A CASE FOR EMAIL ENCRYPTION

Protect Email, Your Company and Relationships with Customers and Business Partners

Email is an excellent communication tool. With a simple 'click,' your employees email all kinds of messages and attachments to business partners and customers. Some are quick and insignificant. Others include sensitive corporate data, from personnel information, to financial or medical records, to customer lists or intellectual property. No matter the importance of the content, exchanging email remains the same – simple – and it's the simplicity that enabled employees and many companies to overlook the risks of unsecure email.

However in recent years, high-profile breaches including the Snowden revelations and the Sony Hack and government security blunders involving emails exchanged by former Secretary of State Hilary Clinton and former Florida Governor Jeb Bush have brought the insecurity of email into focus for both businesses and the general public. And while the public's attention may waver as news' headlines come and go, companies can no longer excuse a lack of security by telling customers and business partners that they didn't know the risks of email if a breach occurs.

By using email encryption to secure sensitive information in email, companies will not only protect trust with customers and business partners, they will also protect their business against the costs of revenue loss, reputational damages and liability associated with a breach, an estimated price tag of $3.8 million per data breach, or $154 per compromised record, according to a 2015 Ponemon Institute study.[1]

An Added Benefit to Email Encryption – Compliance

Securing sensitive emails isn't just a best practice – it's often the law. Compliance with regulations is a priority for healthcare, financial services and government organizations; it may also need to be a priority for companies that work with these organizations or practice business in specific states.

Here's an overview of federal and state regulations that you should be aware of and how email encryption is a solution for your organization's compliance.

Federal Industry Regulations

The Gramm-Leach-Bliley Act (GLBA)[2]

GLBA protects consumers' personal financial information held by financial institutions. Its "Safeguards Rule" requires all financial institutions to design, implement and maintain safeguards to secure confidential data. Its guidelines address standards for developing and implementing administrative, technical and physical processes to protect the security, confidentiality and integrity of customer information.

The Federal Financial Institutions Examination Council (FFIEC) released a handbook[3] on information security practices. Regarding encryption, it stated that financial institutions should use encryption to mitigate the use of disclosure or alteration of sensitive information in storage and transit[4]. Encryption should include:

- Sufficient encryption strength to protect the information from disclosure until such time as disclosure poses no material risk
- Effective key management practices
- Robust reliability
- Appropriate protection of the encrypted communication's endpoints

The Health Insurance Portability and Accountability Act (HIPAA)[5]

The HIPAA Privacy Rule provides federal protections for protected health information (PHI) held by covered entities, their business associates and sub-contractors and gives patients an array of rights with respect to that information.

If a breach of unsecured PHI occurs, covered entities and any related business associates and sub-contractors must provide notification of the breach to affected individuals and the HHS Secretary. If a breach affects 500 individuals or more, the breach is published online on the Office for Civil Rights breach list and media outlets serving the affected individuals' state or jurisdiction must be notified.

In addition, organizations that violate rules to protect patient privacy face onerous resolution agreements or possibly fines of up to $1.5 million.

The Average Data Breach

costs $3.8 million per data breach, or $154 per compromised record.[1]

State Regulations

Massachusetts

Under Mass 201 CMS 17[6], Massachusetts requires companies to encrypt all personal information of state residents transmitted electronically or wirelessly. This includes Social Security and employer identification numbers, drivers' license or identity card data, account, credit and debit card numbers with any password or security and access codes. The law applies to companies within Massachusetts, as well as companies in other states that manage personal information of Massachusetts residents.

Nevada

NRS 603A[7] mandates that all businesses, no matter their size or industry, must secure confidential customer information if it is sent electronically. Statute 603A.215 states that transmission of personal data, including via Web sites and email, must be encrypted.

Washington

HB 2574[8] protects personal information that is managed by any person or organization that conducts business in the state. If personal information – including name combined with Social Security number, driver's license number, financial account information – is transmitted or stored on the Internet, the law requires it to be secured and deems encryption as the accepted practice.

In addition to these laws, forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or government entities to notify individuals of security breaches of information involving personally identifiable information.[9]

Zix Message Encryption for Google Apps

Recognizing the evolving needs of your small business, employees, customers and partners, Google and Zix partnered together to provide Zix Message Encryption for Google Apps (ZME). Just as easy to use as regular email, ZME is innovative secure email developed specifically for Google Apps SMBs. Raising industry standards, our top differentiators include:

Ease of Use

Email encryption shouldn't disrupt employee workflow. It should work without your employees even knowing it, allowing them to focus on their responsibilities and attend

zixcorp.
www.zixcorp.com

to customer needs. With automatic scanning and the use of proven and up-to-date policy filters, emails with sensitive content are encrypted without user action. Removing the hassle and taking the decision out of your employees' hands eliminates human error and better protects your email.

Convenient Delivery for Recipients

If your employees don't have to take any extra steps to encrypt email, why shouldn't your customers and business partners be able skip the hassle too? ZME offers the industry's only automatic decryption of secured emails if recipients use the same platform. Of 1,000,000 Zix-encrypted messages sent every day, 75 percent are accessed without any extra steps or passwords.

For others who don't use the same platform, recipients can receive the message in less than two simple steps, removing hassle and confusion.

Smooth Mobile Experience

Convenient mobile delivery of encrypted messages is a critical component to keeping business moving and making your customers and business partners secure and happy. For senders and recipients using ZME, secure email on mobile devices is once again just as easy as regular email, because it is encrypted and decrypted automatically.

For other recipients, optimized screen layouts combined with easy registration and login experiences ensure mobile access is as seamless as the desktop experience.

With the right solution, email encryption can be an easy way to secure sensitive corporate data, avoid breach costs and meet regulatory obligations. Email encryption also protects relationships and preserves loyalty with customers and business partners. After all, it takes years to build trust, yet only seconds to lose it with a data breach.

Visit www.ZixCorp.com/ZME to learn more.

1. "The Cost of a Data Breach" by Ponemon Institute, 2015. 2. "Privacy Act Issues Under Gramm-Leach-Bliley." 3. "FFIEC IT Examination Handbook Infobase." 4. Encryption under the "FFIEC IT Examination Handbook Infobase." 5. The Health Insurance Portability and Accountability Act (HIPAA). 6. 201 CMR 17.00: Standards for the protection of personal information of residents of the commonwealth. 7. NRS 603A – Security of Personal Information. 8. Washington HB 2574 – Requiring the encryption of certain personal information. 9. Information provided by the National Conference of State Legislatures.