zixcorp

THE CASE FOR ZIXDLP

How Organizations Protect Themselves and Their Employees Against Human Error When Sending Emails

Easy communication is an asset that adds value by maximizing the productivity of employees at all levels of an organization and across all functions. Studies show that email has become the primary method for file exchange. Not only is the use of email vital, but also one in four emails now has an attachment. In fact on average, 98% of the information transferred via email is contained within attached files.

However, there is a downside with email. It was designed in the days before we realized criminals would hack in to our emails for all kinds of reprehensible reasons. Sadly, with the convenience of clicking “send” comes the potential to expose an organization to immeasurable harm to its clients, employees, intellectual property and trade secrets, and – especially – to the organization’s brand image and good name. Just a few short years ago, organizations believed that only regulated industries, such as healthcare under the Health Insurance Portability and Accountability Act, needed to protect their data. The recent breaches involving government, non-profits and businesses of all types have shown that no organization is immune to a data breach and potential scandal.

Corporate Embarrassment

In 2015, Carnegie Mellon University delighted 800 applicants for its master’s program in computer science when it emailed them saying:

> “You are one of the select few, less than 9 percent of the more than 1,200 applicants, that we are inviting. ... Welcome to Carnegie Mellon!”

A few hours later the admissions office was forced to send a new email with the subject line:

> “CORRECTION OF PRIOR EMAIL / REVOCATION OF OFFER OF ADMISSION TO MS IN CS PROGRAM.”

Needless to say, the hurt expressed by many of the applicants and the bad publicity generated for Carnegie Mellon continues to the present day. Yet that same kind of human error occurs over and over again: so far at Johns Hopkins, Cornell, Drexel University, MIT, UC San Diego, UC Berkeley, University of North Carolina at Chapel Hill, New York University, Kellogg School of Management and many more.

In fact similar email-related human errors occur at government agencies, hospitals and corporate businesses worldwide on a regular basis.

For example, Goldman Sachs felt it necessary to go to court after one of their contractors sent “highly confidential brokerage account information” to a wrong recipient. By going to court, the incident became public knowledge and, although down to human error, Goldman Sachs still suffered bad publicity. Something very similar happened to the Rocky Mountain Bank a few years earlier when an employee not only sent a customer’s loan statements to a wrong recipient, but also inadvertently attached an extra file that contained confidential information on 1,325 individual and business customers that included their names, addresses, tax identification or Social Security numbers and their loan information too.

The Office of Civil Rights, part of the U.S. Department of Health and Human Services, reports that in 2015, no less than 39 healthcare providers and insurers suffered email related breaches where more than 500 patient records were exposed. For example, the University of Pittsburgh Medical Center (UPMC) Health Plan inadvertently sent an insecure email with protected health information (PHI) to an incorrect, third-party email address. The breach included the PHI of 722 individuals and included names, dates of birth, member identification numbers, phone numbers, types of insurance, and members’ primary care providers.

Loss of Trust

A study published at the end of 2015 found that nearly two-thirds (64%) of consumers surveyed said they are unlikely to shop or do business again with a company that had experienced a breach where financial information was stolen; and almost half (49%) had the same opinion when it came to data breaches where personal information was stolen. Separately, the Ponemon Institute states that in addition to blemished reputation, the loss of customer loyalty does the most damage to the bottom line, not least because of increased customer churn.

58%
of senior managers
have accidentally sent the wrong person sensitive information

Source: Stroz Friedberg, “Information Security Risk in American Business”

Notification Requirements

In the U.S., forty-seven states have enacted legislation that requires private businesses, government and educational entities to notify individuals of security breaches of information involving personally identifiable information (PII). In addition to incurring potential monetary penalties, businesses can suffer grave damage to reputation as these mandatory notifications become public knowledge. Plus civil suits are now becoming more common.

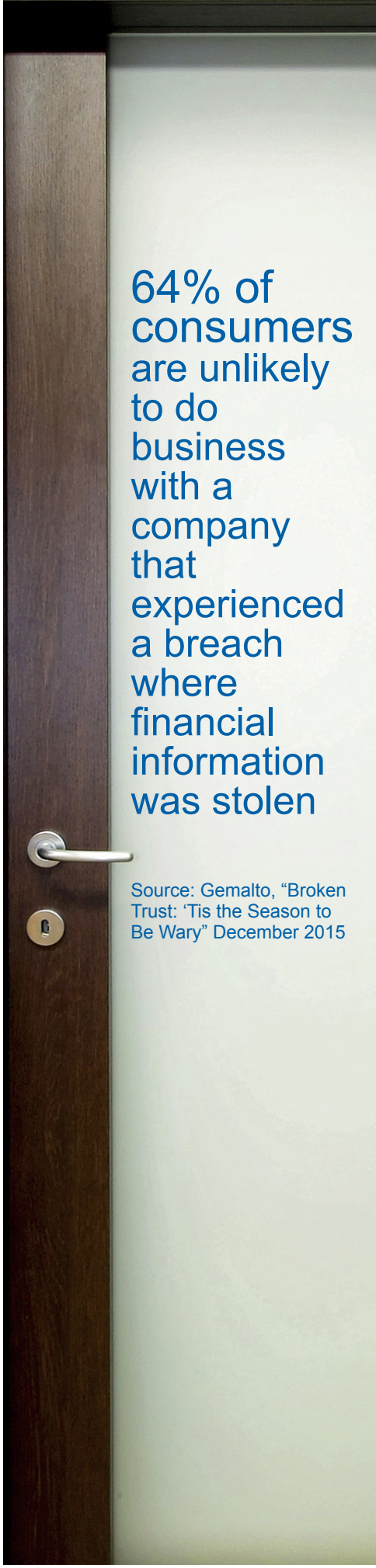
Breaches occur in many ways, and according to Dr. Larry Ponemon the average cost of a data breach is now $3.79 million, equating to $154 per record lost. Some companies are now considering cybersecurity insurance; however this on its own is not a guaranteed panacea: A provision known as the “Mistake Exclusion” precludes coverage in the event that the insured fails to maintain adequate data security safeguards. For example, insurer Columbia Casualty Co. recently sued its client Cottage Health System for being negligent in not maintaining what Columbia regarded as basic security procedures.

Complying with Regulations

Whatever business or market your organization operates in, there are almost certainly regulations that require you to protect sensitive data. In the United States, we have all heard of the Sarbanes-Oxley Act (SOX) and the Gramm-Leach-Bliley Act (GLBA) both of which mandate the secure storage and transmission of sensitive financial information. So too the Payment Card Industry Data Security Standard (PCI) is designed specifically to protect credit card details. There are regulations for protected health information (HIPAA), the title industry (TILA-RESPA), the American Bar Association’s Model Rules of Professional Conduct, and many more. All of these regulations, whether in North America or around the world, mandate that organizations protect client, investor and employee sensitive data by not revealing it to unauthorized people.

Protecting Your Brand

Zix has market leading policy and content scanning capabilities that have been developed over the past 15 years and that are now used by millions of users working for thousands of Zix customers worldwide. ZixDLP leverages that expertise to deliver a quarantine capability, the ability to discriminate between sensitive information being emailed by or to the correct people; or by or to the wrong senders or recipients. It gives your business or organization a safety net, a second chance to be absolutely sure that the right information is being sent to the right people, and that your brand and reputation will be protected.



64% of consumers are unlikely to do business with a company that experienced a breach where financial information was stolen

Source: Gemalto, “Broken Trust: ‘Tis the Season to Be Wary” December 2015

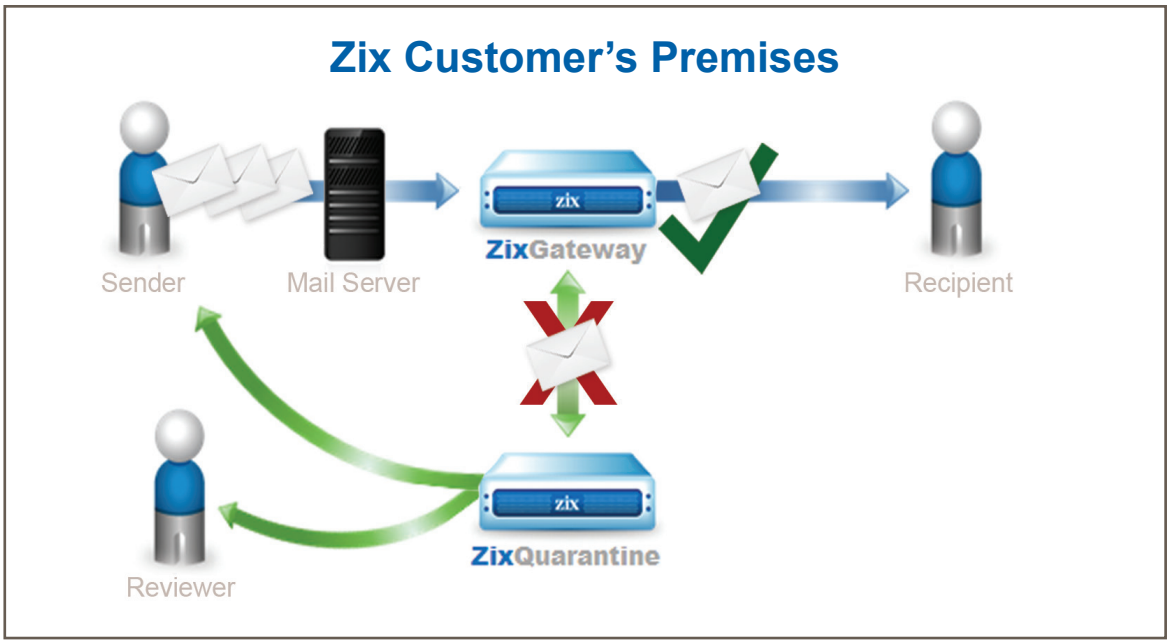
The quarantine system and its intuitive interface allow administrators to:

- Define policies easily and create custom policy filters for quarantining email messages
- Manage quarantined messages conveniently using flexible searching and filtering options
- Release or delete individual or multiple quarantined messages with one click
- Review reports that monitor quarantine activities and trends
- Automate custom notifications informing employees of quarantined messages.

In addition to an easy-to-use administrator interface, ZixDLP provides a convenient end user experience. When an employee uses the company email system to send an email to a recipient outside the company, the message and attachments are scanned. If a policy is triggered, the email is sent to a quarantine system, and the employee receives a notification message. Embedded in the notification is a link to where the user can easily review the quarantined email message. Administrators can give employees the capability to review each quarantined email, to release or delete it, or to draft a new version. Not only does the sender receive the quarantine notification, but also a nominated security officer who additionally can monitor the performance of ZixDLP and make decisions regarding the revision or release of suspect emails.

Here is how it works:

1. The sender creates an email in the normal way.
2. When the sender presses the “send” button, a ZixGateway – either physical or cloud based – scans the email and attachment in real time to detect sensitive information, the sender identity and the addresses of the recipients.
3. If flagged, the email is quarantined and notifications are sent to the sender and to a nominated security manager, these notifications containing the reasons for the quarantine hold.
4. If deemed safe, the email is forwarded to the public Internet in the normal way.



This means that organizations no longer need to worry about human error, about employees accidentally sending sensitive information to wrong recipients. It also reduces stress levels among employees who now do not need to overthink the sending of their emails and reducing their productivity while they review every email in detail.

Take the Next Step

With ZixDLP email protection, your organization can be protected against human error and the harm that can be done by sending sensitive information to the wrong recipients. Not only protecting your brand, but also protecting you against civil litigation and potential regulatory penalties. It takes years to build trust and customer loyalty, yet only one slip to lose that trust with an email data breach.

Find out more about Zix's market leading email data loss prevention solution by contacting Sales@zixcorp.com.

www.zixcorp.com
866-257-4949