



A lost or stolen laptop. A database breach. An intercepted email. Collectively, incidents like these have compromised the confidential information of hundreds of thousands of individuals. The number of people affected and the frequency of such incidents have given birth to federal and state mandates covering nearly every industry vertical. As complex as they are voluminous, each mandate contains provisions for securing (and often archiving), data, and provides best practice guidelines for safeguarding electronic communications including IM and email.

Along with the unfortunate incidents that inspire mandates, go the erosion of the offending organization's reputation and the confidence

Having said that, once this is accomplished, email is almost always the next thing on the priority list."

Though FUD and shocking headlines often hasten the implementation of new security solutions, Dasher says they don't appear to have much affect on the adoption of email encryption. "As companies mature from a security perspective, we see a more methodical approach to ensuring that customer, employee, or patient data is secure regardless of where it lives." *The 2008 Annual Study: U.S. Enterprise Encryption Trends* by The Ponemon Institute, and sponsored by PGP Corporation, found that 21 percent of organizations surveyed now have an encryption strategy applied consistently across the organization, up from 16 percent in

2007. The study also found that 74 percent of organizations have some type of encryption strategy either enterprise-wide or applied based on the type of data or applications used.

For those organizations that have not yet secured messaging, Bibby asks, "What are you waiting for? The last thing a company wants is for an email security breach to damage the reputation of that business. A company can't take a 'wait-and-see' approach; they need to be proactive in protecting the valuable information being communicated through email."

Dasher agrees, "Unprotected email/messaging poses a critical risk to a corporation's most sensitive data: customer information, financial data,

To Encrypt or Not to Encrypt (That No Longer Should The Question Be)

by Melisa LaBancz-Bleasdale

of its customers. "Compliance will always be a driver for email encryption, but more and more companies are realizing the importance of protecting their brand and reputation," observes Geoff Bibby, vice president of corporate marketing for Zix Corporation "Securing email communications gives peace of mind to both partners and customers."

John Dasher, director of product management for PGP Corporation, believes that many, if not most companies developing their enterprise security strategy now place Whole Disk Encryption (WDE) at the top of their list and email encryption second. "From a risk perspective, most companies are first concerned with locking down mobile assets—laptops, primarily," he explains. "In the U.S., breach notification laws tend to drive behavior that first focuses on WDE for these devices as they tend to become lost or stolen.

"The need for information security typically doesn't change with the size of your business. The small company who goes to PGP's corporate Web site and purchases a single copy of PGP Desktop Email is getting the same military-grade encryption that large enterprises depend on to protect their communications."

**—John Dasher,
PGP Corporation**

trade secrets, and other proprietary information. Exposure of this information can result in financial loss, legal ramifications and brand damage."

The New Era of Encryption

While older encryption solutions were difficult to deploy, required mass storage, regular administration, and complex key management, today's encryption vendors now offer streamlined, easy to use, when-you-want-it technologies to secure messaging. Hosted and on-demand encryption are gaining in popularity as organizations look for compliant ways to cut costs and IT burden. Voltage Security is seeing a significant rise in its on-demand encryption requests. "We now have over 600 customers and 4 million licensed users throughout major corporations," says Wasim Ahmad, vice president of marketing for Voltage. "[On-demand] encryption

works with all the other systems you have inside of messaging and messaging environments. It will work with MS Exchange, Notes, or e-Discovery systems. It will also work with anti-phishing countermeasures, so it's highly integrated."

Encryption solutions are also increasingly scalable. Whereas large corporations used to be the only ones that could afford, or needed, such high-level security, SMBs as well as individual users are now part of the equation. PGP supports both large and small organizations. "Let's face it, they are often working with each another," acknowledges Dasher. "The need for information security typically doesn't change with the size of

our solutions. We don't need to talk on the phone or exchange certificates. We don't need to go off and look inside directories. It's as simple as 'I am going to send this person an email and I want to send it securely.' The system will take care of creating the keys and handling the back end." Ahmad goes on to say that there is nowhere in its cloud or in its premier systems where it has keys stored, thus making it very lightweight. "That's a big difference between

encryption and keys and doing all of that in a cloud so that they're not burdened with providing help desk and distributing software."

Encryption Incentives

As part of its 2008 Annual Study The Ponemon Institute examined the costs incurred by companies after experiencing a data breach. The research showed that the average total cost—including notification costs, loss of customers, and increased dif-

"Compliance will always be a driver for email encryption, but more and more companies are realizing the importance of protecting their brand and reputation."—Geoff Bibby, Zix Corporation

State Security Breach Notification Laws

At least 44 states, the District of Columbia and Puerto Rico have enacted legislation requiring notification of security breaches involving personal information. A comprehensive list of state laws regarding security breach notification can be found on the National Conference of State Legislatures Web site at: www.ncsl.org/programs/lis/cip/priv/breachlaws.htm

your business. The small company who goes to PGP's corporate Web site and purchases a single copy of PGP Desktop Email is getting the same military-grade encryption that large enterprises depend on to protect their communications. And of course, the two work seamlessly together."

Weighing the Benefits

Among the testimonials from well-protected customers, ease-of-use tops the list. "Because of our software-as-a-service (SaaS) approach to encrypting email, it takes the burden off of the customer," Bibby states. "We can have our clients up and running in less than four hours and our service is very user friendly. We don't find ourselves being compared with other leading 'in the cloud' solutions, but with traditional software offerings. The leading 'in the cloud' encryption offerings are ZixCorp partners, so we feel very well positioned in either instance."

Ahmad agrees that making encryption easier is key today. "Ease-of-use is a common theme throughout all of

what we do and what everyone else does," he notes. "Everyone else has to store seven years' worth of keys that have to be kept for compliance reasons. We can generate keys from seven years ago, three years ago, today, tomorrow, and it's all done mathematically. That makes it very lightweight and translates to a much lower cost of operation and really good scalability."

For large, global, enterprise customers, the on-demand and hosted encryption model makes good business sense. Combining an on-site encryption solution with an as-you-need-it solution allows maximum flexibility and security. "Customers such as ING Financial Services, work with thousands of brokers and they want to have everyone they work with communicating through email encryption," continues Ahmad. ING has standardized on Voltage internally, but they don't necessarily want to have another extra 13,000 people connecting directly to their systems. Their ideal scenario is if those 13,000 brokers get provisioned online with someone else providing the

facility in acquiring new customers—was \$6.3 million per breach. The loss of customers, difficulty acquiring new ones, irreparable brand damage, and even industry fines are now all part of failing to live up to the business commitment of protecting data. Dasher believes companies need to adhere to local regulatory and compliance mandates, as well as strive to maintain customer confidence. "Increasingly, encryption solutions provide benefits in both areas. While one could argue that companies are only responding to the 'stick', i.e., breach notification laws, they are also finding a 'carrot', i.e. they can market or position as a benefit the fact that they have taken appropriate measures to safeguard customer / employee / patient data. PGP Corporation is offering products and solutions that can actually open up new venues for doing business. Encryption can make it possible to securely engage in business where it was perhaps not possible in the past." **MB/TMP**

FOR YOUR REFERENCE »

PGP Corporation
www.pgp.com

Voltage Security, Inc.
www.voltage.com

Zix Corporation
www.zixcorp.com