



# The Case for Email Encryption

## Why protecting your customers' data is a top priority

You can't escape the headlines — 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,<sup>1</sup> up from 8.1 million victims in 2007.<sup>2</sup> Also that year, there were more than 35 million data breaches in the United States.<sup>3</sup>

Cyber-criminals take advantage of the fact that many companies don't bother to report security breaches because they don't want bad publicity, according to Shawn Henry, assistant director for the Federal Bureau of Investigation's Cyber Division. "Of the thousands of cases that we've investigated, the public knows about a handful," he is quoted by Reuters. "There are million-dollar cases that nobody knows about." Henry notes that cyber-crime is mushrooming and that as the Internet grows as a commerce tool, companies and consumers are more comfortable sharing valuable data online and in emails. "There are hundreds of billions of dollars that traverse the Internet," he said.<sup>4</sup>

While this is sobering, the world is unreservedly embracing email as a method of exchanging information. The number of worldwide email users is projected to increase from more than 1.4 billion in 2009 to almost 1.9 billion by 2013. Global email is expected to soar to 507 billion messages per day.<sup>5</sup>

As a business tool, email is invaluable. It's so vital that employees can't leave it behind at the office. According to a September 2009 Osterman Research study, 82% of employees working in large companies regularly check email from home on weekdays, 78% log in on weekends and 61% while on vacation.<sup>6</sup> The electronic exchange of

## 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*

<sup>1</sup> 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>

<sup>2</sup> Network World, January 20, 2010 -- IC3 includes identity theft in statistics:  
<http://www.networkworld.com/newsletters/sec/2010/011810sec2.html?hpg1=bn>

<sup>3</sup> 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>

<sup>4</sup> Reuters, November 24, 2009 – Cyber Breaches are a closely kept secrets:  
<http://www.reuters.com/article/idUSTRE5AN4YH20091124>

<sup>5</sup> The Radicati Group, May 6, 2009 -- Email Statistics Report, 2009-2013:  
<http://www.radicati.com/?p=3237>

<sup>6</sup> An Osterman Survey Research Report – Results of an End User Survey on the Use of Communications Tools, September 2009:  
<http://www.messagingnews.com/michael-osterman>

information underscores the fact that email is the backbone and driver of business communications today.

Of course this begs the question — with such a large volume of data streaming through, and with computer crime on a sharp upswing, is the information we send via email adequately protected?

### Encryption becoming the law

This is a question that is increasingly asked by Washington and state governments. Legislative pressure is speeding the move to demand the encryption of sensitive information sent by email. New rules at both the federal and state levels will require organizations to deploy protective technologies such as encryption to achieve compliance.<sup>7</sup>

As concerns mount over data breaches, state governments<sup>8</sup> and regulatory bodies<sup>9</sup> 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.<sup>10</sup> In Massachusetts, effective March 2010<sup>11</sup>, companies must encrypt all personal information of state residents transmitted electronically or wirelessly.<sup>12</sup> All states, except for a handful, have put in place data security breach notification laws<sup>13</sup> — an indication that the protection of electronic information is fast becoming a priority.

Gartner, Inc. 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. This will create a strong demand for embedded encryption and key

<sup>7</sup> The Industry Standard, December 15, 2009 – New Laws Complicate Security Efforts in 2010: <http://www.thestandard.com/news/2009/12/15/new-laws-complicate-security-efforts-2010?page=0%2C0>

<sup>8</sup> Virginia Information Technologies Agency – Sensitive data should not be transmitted electronically unless encryption is utilized: [http://www.accessmylibrary.com/coms2/summary\\_0286-6156087\\_ITM](http://www.accessmylibrary.com/coms2/summary_0286-6156087_ITM)

<sup>9</sup> 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>

<sup>10</sup> Wall Street Journal, October 16, 2008: New Data Privacy Law Set for Firms: <http://online.wsj.com/article/SB122411532152538495.html>

<sup>11</sup> 201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH: <http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf>

<sup>12</sup> Ibid.

<sup>13</sup> Security Law Blog, August 5, 2009 – Data Security Breach Notification Law Update: <http://www.huntonprivacyblog.com/2009/08/articles/information-security/data-security-breach-notification-law-update/>

management services. In due time, according to Gartner, legislation will make in-transit data encryption the new “standard of due care” in law suits.<sup>14</sup>

Stiff punishment is being meted out to healthcare organizations that run afoul of the strict new Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of American Recovery and Reinvestment Act of 2009 (ARRA). It calls for the encryption of all PHI sent via email. Breaking the rules will cost you. Under the new legislation, organizations will be fined up to \$1.5 million — up from \$25,000 — for violating patients’ privacy.<sup>15</sup> It also extends the effective reach of HIPAA coverage to business associates. Companies must re-evaluate their overall privacy compliance programs and implement more effective information security practices, including encryption wherever possible.

### **Not securing email is a dangerous game**

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. In a survey released in 2009, 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.<sup>16</sup>

Despite this growing awareness, a 2009 report by Imperva and Ponemon Institute reveals that more than half of the 500 businesses they surveyed admitted they did not secure Social Security numbers, bank account details, and other personal data.<sup>17</sup> According to a recent survey of 347 banks conducted by Wolters Kluwer Financial Services, two-thirds of those 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.<sup>18</sup> This is a dangerous game of electronic Russian roulette, as federal and state regulators are demanding tighter email security.

<sup>14</sup> Gartner Inc., October 6, 2008 – Expect Other States to Follow Nevada’s Lead in Encryption Law:

<http://www.gartner.com/DisplayDocument?id=771514>

<sup>15</sup> Healthcare IT News, November 2, 2009 -- HIPAA violators could face fines of up to \$1.5M:

<http://www.healthcareitnews.com/news/hipaa-violators-could-face-fines-15m>

<sup>16</sup> 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](http://www.cxotoday.com/Events/Storage/India/CXOToday_Storage/Data_Protection_Top_Priority_Say_Pros/551-97914-491.html)

<sup>17</sup> cnet news, September 24, 2009 -- Survey: Half of businesses don’t secure personal data:

[http://news.cnet.com/8301-1009\\_3-10360639-83.html](http://news.cnet.com/8301-1009_3-10360639-83.html)

<sup>18</sup> 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>

## More security breaches expected in 2010

According to a recent Global Security Survey from Deloitte, financial institutions are bracing for an increased risk of security breaches in 2010, attributed to tight budgets and potential insider misconduct.<sup>19</sup> “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.<sup>20</sup>

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 Ponemon Institute, the average cost of a data breach for an organization is \$6.6 million—more than \$200 per compromised record.<sup>21</sup> Forrester Research 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 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.”<sup>22</sup>

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.”<sup>23</sup>

## 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](mailto:sales@zixcorp.com) or visit [www.zixcorp.com](http://www.zixcorp.com).

<sup>19</sup> Deloitte, 2008 – Protecting What Matters, The Sixth Annual Global Security Survey [http://www.deloitte-ftp.fr/Publications/Mar\\_09/globalsecuritysurvey\\_2009.pdf](http://www.deloitte-ftp.fr/Publications/Mar_09/globalsecuritysurvey_2009.pdf)

<sup>20</sup> 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>

<sup>21</sup> 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](http://blog.fulldisclosure.org/data_breach_cost/20090208-18558-Data-Breach-Cost-an-Average-of-66-Million)

<sup>22</sup> 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/>

<sup>23</sup> Ibid.