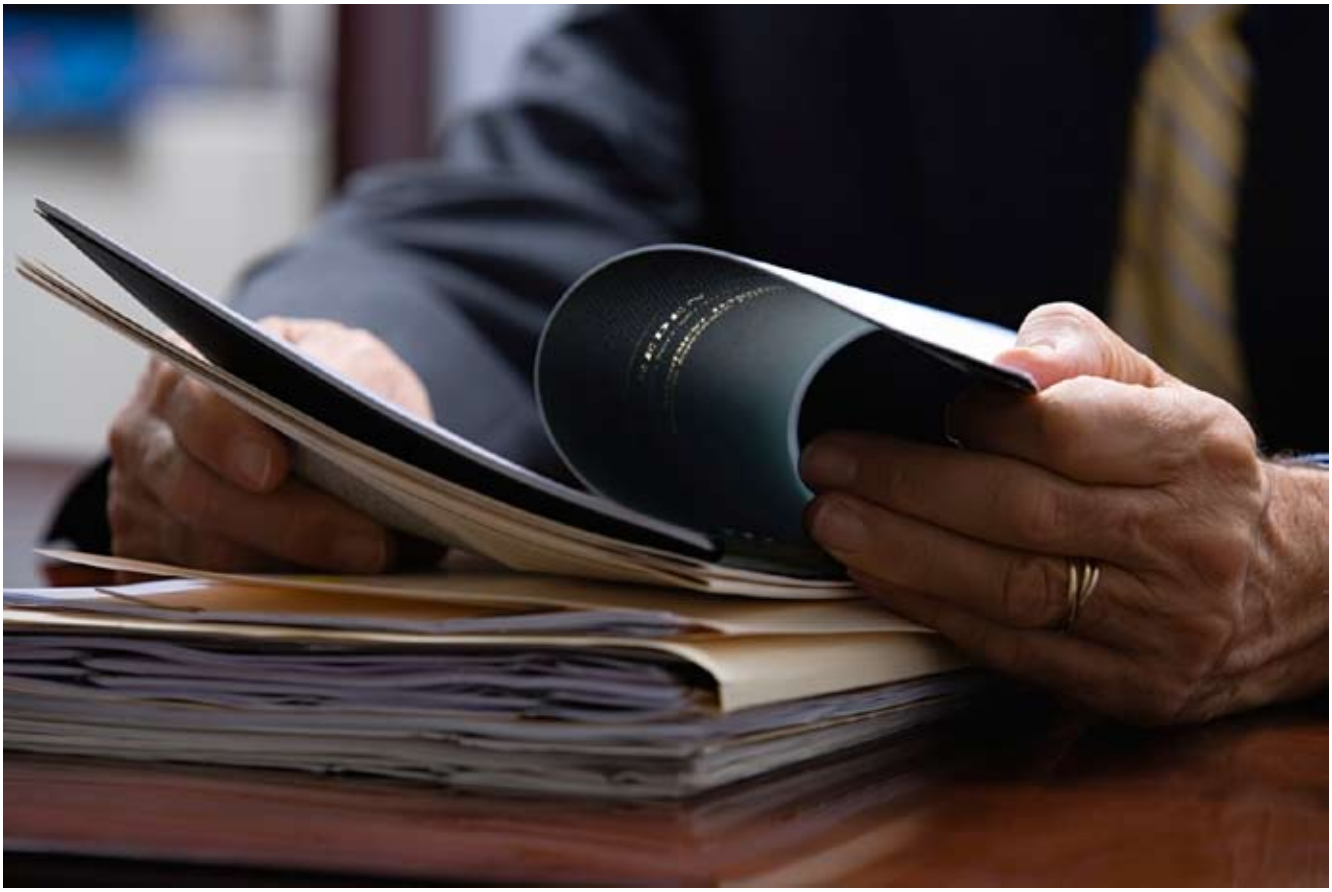
zixcorp | *Email Encryption*

ZixIntelligence Report:

Data Breach Risks and the Effect on Corporate Email



ZixIntelligence Reports provide strategic advice on issues of compliance and technology.

ZixCorp provides easy-to-use email encryption services for privacy and regulatory compliance. As the largest email encryption services provider, ZixCorp protects tens of millions of members in our ZixDirectory® and approximately 100,000 new members are being added every week. ZixCorp provides transparent, seamless secure communications with your customers, partners and regulators.

Data Breach Risks and the Effect on Corporate Email

The news media have recently reported many high-profile breaches of corporate data security. These incidents should prompt two reactions. First, IT security personnel need to focus on assessing all potential risks concerning email data security, email data privacy and email data breaches. In addition, they need to place priority on email as a significant source of data loss.

Most of the recent data breach reports have focused on incidents in which consumers' personal information was exposed while in an unprotected database. Sony Corporation experienced multiple instances of hackers breaching several of its databases, potentially exposing the personal information of more than 100 million users; some of the data was even in unencrypted plain text files. In another recent example, hackers targeting marketing services company Epsilon accessed email addresses for customers of dozens of major consumer brands.

While the above examples were related to unencrypted databases and files, we were recently reminded of the risks associated with unencrypted email. In May 2011, the SEC's employees were affected by a data breach when the Department of the Interior's National Business Center sent out SEC employees' social security numbers and other payroll information in unencrypted email.

It's a simple and sometimes overlooked fact that email is also a significant source of data loss due to the fact that it's not secure; anybody can read it. This idea has been discussed since the beginning of the Internet. In the past, email has been compared to sending a post card. Unlike sending a sealed letter, anybody can read the content of a post card.

The problem with the analogy of a post card is that it doesn't do justice to the intense risk posed by email. We imagine picking up a post card, reading it, finding nothing interesting and then putting it down. Email is very different. Email is relied on as a critical communication platform for businesses and often contains valuable information, such as sensitive customer data or company intellectual property. Email is also different, because it can be automatically and invisibly searched for relevant information without the knowledge of the sender or receiver.

Potential Materiality of Data Security

Why are data breaches significant to your organization? A data breach can seriously impair a company's brand and reputation, and if consumers or business partners lose confidence in the ability of a company to protect information, they may move their data and business elsewhere. Furthermore, as the Inside Investor Relations blog points out in a June 7, 2011, post, "hackers can bring down your networks - and your stock price." A data breach can remove a competitive advantage through the loss of proprietary information. A data privacy breach can also expose companies to considerable costs. According to a 2011 study from the Ponemon Institute, a single breach averages more than $7 million, including more than $200 per individual whose personal data is compromised. A data breach can subject companies to fines and penalties, such as

the $4.3 million fine imposed on Cignet Healthcare for violations against Health Insurance Portability and Accountability Act (HIPAA). In addition to the federal and state regulations in place, the White House issued its U.S. cybersecurity legislative proposal in May 2011, which promotes a federal standard for data breach notification to individuals.

Containing the Risks of Unsecure Email

According to a 2010 Osterman Research report, the time spent communicating via email exceeded the combined time spent using all other communication tools. Considering the risks associated with unsecure email (as referenced earlier) and that email is the most common communication platform in business, an evaluation of your email communication is a good place to start in the prevention of data breaches and the protection of your customers.

Assess your organization's outbound and inbound email traffic containing sensitive information. This will offer you a comprehensive look at the people inside and outside your organization who are sending sensitive emails with or without secure measures. With this foundation in place, you can determine if email poses a risk to your firm and clients, and if it would be appropriate to leverage encrypted email as a safe harbor.

Encryption makes the contents of every email, both the message text and any attachments, indecipherable to unauthorized individuals. Encryption uses complex mathematical algorithms to convert the original email content into an information package that cannot be read until the intended recipient unlocks the message. There are many algorithms for securing email, but they generally use hundreds or thousands of bits (information elements) in a precise sequence that is practically impossible to guess. So, as a practical matter, if an unauthorized individual intercepts a copy of an encrypted email while it is moving across the Internet, they simply will not be able to read it.

Approaches to delivery: Push, Pull, and Transparent Email Encryption

It's important to understand which mechanisms are available for delivering encrypted email to the intended recipient. Different types of recipients will have different preferences regarding how they receive secure email messages, and the solution you chose should meet the needs of your email recipients. Conventional email encryption solutions are focused on the sender; the typical means of sending an encrypted message involve desktop to desktop or "push" delivery; secure portal or "pull" delivery; or training users to trigger encryption through use of a keyword or phrase in the subject line.

Push versus Pull

In the world of email encryption, push and pull are industry terms that refer to the different technologies used for delivering encrypted email to users who do not have email encryption capabilities. Pull refers to the concept of a secure portal where users can pull encrypted email from a secure Web site. The pull method can also be thought of as pulling users back to a Web portal.

Who uses ZixCorp Email Encryption Services?

- Federal banking regulators, including FFIEC
- More than 30 Blue Cross Blue Shield organizations
- Health insurers protecting data for more than 70 million people
- More than 1,200 U.S. hospitals
- More than 1,500 U.S. financial institutions

Benefits:

- Ability to send secure email to anyone
- Built-in content scanning
- Quick deployment in less than a day
- No training for end-users
- No software to install and no additional resources needed
- Seamless integration with existing infrastructure and systems

Features:

- Policy management for regulatory compliance
- Automatic retrieval and distribution of encryption keys
- Full content scanning of subject line, message and attachments
- S/MIME, OpenPGP and TLS support
- LDAP integration
- FIPS 140-2 cryptographic engine

With pull technology, the secure portal provides a way to deliver the encrypted message to users without requiring users to install any client software. Users receive a notification message with a link to the secure portal. When users click on the link, they are taken to the portal, where they are authenticated (typically with a password), and the messages are decrypted and presented to them via their Web browsers.

It's important for the secure portal to be capable of allowing users to download attachments and reply to or forward the message. It's also important for the secure portal to allow users to compose or originate new messages, thus providing full two-way secure communication. Additionally, organizations should look for vendors that can brand the secure portals to match the company's Web site. Finally, in today's marketplace it's critical to select a vendor capable of offering seamless support for mobile devices.

Push refers to the ability to push the encrypted email directly to user email inboxes. Similar to the pull technology, push does not require users to install any client software to read the encrypted message. In this model, users receive an email message with an attachment. The attachment is an HTML file that contains the encrypted message.

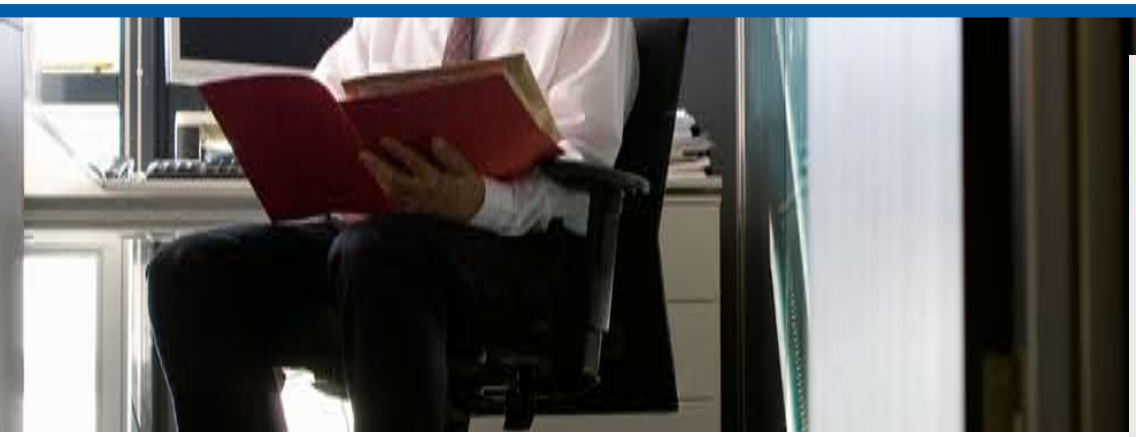
When users double click on the attachment, it launches their Web browsers where they are authenticated (typically with a password) and the message is displayed. From there, users can save attachments, as well as reply to and forward the message. In addition, most solutions provide the capability to add branding to the email.

The pull approach is ideal when organizations already have a portal that provides a variety of services and secure communications can be added as one of these services. The push approach is ideal for organizations that want to have secure messages delivered to users just like any other email message. Both push and pull provide companies with a way to send email securely to users who do not have an encryption solution.

While these methodologies may prove valuable in certain circumstances, the methodology that's least disruptive is known as transparent email encryption.

The Optimal Choice: Transparent Email Encryption

By implementing ZixCorp® Email Encryption Services, you, your customers and business partners can trust that all private and sensitive



information is transmitted securely. You also benefit from ZixCorp's industry-leading ease of use.

Developed on a principle that security must be simple-to-use to be effective, ZixCorp Email Encryption Services offer the only fully transparent email encryption. Through transparent delivery, senders and recipients can access secure email without any extra steps. Not even a password is needed.

Transparent email encryption is enabled between ZixCorp customers through ZixDirectory®, the world's largest network of email encryption members. ZixDirectory includes tens of millions of members and adds approximately 100,000 members a week.

When you plug into ZixDirectory, you immediately have access to secure email exchange with all other members. Every time a new organization joins ZixDirectory, you can automatically send them transparent encrypted email without manually exchanging any information and they can send email transparently to you. The only indication that the email was encrypted is a small footer that displays "This message was secured by ZixCorp."

Within a strategic plan to protect your organization from a data breach, email encryption is an easy component that eliminates the risk of a critical business communication tool. Consider email encryption as a convenient solution and ensure effective email security with the ease of use of Transparent Email Encryption. Customers and business partners can trust that all private and sensitive information is transmitted securely. You also benefit from ZixCorp's industry-leading ease of use.

About ZixCorp

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, Humana, the SEC and more than 1,200 hospitals and 1,500 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,
email sales@zixcorp.com,
visit www.zixcorp.com or
read blog.zixcorp.com.