e-mail. Instead of solving the problem, however, these decisions generally force employees to find alternative, and usually insecure, methods of transmitting PHI via e-mail in order to accomplish their jobs. This leaves organizations vulnerable to lawsuits based, at best, on non-compliance with HIPAA and, at worst, exposed PHI. The liability is tremendous - leading many insurance providers to be extremely hesitant to provide coverage in the IT space unless sound security practices and compliance can be proven.

The same problems arise with client-based encryption technologies that require the user to be trained or to take extra time to accomplish his or her task. The effect is an increase in likelihood that PHI will be transmitted through an insecure channel as rushed or untrained employees break policies set up to protect information.

Another issue faced by organizations is a lack of technological standards. Some organizations may be employing technologies such as S/MIME or PGP encryption, while others utilize secure connection technologies such as TLS or HTTPS. The effect is that any two organizations, each complying with HIPAA regulations in their own way, may be unable to communicate electronically due to a lack of

standardization within the industry.

The solution to each of these issues is to move the encryption responsibility from the individual user to a specialized server, and to utilize a system that can select from a number of encryption technologies depending on the recipient's technological capabilities. The server should be capable of applying encryption policies based on heuristics determined by the security officer, administrator, or business rules. Individual users should be able to specify that a message be encrypted, but the encryption should automatically be applied where appropriate regardless of user involvement.

Beyond encryption issues, CE's need to maintain system integrity, and availability of information. At all times, the network should not be at risk of downtime due to hacking attempts, Denial of Service (DOS) attacks, spam attacks, phishing, social engineering, or viruses.

E-mail Security Issues for Graham-Leach-Bliley Act

The Graham-Leach-Bliley Act (GLBA) was signed by Bill Clinton in 1999 and made fully effective on July 1, 2001. GLBA requires financial institutions, partners and contractors to protect consumer's private financial information. It is similar in purpose to the HIPAA regulations governing the use and transmission of information in the healthcare industry. It also imposes many of the same challenges on the financial industry as those faced by the healthcare industry.

As with organizations affected by HIPAA and Sarbanes-Oxley regulations, financial institutions are

faced with the need to protect confidential data, comply with regulations, keep the network operational and secure, and operate on a budget. The consequences of a failure to perform in any of these areas could result in imprisonment of company officers and fines. It could also have devastating effects on the business itself - potentially causing existing and potential customers to lose faith in the company's ability to service their financial needs.

As with healthcare organizations and corporate entities, the need to establish centralized policy-based governance over the transmission, encryption, and archival of sensitive information requires a secure server-based solution. The solution should be capable of interfacing with all of an organization's business partners regardless of the partner's technological capabilities, and it should be transparent to the user in order to maximize the efficiency and utility of e-mail and encourage adoption of acceptable means of corporate communication.

Conclusion

The trend is clearly in the direction of more complex security regulations and an increasing concern by consumers and investors over an organization's ability to protect privileged information. Fortunately, this increasing awareness of the general public and government agencies has coincided with a rapid development of the technologies required to meet these demands. CipherTrust has led the e-mail security industry in developing comprehensive solutions to e-mail borne threats such as spam, hackers, phishing, DOS attacks and more.

CipherTrust's IronMail provides the first true balance of security and usability that will enable businesses to protect the confidentiality and integrity of information as required while ensuring that employees can continue to use e-mail easily as a central communication medium. IronMail enables e-mail security governance with ease, solving a problem that has plagued the industry for 15 years.

Others merely claim it. IronMail does it. We invite you to try it.

CipherTrust manufactures the leading Enterprise E-mail Security appliance, IronMail. To learn more about how IronMail can help your organization filter spam, block attacks, and prevent fraud, download our white paper,

Stay up to date on all E-mail security issues by signing up for the

CipherTrust is the leader in anti-spam and email security. Learn more by downloading our free whitepaper, "

" or by visiting

Sending Passwords By Email

By Bryce Whitty

It amazes me how many sites allow you to register, and then send you an e-mail to your registered address containing your password in plain-text. There is never a warning stating that the site will email the password you use, for all to see.

Sending passwords by e-mail works when you forget a password. The site changes it and e-mails you the new one, which you then use to log in and change it to something else. The e-mailed password is not active for very long, and it isn't something you chose.

Sending you your own password, either in a welcome e-mail once you register, or as a response to a "forgot password" request is bad security. Really bad security.

Compounding this is the fact that e-mail providers such as Google Gmail state in their privacy policy that "deleted" e-mail may be kept indefinitely on their backup servers. As soon as someone e-mails you your password in plain-text, to a Gmail account, Google are likely to have that archived forever.

You can't tell whether a site is going to do to this, so it isn't possible to use a "less sensitive" password for sites which will e-mail your password back to you. If you have groups of passwords; one for sites you use to pay for things, one for forums, one for other less important sites, for instance, then you may enter your "usual" password without realising it may be compromised by being sent in an e-mail, visible

to anyone along the way that wants to read it.

Sites should seriously consider the security implications of sending passwords by e-mail, especially if there is no prior warning that this will happen!

Bryce Whitty owns and runs

called

. A website that provides

technical how-to's for repairing your computer. Technibble also has many guides for getting into the

or managing your existing one. We also cover other side topics such as Security

and Software.

Sending Passwords By Email

Security Issues Everyone Should Know About Online Shopping

Customizing E-Mail Addresses

Public-Key SSH Login

How HIPAA Security Policies Affect Corporate E-mail Systems

Build Your Own Mail Order Empire

Mega-Wealth Audio Library

AX Gold's Website Guardian

Stamp Collector Software

Free List Pro



This Free E-Book has been brought to you by Natural-Aging.com.

[100% Effective Natural Hormone Treatment](#)
Menopause, Andropause And Other Hormone Imbalances
Impair Healthy Healing In People Over The Age Of 30!