

The Case for Email Encryption

Why protecting your customers' data is a top priority

The shaky financial situation across the globe, marked by uncertainty for what the economic future holds, has had an ominous side effect—computer crime is on the rise. According to Javelin Strategy & Research, nearly 10 million Americans lost \$48 billion in 2008, due to online identity theft.¹ Also that year, more than 35 million data records were breached in the United States.²

The situation has merited the attention of President Barack Obama, who, in his first few days in office directed National and Homeland Security advisors to conduct an immediate cyber security review. "The national security and economic health of the United States depend on the security, stability and integrity of our nation's cyberspace, both in the public and private sectors," said John Brennan, assistant to the president for counterterrorism and security, in a White House news release.³

Financial and health care institutions, as well as governments — in fact, any organization dealing with personal and confidential information — are increasingly concerned with protecting privacy and preventing data breaches. Securing personal data is seen as a key priority. In a recent survey conducted by the American Institute of Certified Public Accountants (AICPA) on the most crucial technology initiatives facing businesses globally, information security management, privacy management and secure data file storage, transmission and exchange, topped the list.⁴

Not securing email is a dangerous game

But despite this growing awareness, a distressing number of financial institutions do not encrypt emails containing confidential information. According to a recent survey of 347 banks conducted by Wolters Kluwer Financial Services, two-thirds of those

¹ Reuters, January 9, 2009 - Identity theft has become more prevalent, with nearly 10 million American victims losing \$48 billion in 2008:

<http://uk.reuters.com/article/marketsNewsUS/idUKN0646389320090209>

² IT World, January 7, 2009 – Data Breaches Rose Sharply in 2008, says study:

<http://www.itworld.com/security/60271/data-breaches-rose-sharply-2008-says-study>

³ White House Press Release, February 9, 2009 - President Obama Directs the National Security and Homeland Security Advisors to Conduct Immediate Cyber Security Review:

http://www.whitehouse.gov/the_press_office/AdvisorsToConductImmediateCyberSecurityReview/

⁴ CXO Today, January 19, 2009 - Data Protection Top Priority Say Pros:

http://www.cxotoday.com/Events/Storage/India/CXOToday_Storage/Data_Protection_Top_Priority_Say_Pros/551-97914-491.html

ZixDirectory Includes

- Over 15 million protected email addresses and growing at 100,000 new recipients every week
- The FFIEC federal banking regulators and the Securities and Exchange Commission
- Over 20 state bank regulators
- More than 800 financial institutions
- 3 out of the 5 largest US health insurance companies
- More than 1,000 hospitals in the US (1 in every 7)
- Over 30 Blue Cross Blue Shield Institutions

News Alerts:

- ZixCorp's ZixVPM 3.3 voted *Network Products Guide's* 2008 Reader Trust Award Winner for Best in Secure Email
- Positioned in the Leader's Quadrant in Gartner's *Magic Quadrant for Email Encryption*

polled rely on unencrypted delivery methods to send confidential data. One-third use regular email to send personal information to customers, service providers and partners, while another third rely on regular or overnight mail, or are unsure of the method they employ.⁵ This is a dangerous game of electronic Russian roulette, as federal and state regulators are demanding tighter email security. Case in point—in 2004, St. Louis-based Southern Commercial Bank was investigated by state regulators for compromising the privacy of more than 40,000 customers when it emailed unsecured personal information, including addresses, bank account and Social Security numbers to an independent computer programmer.⁶

More security breaches expected in 2009

According to the latest annual Global Security Survey from Deloitte, financial institutions are bracing for an increased risk of security breaches in 2009, attributed to tight budgets and potential insider misconduct. “In this economic climate it is vital that firms become extra vigilant in protecting their data, and implement checks and measures to reduce the potential impact of human error,” said Mike Maddison, head of Deloitte’s security and privacy practice in an article published on iTnews.com.⁷ Occidental Petroleum Corporation learned firsthand about employee misconduct when a former worker was caught with a spreadsheet of employees’ names, addresses, birthdates and Social Security numbers, as well as other confidential information. He had sent the data to a personal email account.⁸

Savvy businesses are proactive about securing their customers’ personal information because they realize their reputations would be on the line with a data breach. According to the Ponemon Institute, a Tucson-based research firm, the average cost of a data breach for an organization is \$6.6 million—more than \$200 per compromised record.⁹ Forrester Research, the eminent technology and market research company, reports small and medium-size businesses (SMBs) are earmarking a significant portion of their 2009 IT budgets for data protection. “Data protection is the number one issue, and the availability of data follows that,” said Jonathan Penn, Forrester’s vice president of

⁵ SC Magazine (for IT Security Professionals), January 23, 2009 – Banks Not Encrypting Confidential Data:
<http://www.securecomputing.net.au/News/135154,banks-not-encrypting-confidential-data-survey.aspx>

⁶ St. Louis Post-Dispatch, February 22, 2004 - E-mail Ensnarls St. Louis-Based Bank in Privacy Inquiry:
http://www.accessmylibrary.com/coms2/summary_0286-6156087_ITM

⁷ iTnews, February 5, 2009 -- Financial institutions brace for rise in security breaches:
<http://www.itnews.com.au/News/95619,financial-institutionsgb-brace-for-rise-in-security-breaches.aspx>

⁸ Privacy Rights Clearing House, January 14, 2009 – A Chronology of Data Breaches:
<http://www.privacyrights.org/ar/ChronDataBreaches.htm>

⁹ Ponemon Institute, February 8, 2009 – Data breach cost an average of \$6.6 million:
http://blog.fulldisclosure.org/data_breach_cost/20090208-18558-Data-Breach-Cost-an-Average-of-66-Million

tech industry strategy – security, in an article on EWeek.com. “They are recognizing that protection of the data is a key part of their business. The last thing you need is to somehow erode that [customer] trust with a big data breach.”¹⁰

Penn says SMBs will be looking for ways to streamline IT management and stick to budgetary diets, and that outsourcing security will be a popular choice. “Focusing on what’s important, the data, is exactly the right way to go,” Penn was quoted in the EWeek.com article. “SMBs have been ahead of enterprises in outsourcing, but both are looking for ways to offload some of the tactical expertise.”¹¹

Encryption is—or soon will be—the law

Legislative pressure will speed the move to email encryption of sensitive information. As concerns mount over data breaches, state governments¹² and regulatory bodies¹³ are taking action. In October 2008, Nevada passed a law requiring all businesses, no matter their size or nature, to secure confidential customer information if it’s transmitted electronically.¹⁴ In Massachusetts, effective January 1, 2010¹⁵, companies are required to encrypt all personal information of state residents transmitted electronically or wirelessly.¹⁶ The safeguarding of private data, especially in regard to the Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley Act (GLBA), has become a major concern.¹⁷

¹⁰ EWeek.com, January 7, 2009 -- SMBs to Increase Security Spending in 2009:
<http://www.eweek.com/c/a/Midmarket/SMBs-to-Increase-Security-Spending-in-2009/>

¹¹ Ibid.

¹² Virginia Information Technologies Agency – “Sensitive data should not be transmitted electronically unless encryption is utilized”:
<http://www.vita.virginia.gov/security/default.aspx?id=327>

¹³ FDIC Law, Regulations, Related Acts -- c. Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access:
<http://www.fdic.gov/regulations/laws/rules/2000-8660.html>

¹⁴ Wall Street Journal, October 16, 2008: New Data Privacy Law Set for Firms
<http://online.wsj.com/article/SB122411532152538495.html>

¹⁵ The Office of Consumer Affairs and Business Regulation, February 12, 2009 – New personal security for consumers begins Jan. 1, 2010:
http://www.mass.gov/?pageID=ocapressrelease&L=1&L0=Home&sid=Eoca&b=pressrelease&f=20090212_idtheft&csid=Eoca

¹⁶ SC Magazine (for IT Security Professionals), November 4, 2008 - Nation’s First Encryption Law:
<http://www.scmagazineus.com/Nations-first-encryption-law/article/120402/>

¹⁷ CRS Report for Congress, July 31, 2007 – Information Security and Data Breach Notification Safeguards:
http://assets.opencrs.com/rpts/RL34120_20070731.pdf

Gartner, Inc., a world-leading information technology research and advisory company, predicts the Nevada law will put pressure on organizations to encrypt electronic transmissions of personal data and encourage other states to follow suit with similar legislation. Compliance means businesses, including healthcare providers, hospitality companies, insurance companies and credit bureaus, to name only a few, will have to accept only encrypted transmissions of sensitive personal or financial data from their partners. This will create a strong demand for embedded encryption and key management services. In due time, according to Gartner, legislation will make in-transit data encryption the new “standard of due care” in any law suits.¹⁸

¹⁸ Gartner Inc., October 6, 2008 – Expect Other States to Follow Nevada’s Lead in Encryption Law <http://www.gartner.com/DisplayDocument?id=771514>

ABOUT ZIXCORP

ZixCorp provides easy-to-use-and-deploy email encryption and e-prescribing services that protect, manage and deliver sensitive information to the healthcare, finance, insurance and government industries. ZixCorp’s hosted Email Encryption Service enables policy-driven email security, content filtering and send-to-anyone capability. Its PocketScript e-prescribing service provides point-of-care access and transmission of patient and payor data that improves patient care, reduces costs and improves efficiency.

For more information about ZixCorp call toll free **866-257-4949**, email sales@zixcorp.com or visit www.zixcorp.com.