



The Case for Email Encryption

How Financial Institutions Secure Communication and Protect Relationships



The ZixDirectory® includes:

- Tens of millions of members and growing at approximately 100,000 new members every week
- All members of the Federal Financial Institutions Examination Council
- Divisions of the U.S. Treasury
- The Securities and Exchange Commission
- More than 20 state financial regulators
- More than 1,600 financial institutions

Easy, secure communication is a valuable asset in the financial services industry. Sensitive information is circulating on a day-to-day basis to customers, third-party organizations and strategic partners, and one communication tool emerges above the rest when exchanging sensitive personal information – email.

The average user spends 146 minutes per day in email, according to Osterman Research¹. Email outpaces all other communication methods, combined. In comparison, an average user spends 54 minutes per day on the telephone, 23 minutes per day on instant messaging and 18 minutes per day on social networking sites. Further emphasizing email as an essential business tool, Osterman Research found email has become a popular file-transfer method, estimating 20-25 percent of all email messages contain attachments¹.

With the convenience of email as a communication and file-transfer method, financial organizations need to ensure the security of email for the privacy of its customers, the protection of its business relationships and brand and compliance with regulatory requirements.

Regulations and Regulators

The Gramm-Leach-Bliley Act (GLBA) of 1999² 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 also address standards for developing and implementing administrative, technical and physical processes to protect the security, confidentiality and integrity of customer information.

¹ "Educating Decision Makers about the Need for Encryption" Osterman Research, August 2010.
http://zixcorp.com/documents/white-papers/OR-Educating_Decision_Makers_About_the_Need_for_Encryption.pdf

² "Privacy Act Issues Under Gramm-Leach-Bliley"
<http://www.fdic.gov/consumers/consumer/alerts/glbs.html>

The Federal Financial Institutions Examination Council (FFIEC) released a handbook³ 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 transit⁴. 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

All members of the FFIEC, divisions of the U.S. Treasury, the Securities and Exchange Commission and more than 20 state financial regulators understand the risks of unsecure email. They've implemented email encryption, specifically using *ZixCorp*[®] Email Encryption Services. As financial institutions assess risks and meet compliance standards, encrypted email should certainly be a component of any strategy.

Not only does email encryption offer confidence when exchanging messages and documents with regulators, it also addresses old and new email threats.

³ "FFIEC IT Examination Handbook Infobase"
<http://ithandbook.ffiec.gov>

⁴ Encryption Under the "FFIEC IT Examination Handbook Infobase"
<http://ithandbook.ffiec.gov/it-booklets/information-security/security-controls-implementation/encryption.aspx#9>

The Continued Risk of Employee Behavior

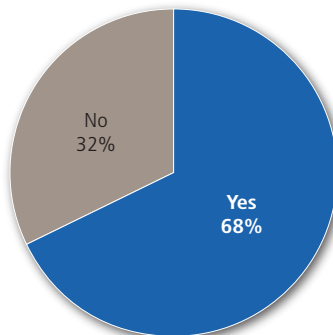
Financial institutions implement policies, offer employee training and leverage portals to prevent employees from leaking sensitive personal information, however a Ponemon Institute study⁵ found email leaks are still a high concern. Of financial respondents surveyed:

- 68 percent believe employees ignore policies about emailing unencrypted sensitive or confidential documents through insecure channels
- 61 percent believe employees send unencrypted confidential information through insecure email channels, such as personal Web-based email

Malicious intent may not be common when employees circumvent company policies, but the risk of unsecure email remains the same.

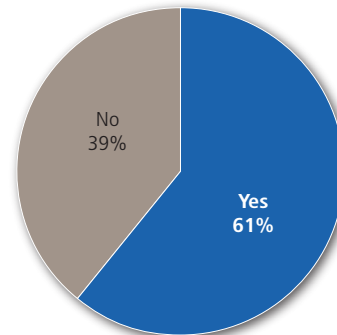
Value of Encryption Policies

Do you believe employees ignore policies about emailing unencrypted sensitive or confidential documents through insecure channels?



Use of Insecure Channels

Do you believe employees send unencrypted confidential information through insecure communication channels, such as personal Web-based email?



“Email is essential to business productivity and collaboration. It is such a significant tool that employees are inclined to circumvent policy and email sensitive information, so they can effectively perform their responsibilities in a timely manner,” said Dr. Larry Ponemon, Chairman and Founder of Ponemon Institute⁶.

⁵ “The State of Email Encryption” by Ponemon Institute, September 2011.
<http://survey.zixcorp.com>

⁶ “Zix Corporation and Ponemon Institute Survey Reveals Risk and Frustration with Outdated Email Encryption Solutions” by Zix Corporation, September 20, 2011.
<http://investor.zixcorp.com/phoenix.zhtml?c=108645&p=irol-newsArticle&ID=1608271&highlight>

About Zix Corporation

Zix Corporation (ZixCorp) provides the only email encryption services designed with your most important relationships in mind. The most influential companies and government organizations use the proven ZixCorp® Email Encryption Services, including WellPoint, the SEC and more than 1,200 hospitals and 1,600 financial institutions. ZixCorp Email Encryption Services are powered by ZixDirectory®, the largest email encryption community in the world. The tens of millions of ZixDirectory members can feel secure knowing their most important relationships are protected.

For more information about ZixCorp, call [866.257.4949](tel:866.257.4949), email sales@zixcorp.com or visit www.zixcorp.com.

Zix Corporation
2711 N. Haskell Ave.
Suite 2300, LB 36
Dallas, TX 75204

866.257.4949
sales@zixcorp.com
www.zixcorp.com

The New Threat of Mobility

Business is no longer conducted behind a desk. Mobile phones have expanded the workplace and work hours, and more users spend time on email than any other internet-enabled activity. According to a study conducted by The Nielsen Company, users spend an average of 42 percent of their mobile time using email. The next most used internet-enabled activity falls to social media at 11 percent, and all other activities are under 5 percent⁷.

With increasing dependence on mobile devices for access to data whenever, wherever, mobile email is a major concern. Of financial respondents in the Ponemon Institute study, 70 percent stated concern about the loss of information via email on mobile devices⁵.

Confidence in Email Encryption

Despite the challenges posed by compliance standards, employee behavior and mobility, a convenient solution is available – next generation email encryption. Innovative secure email technology merges the protection of encryption with advances in automated, policy-based services, easy-to-use functionality and next generation mobility.

In implementing next generation email encryption, financial institutions address old and new threats alike, prevent data loss and avoid unexpected and often high costs. Organizations are responsible for notifications and consumer protection and also face potential lawsuits; the price tag adds up quickly. In its annual survey⁸, the Ponemon Institute estimates the average cost per data breach is \$7.2 million, or \$214 per compromised record.

Beyond the prevention of financial damages, organizations also benefit from continued loyalty with customers and strategic partners. It takes years to build trust, yet only seconds to lose it. By leveraging email encryption, financial institutions secure a basic communication tool and, ultimately, protect the value of its company and its assets.

⁵ "The State of Email Encryption" by Ponemon Institute, September 2011.
<http://survey.zixcorp.com>

⁷ "How Americans Spend Mobile Internet Time: A New Look" by The Nielsen Company, May 2010.
http://blog.nielsen.com/nielsenwire/online_mobile/how-americans-spend-mobile-internet-time-a-new-look

⁸ "Assessing the Cost of Data Breach" by Jennifer Lawinski, *Baseline*, March 22, 2011.
<http://www.baselinemag.com/ca/Intelligence/Assessing-the-Costs-of-Data-Breaches-108265>