WHITE PAPER

# Email Encryption is an Essential Best Practice

**An Osterman Research White Paper**

*Published August 2014*

***SPONSORED BY***

zixcorp®


**Osterman Research, Inc.**
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

# EXECUTIVE SUMMARY

On a typical workday, the average information worker sends a median of 30 emails and receives 100 emails while spending a median of 120 minutes doing work in an email system. The typical corporate email user spends significantly more time communicating and collaborating via email than in any other tool, including the telephone, instant messaging or social media. Add to this the fact that one in four emails contains an attachment, resulting in email's dominant role in corporate communications and the fact that it has become the primary method for sending files within and outside of an organization.

However, most email communications are sent in clear text without any sort of encryption to secure the content of those messages. Osterman Research has found that only 39% of corporate users are equipped with a manual email encryption capability and only 28% are supported by policy-based encryption. While the majority of organizations have deployed email encryption at some level, most users continue to send email – including messages that contain sensitive or confidential information – in clear text.

A failure to encrypt email significantly increases corporate risk on a number of levels:

- It increases the likelihood that data breach notification and other laws that require content to be transmitted securely can be violated.
- It increases the risk that intellectual property might be lost.
- Corporate reputation can be severely damaged, resulting in lost customers and lost revenue.

*A failure to encrypt email significantly increases corporate risk on a number of levels.*

## KEY TAKEAWAYS

To minimize the severity of the consequences that can result from unencrypted email being intercepted by unauthorized parties, all organizations should implement a solution that will encrypt email communications. While this seems like an obvious best practice, the legacy of difficult-to-use encryption solutions and a misperception that encryption will impede business processes has kept many decision makers from implementing current-generation encryption solutions. These decision makers need to evaluate current encryption solutions, particularly in light of the significant risk they face by not encrypting all sensitive and confidential email communications.

## ABOUT THIS WHITE PAPER

This white paper discusses the risks and consequences of not encrypting email and offers some practical solutions on implementing email encryption. It also offers a brief overview of ZixCorp, the sponsor of this paper, and their relevant solutions.

# ENCRYPTION IS NOT A BEST PRACTICE IN MANY ORGANIZATIONS, BUT IT SHOULD BE

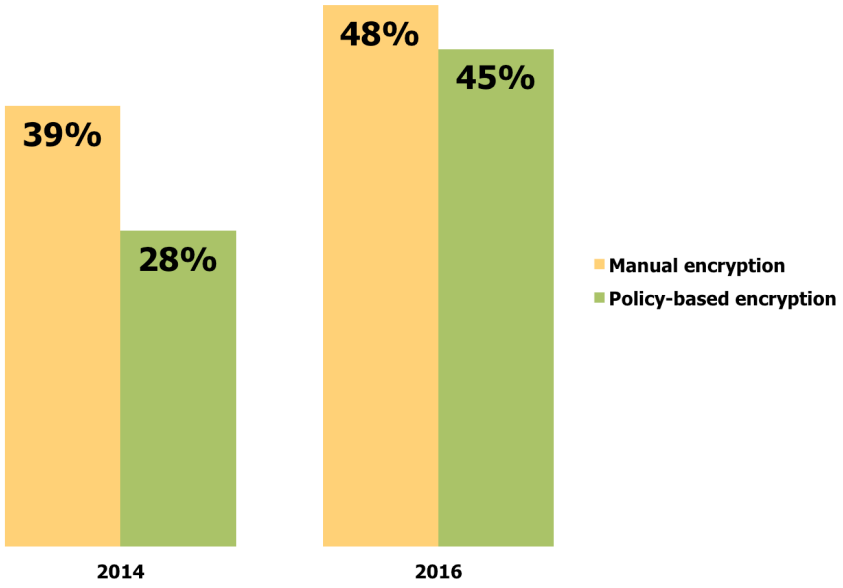
## EMAIL CONTINUES TO BE THE PRIMARY COMMUNICATIONS MEDIUM IN MOST ORGANIZATIONS

Despite the various communications and collaboration tools to which most information workers have access, email continues to be the primary tool for corporate communications. An Osterman Research survey of information workers conducted during March 2014 found that the typical email user spends a median of 120 minutes per day working in email, sending or receiving a median of 130 emails. Other Osterman Research surveys have found that email use is far greater than the use of the telephone, instant messaging and social media. Even more telling is the fact that 52% of those in the March 2014 survey indicated that their use of email is increasing compared to 12 months earlier, while only 3% reported a decrease in email use.

## MANY ORGANIZATIONS HAVE NOT DEPLOYED ENCRYPTION

Most of the emails that are sent by corporate users are not encrypted, but instead are sent in clear text that allows their contents to be intercepted. An April 2014 Osterman Research survey[i] found that only 39% of users in mid-sized and large organizations have the ability to manually encrypt email, while only 28% are supported by a policy-based encryption solution. These figures are expected to increase over the next two years, but will still result in less than one-half of corporate users provided with access to email encryption technology.

**Figure 1**
**Users Supported by Encryption**
2014 and 2016




*Source: Osterman Research, Inc.*

While this lack of encryption focuses primarily on email given its dominant role in corporate communications and collaboration, instant messages, social media and other forms of communications are also sent unencrypted in most cases. For example, a large amount of application-generated content, as diverse as payment statements or travel schedules, is sent in clear text.

## MOST OTHER INFORMATION IS NOT ENCRYPTED

Despite the fact that most email is not encrypted, including attachments sent through email, there is a significant need to securely transmit every form of communication that contains sensitive data. Even content that is normally sent in clear text, such as embargoed press releases, financial statements, or purchase orders – should be sent with encryption to prevent its unauthorized interception. Moreover, there is also value in removing access to content at a later date by enabling revocation of decryption rights, such as when an employee or business partner has left the company or should no longer be in a position to receive sensitive communications.

## BYOD/BYOC/BYOA ARE MAKING THE PROBLEM WORSE

The Bring Your Own Device (BYOD), Bring Your Own Cloud (BYOC) and Bring Your Own Applications (BYOA) phenomena are making the problem of securing data even worse. When individuals employ their own mobile devices, deploy their own cloud-based applications in which they store corporate content, or deploy their own applications to generate and process corporate data, ensuring that this content is

***There is a significant need to securely transmit every form of communication that contains sensitive data.***

encrypted in transmission or at rest becomes more difficult because IT has less control over these platforms and applications.

BYOD, BYOC and BYOA are essential elements of a broader trend toward mobile interaction with corporate applications and cloud-based services from various platforms. These trends are being driven by several factors, including employees' desire to use the latest and greatest platforms at a time when IT budgets often are not able to afford them, the trend toward telework in many organizations, and the general trend toward greater employee autonomy. Moreover, employee-specified applications and devices enable employees to be more productive, complete their tasks more quickly, and avoid the frustration and delays of dealing with an overtaxed and underfunded IT department.

# WHY IS ENCRYPTION NOT MORE POPULAR?

## THERE IS A LEGACY OF ENCRYPTION SOLUTIONS THAT ARE DIFFICULT TO USE

In a survey conducted by Osterman Research in March 2014, corporate end users were asked if their organization always encrypts sensitive data when sending it by email – only 53% of organizations responded that they do so[ii]. Further, another Osterman Research survey found that only 42% of organizations believe that their current corporate policy on email addresses use of encryption for confidential email and attachments "well" or "very well"[iii].

*Corporate end users were asked if their organization always encrypts sensitive data when sending it by email – only 53% of organizations responded that they do so.*

Many older encryption solutions were too difficult for users to employ as a normal part of their daily workflow, and so were not used to the extent they should have been – or at all – in many cases. Many solutions were not scalable and required a great deal of IT effort to maintain. Moreover, there is an enduring mindset that encryption will impede business processes and prevent customers, business partners and others from accessing content in a timely or seamless manner.

As a corollary to the point above, many think of encryption as cumbersome and onerous, and so perceive that newer solutions are saddled with these problems as well. While that is not the case for some current-generation solutions, the perception still exists for many decision makers.

## MOBILITY HAS INCREASED IN IMPORTANCE

The mobile experience is also becoming more important because of the growing trend toward BYOD, the growing number of platforms and operating systems in use, the increasing diversity of operating system versions used, etc. When evaluating email encryption solutions, it is important to consider those solutions' support being able to send, receive, encrypt and decrypt messages across a wide array of mobile devices. Ideal solutions will support all popular mobile devices without requiring the installation of plug-ins or additional software.

## NEED FOR POLICY AUTOMATION

Some outdated solutions lack efficient automation schemes and do not offer simple policy definition schemes, adding to the difficulty of using email encryption. Ideally, encryption will be policy based and solutions will automatically encrypt content – or at least inform users of the potential need to encrypt – preventing employee errors and eliminating the stress for employees who no longer need to determine if an email should be encrypted. Encryption can be triggered based on the detection of various keywords, character strings or identifiers associated with sensitive and confidential information (e.g., Social Security Numbers, credit card numbers, healthcare-related terms) in an email, file transfer, etc.

## VARIATIONS IN KEY MANAGEMENT

Any encryption solution must include some sort of key management capability, but the cost and ease of administration for these capabilities can vary widely between

solutions. Some solutions offer simple key management that requires a minimum of infrastructure and IT staff time to administer, while others employ cloud-based key management to entirely eliminate on-premises requirements.

# WHAT IF YOU DON'T ENCRYPT EMAIL?

## VIOLATION OF STATUTORY REQUIREMENTS

When email is not encrypted, one of the most serious impacts will be that sensitive or confidential data can be breached in clear violation of data breach notification laws or other requirements, such as the Health Insurance Portability and Accountability Act (HIPAA). Forty-six of the 50 US states, as well as many countries, have laws focused on data breaches that specify the steps that must be taken if sensitive content is exposed in an unauthorized manner. When a data breach occurs – such as when an unencrypted email that contains sensitive data is sent to the wrong party – it triggers a variety of often expensive consequences, such as remediation efforts, regulatory fines, lawsuits, negative publicity, etc.

## SENSITIVE OR CONFIDENTIAL CONTENT CAN BE EXPOSED

While some emails are not sensitive or confidential and so of little interest to unauthorized parties, there are cases in which email has been intercepted. For example, the revelations about activities at the National Security Agency with regard to intercepting email and other content is just one example of many in which interception of email traffic has occurred in less official ways.

## INTELLECTUAL PROPERTY CAN BE LOST

A serious consequence of not encrypting email is the potential for losing intellectual property that might be contained within messages sent outside of a company. For example, product plans, marketing plans, graphic files, product designs and other sensitive or confidential content that is not encrypted can be intercepted by parties intent on stealing this information, or it can be lost if sent mistakenly to the wrong party.

***A serious consequence of not encrypting email is the potential for losing intellectual property that might be contained within messages sent outside of a company.***

## USERS SOMETIMES MAKE MISTAKES

Another consequence from the failure to encrypt content can arise from user mistakes. For example, the type-ahead feature in most email clients all but ensures that eventually an employee will send an email to the wrong party. The same is true when employees send content via file-sharing services, when they send files via collaborative tools that permit a Web link to be sent to an external party, or when they fail to log out of an application and leave sensitive data vulnerable to access by others.

## THERE CAN BE DAMAGE TO CORPORATE REPUTATION

Yet another serious consequence of an email or other data breach is the potential damage to an organization's reputation. The negative publicity that follows a data breach, as well as the backlash that can come from regulators, investors, stockholders, prospects and customers, can seriously damage an organization's industry standing, possibly putting it out of business. Moreover, customers are less likely to do business with an organization they cannot trust, resulting in potentially serious impacts to corporate revenue in the short term and possibly more significant impacts over the long term. For example, one study found that following a retailer's data breach, one in eight customers report they will stop shopping at that retailer and 36% will shop there less frequently[iv].

Add to this the remediation costs for data breaches that can be very expensive: notifying customers of the breach, responding to angry customers' inquiries, updating security systems, establishing new policies, purchasing credit reporting services for customers, etc.

### EXAMPLES

The problems discussed above are by no means theoretical, but are occurring on a regular basis as exemplified by the following examples:

- On June 23, 2014, a contractor for Goldman Sachs mistakenly emailed sensitive client data to a Gmail account instead of a similarly named "gs.com" account. Goldman Sachs asked a federal judge to require Google to delete the email, since the mistaken recipient did not respond to Goldman Sachs' request to recover the information[v].

- In June 2014, an employee of Rady's Children's Hospital mistakenly sent information on 14,100 patients to six job applicants. The information sent included patient names, their medical records, dates and information on their insurance claims[vi].

- On May 30, 2014, an employee of Riverside Community College needed to send a file that contained information on more than 35,000 students. Because the file was too large to send through the college's email system, a personally-managed Webmail system was used, but the file was sent to the wrong address. The breached information included students' names, Social Security numbers, telephone numbers, and birthdates[vii].

## WHAT SHOULD YOU DO?

### DEVELOP AN OVERALL CORPORATE ENCRYPTION PLAN

Many organizations will want to begin the encryption process by targeting the "low-hanging fruit" that is most obviously in need of encryption. Look for privileged communication, content that if intercepted could greatly harm the companies standing with business partners and other key communications. This includes emails containing clearly sensitive documents like financial projections or draft policy statements; content that contains obviously confidential information like bids, tenders, acquisition information, employee medical records or customer financial information; and the like. This content normally represents that vast majority of the problem in most organizations and is the easiest to address. This can be followed by the less obvious use cases that might require more effort and integration.

It is essential to sell decision makers on the critical need for encryption by illustrating the consequences of lost customer information, the consequences of lost internal data, and the significant costs associated with a data breach. Moreover, organizations need to establish a set of best practices for encryption, such as automatic encryption of email between gateways or, in some cases, encrypting email between desktops.

### TRAIN EMPLOYEES ON CONSEQUENCES AND BEST PRACTICES

An essential part of any encryption plan should be to educate employees about the policies and the dangers of not using encryption. For example, encryption solutions should be used to provide feedback so that employees can learn how to handle sensitive information more effectively, such as through notifications when confidential information is included in an unencrypted email. Moreover, if employees are normally sending content that should be encrypted when sent externally, automated, policy-based systems should be deployed to handle these tasks automatically.

### IMPLEMENT POLICY CONTROLS AT THE GATEWAY AND/OR IN THE CLOUD

Encryption can be policy based and so automatically encrypt content – or at least inform users of the potential need to encrypt – based on various aspects of the message, such as the presence of a credit card number or Social Security number either in the body of the message or in an attachment. Alternatively, some

***An essential part of any encryption plan should be to educate employees about the policies and the dangers of not using encryption.***

organizations might opt for a manual capability that enables easy and reliable encryption of sensitive content.

However, some encryption solutions do not have efficient automation schemes or simple policy definition schemes. Moreover, IT generally wants policy definition for encryption to be part of a larger policy management system instead of a separate tool that requires its own interface and learning curve.

### CREATE POLICIES FOCUSED ON ORGANIZATIONAL NEEDS

In addition to the use of policy-based encryption for federal and state regulatory compliance and common sensitive information, such Social Security Numbers and credit card numbers, it is also critical to create policies based on organizational and legal requirements to protect content through encryption. This step should include a discussion of the key business risks that need to be mitigated, consequences for violating corporate data protection policies, and should also provide a detailed and thorough perspective on BYOD/BYOC/BYOA policy. The latter should include devices, operating systems and applications that can and cannot be used by various roles within the organization.

### EVALUATE AVAILABLE DEPLOYMENT OPTIONS

Finally, decision makers should evaluate the available deployment options for encryption solutions. These include traditional, on-premises software deployed on IT-managed servers; physical and virtual appliances; cloud-based services; and combinations of two or more of these in a hybrid configuration. Many organizations, particularly larger ones, will want to consider a hybrid approach to encryption, perhaps deploying on-premises solutions for headquarters staff and a cloud-based service for remote users in satellite offices that do not have dedicated IT staff.

***It is also critical to create policies based on organizational and legal requirements to protect content through encryption.***

## ABOUT ZIXCORP

ZixCorp is a leader in email data protection. ZixCorp offers industry-leading email encryption, a unique email DLP solution and an innovative email BYOD solution to meet your company's data protection and compliance needs. By providing easy to use, reliable, secure email solutions, ZixCorp has gained the trust of the nation's most influential organizations in healthcare, finance and government, including:

- All federal financial regulators
- Five divisions of the U.S. Treasury
- The U.S. Securities and Exchange Commission (SEC)
- More than 20 state regulators
- One in five U.S. banks
- More than 30 Blue Cross Blue Shield organizations
- One in five U.S. hospitals

ZixCorp offers the industry's leading email encryption by combining a unique community approach with a Software-as-a-Service (SaaS) architecture. In doing so, *Zix*® Email Encryption is easy to install, easy to maintain and, most importantly, easy to use.

Companies and organizations can protect their outbound email through ZixGateway, a content-aware, policy-based email encryption appliance that automatically scans email for sensitive information. If sensitive content is found in the subject line, message body or attachments, ZixGateway can automatically encrypt, route block or brand outbound email based on corporate policies. No training or extra steps needed.

Just as ZixGateway automatically scans email, it also automatically determines the most efficient way to securely deliver messages. When a ZixGateway customer sends email to another ZixGateway customer, the email and replies are automatically delivered securely and transparently, so that no extra steps or passwords are needed.

All ZixGateway customers belong to the Zix Encryption Network, which automatically encrypts and decrypts 100% of messages between its more than 10,000 members. The added security provides customers with unparalleled confidence that outbound email is protected against interception without any impact to its employees or member recipients. On a typical day, current members of Zix Encryption Network send around 1,000,000 encrypted messages per day. On average, 75 percent of these encrypted messages are sent through the Zix Encryption Network to other members seamlessly and transparently without any extra steps or passwords.

For recipients who do not have ZixGateway, encrypted email can be delivered through superior Transport Layer Security (TLS), ZixPort and ZixDirect.

Superior support for TLS is enabled by integrating TLS directly into ZixGateway encryption policies. In doing so, email is sent securely, and secure replies are guaranteed. Exclusive TLS benefits not available with any other competing solutions include:

- Secure, bidirectional transparency
- Simplified set-up of Mandatory TLS with the simple check of a box
- Increased delivery control using TLS only where appropriate
- Reporting capabilities offering unique visibility for compliance officers
- "Secured by ZixCorp" branding for added recipient confidence

ZixPort is a pull technology that provides a mobile-friendly secure Web portal for delivering sensitive information to customers and partners. When an encrypted email is delivered via ZixPort, your recipient receives a notification email that links and "pulls" the user to a secure messaging portal. It can be branded and integrated into your corporate portal and features unique capabilities, such as secure compose.

ZixDirect is a push technology that delivers encrypted email directly to user inboxes. ZixDirect sends the encrypted message as an HTML attachment within a plaintext email. After the user clicks on the attachment and enters a password, the message is decrypted in his/her local Internet browser.

For more information on Zix Email Encryption, visit zixcorp.com/email-encryption or contact sales at 866-257-4949.

zixcorp®

**www.zixcorp.com**

**@ZixCorp**

**+1 866 257 4949**

**info@zixcorp.com**

## REFERENCES

[i] Source: *Messaging Platform Market Trends 2016*, Osterman Research, Inc.
[ii] Source: *Survey of End Users, March 2014*, Osterman Research, Inc.
[iii] Source: *Messaging Policy Market Trends Through 2016*, Osterman Research, Inc.
[iv] http://www.interactionsmarketing.com/retailperceptions/
[v] Source: PrivacyRights.org
[vi] Source: PrivacyRights.org
[vii] Source: PrivacyRights.org