The Risks of Email and the Rewards of Innovative Encryption

zix®

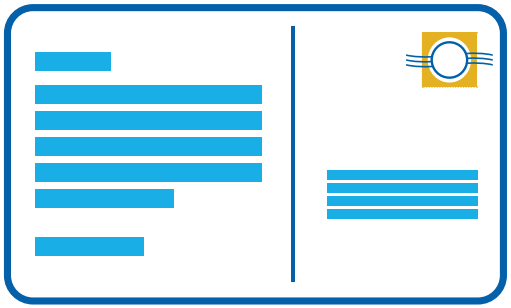
www.zixcorp.com

EMAIL IS HOW YOUR COMPANY KEEPS BUSINESS MOVING.

Your employees, from the C-suite to entry level, hit 'Send' hundreds of times every day. It's so easy to click that seemingly innocent Send button that—in the moment—you may not realize the risk. Thanks to the Snowden revelations and a never-ending cycle of breach news, we are now far more aware of the risk. Now we need to understand the challenge and how to solve it—without interrupting our business processes.

THE VULNERABILITY OF EMAIL

When you think of a postcard, it often stirs up fun memories of family vacations or adventures with friends. Postcards are sent across the country or around the world without any hesitation of a stranger reading the back. And why would you care if someone read your postcard? It only offers a simple, short note to a loved one back home.



Email is roughly the same with one critical difference. While email is as easy for a stranger to read as a postcard, the content is not as frivolous. Sure, there are emails that exchange pleasantries to old colleagues and new connections, but more importantly, there are emails that distribute valuable corporate data, such as customer information or pending contract negotiations. It's valuable to you, your customers and your partners, but it can also be valuable to your competitors and hackers who can sell your data for a nice profit. Without the proper security measures in place, it's easy for an unauthorized person to capture corporate data in email as it travels across the public Internet, and worse yet, you and your company may never know it's happening.

THE RISKS TO YOUR BOTTOM LINE

When evaluating the need for email security, it may be easier to turn a blind eye, especially for an issue that does not appear to be a business priority. And when considering customer and partner data, you may find yourself balancing corporate responsibility with the statistical odds that your valuable customers and partners discover your company has had an email breach. However, more is at stake than just a reputation hit.

According to the Ponemon Institute's annual "Cost of a Data Breach" report, the average cost of responding to and resolving a corporate data breach is $3.5 million. That high cost does not reflect potential lawsuits or the revenue loss of customer business. It also doesn't account for any regulatory fines that may be associated with expanding industry or state requirements.

If your company conducts business with healthcare organizations or financial institutions, you're well aware of the regulations outlined by The Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA). You may be less familiar with state requirements that impact your company if you operate in one of 46 states that have data breach notification laws. Complicating the issue further are other state laws that protect their residents' data even if your company does not have an office located in that state. For example, simply collecting personal data from a resident in such states as Massachusetts and then losing the data may warrant a fine.

PROTECTING EMAIL AND YOUR COMPANY: A COMPETITIVE ADVANTAGE OR A PAINFUL DISTRACTION?

Encryption makes the contents of 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. So, if an unauthorized individual intercepts an encrypted email while it is moving across the Internet or stored in message archives, they will not be able to read it. Although the algorithms are complex, the user experience must be easy for email encryption to be effective.

"The average cost of responding to and resolving a corporate data breach is

$3.5 MILLION

not including potential lawsuits, loss of customers and regulatory fines."

—"Cost of a Data Breach" Report, Ponemon Institute

THE DRAWBACKS OF A DIFFICULT SOLUTION

Not all email encryption solutions are created equal. Some can compromise ease-of-use and force users—both your employees sending encrypted email and your customers and partners receiving encrypted email—to jump through hoops. What once was a fast communication tool can become a frustrating barrier to business. The consequences of implementing difficult email encryption may prove worse than not having a solution at all.

- **Employees Workarounds**

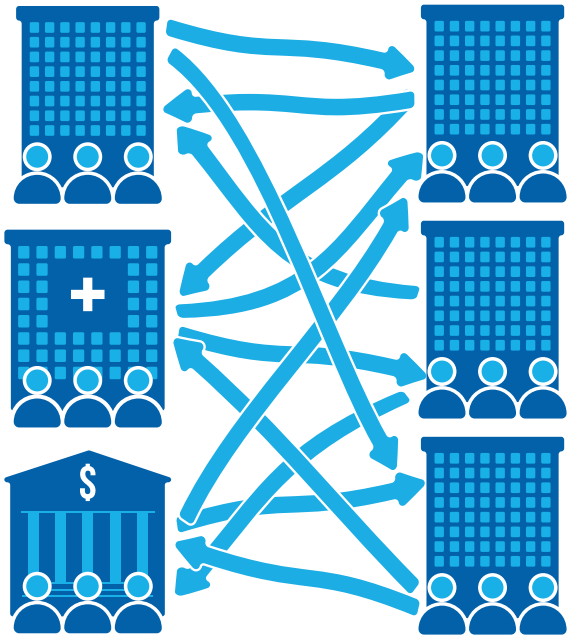
Most employees wouldn't purposely place your company, customers and partners at risk, but if email encryption interferes with executing their responsibilities, they will look for an easier way. Whether that includes using personal email or unauthorized Cloud storage such as Dropbox, employees will find a way to efficiently meet the needs of their role.

- **Complaints from Your Most Valuable Customers and Partners**

One of the advantages of email is its ubiquitous nature. Whether your company is communicating with consumers or other businesses, email is a convenient tool that most people can use without any trouble. Introduce annoying extra steps associated with decrypting email, and you'll experience plenty of customer and partner complaints to your employees, IT department and perhaps your own office.

- **Disruption to Your Business**

As much hassle is created by complaints, a worse consequence is the delay of critical business communication, because customers and partners aren't opening and replying to encrypted emails. Requiring too many extra steps for a tool that's known for its ease-of-use will certainly impact decision-making and slow business workflow.



THE BENEFITS OF AN EASY-TO-USE SOLUTION

Email encryption does not have to be difficult. Many technology advancements have made encrypted email just as easy to use as regular email. And solutions continue to adapt to meet the changing needs of your company, employees, customers and partners. Such advancements include:

- **Automatic Scanning of Employee Emails**

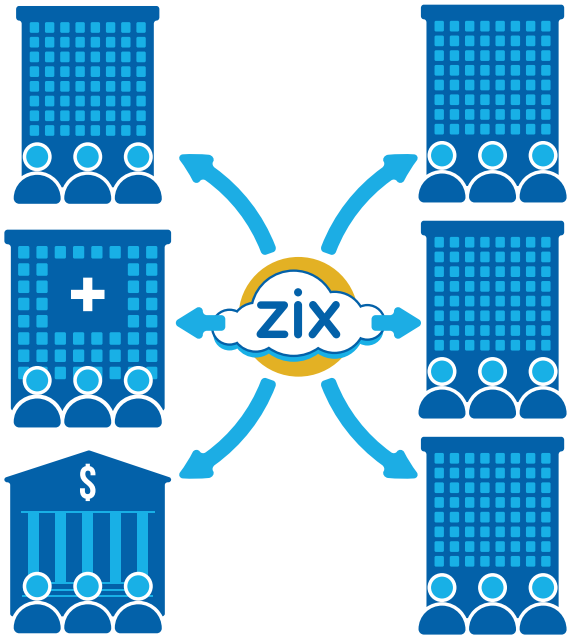
Powerful email encryption allows your employees to maintain their normal workflow and focus on their responsibilities. With automatic scanning and the use of proven and up-to-date policy filters, emails with sensitive content are encrypted without user action. Removing the hassle and taking the decision out of your employees' hands eliminates human error and better protects your email.

- **Convenient Delivery for Recipients**

If your employees don't have to take any extra steps to encrypt email, why shouldn't your customers and partners be able skip the hassle too? Innovative email encryption enables the automatic decryption of secured emails if recipients use the same platform. For others who don't use the same platform, recipients can receive the message in less than two simple steps, removing any hassle and confusion.

- **Smooth Mobile Experience**

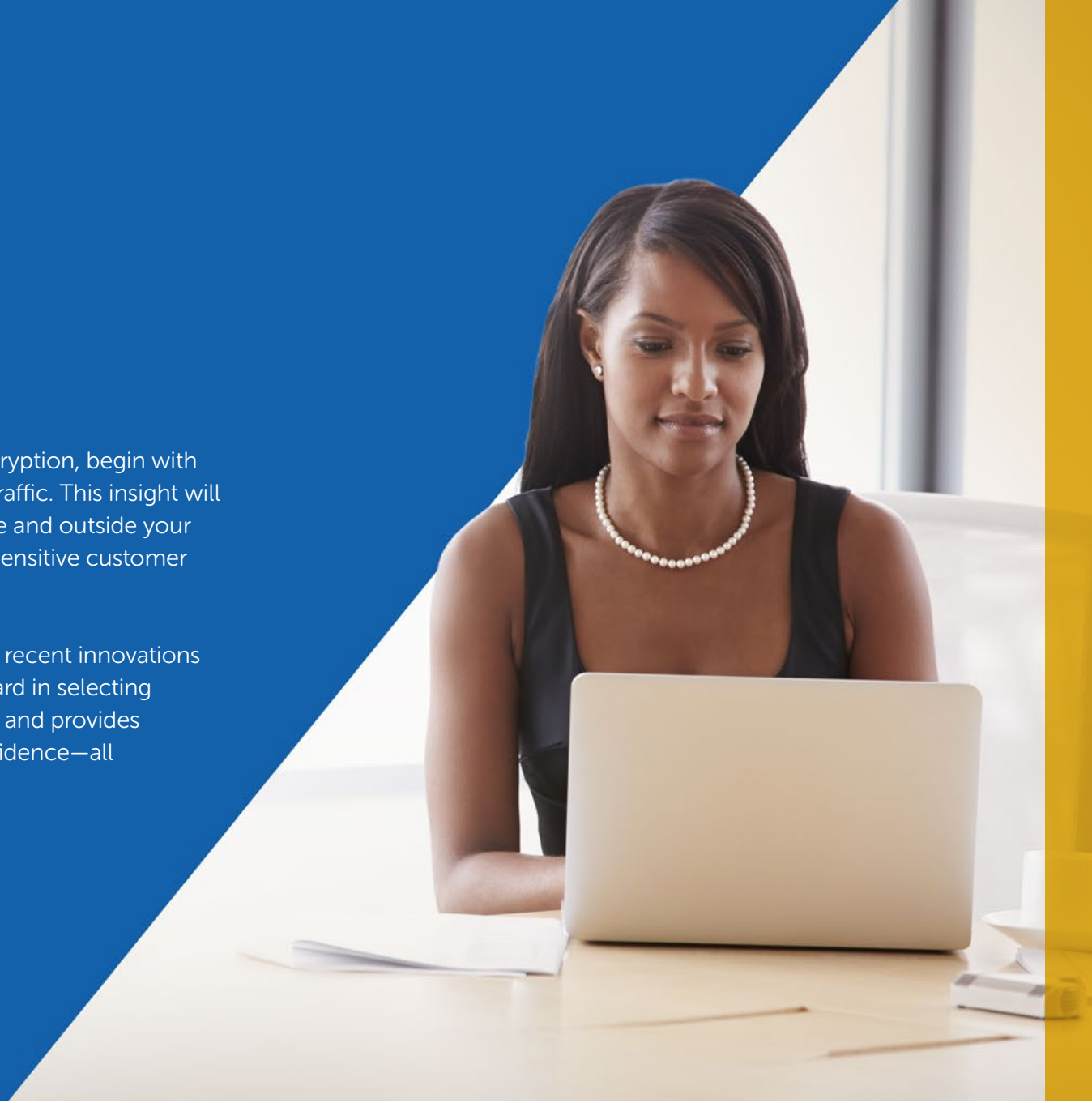
Business is no longer conducted behind a desk. Smartphones and tablets have expanded the workplace and work hours, and more users spend time on email while on their mobile devices than on any other Internet-enabled activity. With this increasing dependence on mobile devices, convenient mobile delivery of encrypted messages is a critical component to keeping business moving and making your customers and business partners secure and happy.



NEXT STEPS TO AN EFFECTIVE SECURE EMAIL STRATEGY

To understand your company's needs for email encryption, begin with an IT assessment of outbound and inbound email traffic. This insight will offer you a comprehensive look at the people inside and outside your company who are exchanging emails that include sensitive customer and corporate data.

With this foundation in place and the knowledge of recent innovations in email encryption, your company can move forward in selecting a solution that best enables secure communication and provides customers and partners with a sense of added confidence—all without hassle and business disruption.



Zix®

Zix is a trusted leader in email data protection. Zix offers industry-leading email encryption, a unique email data loss prevention (DLP) solution, and an innovative bring your own device (BYOD) email solution to meet your company's data protection and compliance needs. Zix is trusted by the nation's most influential institutions in healthcare, finance and government for easy-to-use secure email solutions. For more information, visit www.zixcorp.com

866-257-4949 . sales@zixcorp.com . www.zixcorp.com