InformationWeek :: reports

Reports.InformationWeek.com

December 2011

Next

Email and Data Loss

Email encryption, rights management, email gateways and full-on data loss prevention systems can keep corporate data secure. Consider the pros and cons of each to determine what's best for your business.

By Jim Rapoza

Presented in conjunction with

SECURITY dark READING
Protect The Business Enable Access

Report ID: S3821211

TABLE OF CONTENTS

Figures

ABOUT US

InformationWeek Reports' analysts arm business technology decision-makers with real-world perspective based on qualitative and quantitative research, business and technology assessment and planning tools, and adoption best practices gleaned from experience. To contact us, write to managing director **Art Wittmann** at *awittmann@techweb.com,* content director **Lorna Garey** at *lgarey@techweb.com,* editor-at-large **Andrew Conry-Murray** at *acmurray@techweb.com,* and research managing editor **Heather Vallis** at *hvallis@techweb.com.* Find all of our reports at *reports.informationweek.com*

Jim Rapoza

InformationWeek Reports

For more than 17 years, Jim Rapoza has been using, testing and writing about the newest technologies in software, enterprise hardware and the Internet. He served as the director of an award-winning technology testing lab based in Massachusetts and California. Jim is also the winner of five awards of excellence in technology journalism, and was the co-chair of a summit on technology industry security practices. He is a frequent speaker at technology conferences and expositions, and has been regularly interviewed as a technology security expert by national and local media outlets including CNN, ABC, NPR and the Associated Press.

EXECUTIVE SUMMARY

Data loss prevention (DLP) should be a major concern for all companies, and one of the major conduits for the accidental or intentional leakage of data is enterprise email systems. There are many DLP models that can be put into place, including email encryption, rights management, email gateways and full-on DLP systems. Unfortunately, none of these approaches is bulletproof, and companies will have to perform a risk assessment to determine how much risk they can ensure relative to how much money they can spend to mitigate that risk. This report details the benefits and drawbacks of the different methods of preventing data loss through corporate email systems, and provides recommendations for making the right choice for your company.

What's the Big Deal About a Little Leaked Email?

The ease with which a massive amount of Defense Department information was smuggled to WikiLeaks in 2010 put the fear of data leakage into government agencies and businesses alike. But it doesn't take hundreds of thousands of documents smuggled out on removable media to make for a serious data breach. All it takes is a hit—intentional or not—of the send button on your corporate email system.

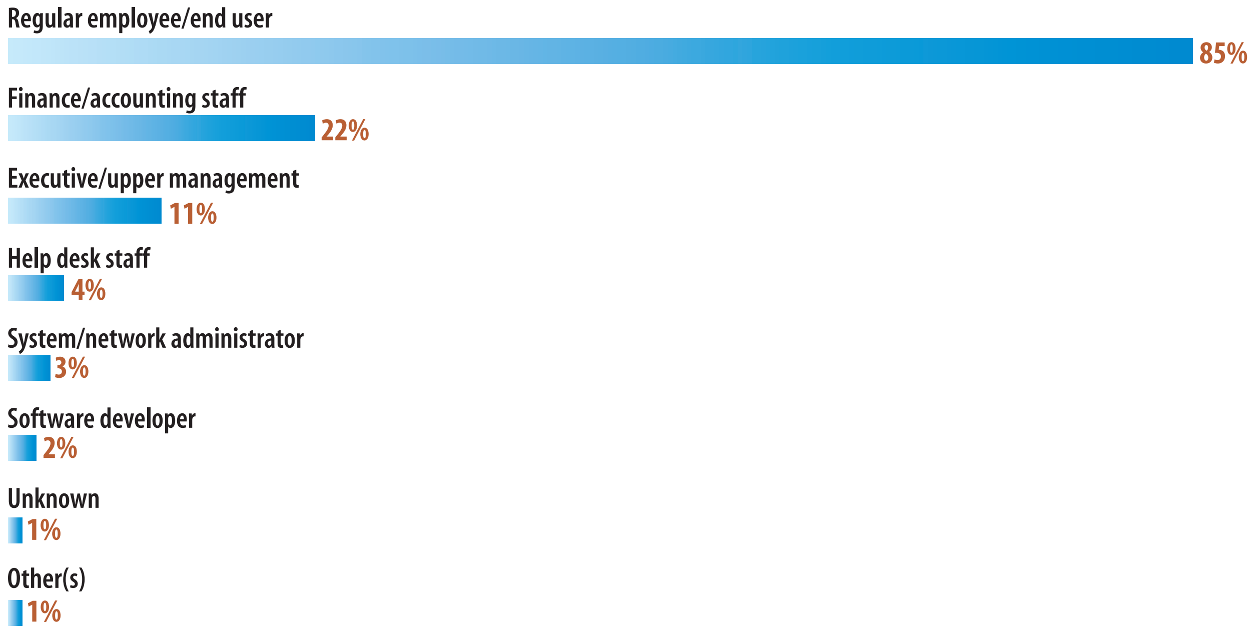
A single email doesn't seem like much to worry about. After all, how much damage can one email cause? A lot, as many companies have discovered in the past few years. All it takes is one email for a disgruntled employee to send product secrets to a competitor. And just one email sent to the wrong person can result in a company's dirty laundry being aired on public social networking sites. The possibilities, unfortunately, are almost unlimited.

Putting usage policies and rules into place will let employees know exactly how company information should be handled and communicated via email, instant messaging (IM) and text messaging, and will lay out the consequences for not abiding by the rules. But a policy can't stop a mistake once it has been made, and it won't slow an insider determined to expose sensitive data.

Figure 1

Sources of Internal Threats

According to the Verizon 2011 Data Breach Investigations Report, it is regular employees and end users—not highly trusted users—who are behind the majority of data compromises.

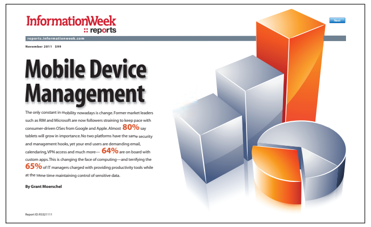


Data: Verizon 2011 Data Breach Investigations Report

Companies need to take purposeful, proactive steps to ensure that their email systems are protected against data leakage. Indeed, it's a requirement for enterprises that must comply with various industry regulations. The good and bad news is that there are

Previous Next

Table of Contents



InformationWeek :: reports

reports.informationweek.com

November 2011 $99

Mobile Device Management

The only constant in mobility nowadays is change. Former market leaders such as RIM and Microsoft are now followers straining to keep pace with consumer-driven OSes from Google and Apple. Almost 80% say tablets will grow in importance. No two platforms have the same security and management hooks, yet your end users are demanding email, calendaring, VPN access and much more— 64% are on board with custom apps. This is changing the face of computing—and terrifying the 65% of IT managers charged with providing productivity tools while at the same time maintaining control of sensitive data.

By Grant Moerschel

Report ID: R3321111

Related Report

Learn about the latest trends in mobile device management and security, and delve into mobile device policy development.

Download

many different approaches to take—from email encryption to rights management systems to gateways that scan messages for sensitive content to massive data loss prevention (DLP) systems that try to lock down all ways that data can leak from a business.

In this report, we'll look at all these approaches and evaluate their strengths and weaknesses to provide a clear picture of the current state of tools to prevent messaging data loss.

Email Encryption

One of the oldest forms of securing messages is through email encryption. In its simplest form, email encryption can secure a message so that only the sender and recipient can see its content. If the encrypted message finds its way into the hands of someone who shouldn't have access to it, there is nothing he or she can do with it.

Traditionally, email encryption has worked through standard public key systems. In this model, two separate keys are used: one to lock or encrypt the plain text and the other to unlock or decrypt the encrypted text. One of the keys is public, the other is private.

In the past, encrypting an email to be sent securely to someone was not always easy—it required an exchange of public keys and a mutual understanding between the messaging parties that encryption would be used. This complexity often led to the avoidance of email encryption.

Recent advances in email and email security systems have helped ease some of these burdens. Many modern systems can be set to automatically encrypt all communications within a company (though external emails remain open). Today's encryption systems also take advantage of the cloud and advanced Web application technology to remove some of the barriers to email encryption. In these systems, public keys are maintained on a cloud server, and online browser-based applications can be used to decrypt and view sensitive communications.

This makes email encryption much more user-friendly, but there are still some drawbacks. Probably the biggest is that email encryption exists mainly as an intentional system to protect specific messages. A sender must say, "This message needs to be secure; I'll use encryption on it." This works well in certain situations, but does nothing to prevent a malicious insider from leaking information. In fact, a disgruntled insider could use an external email encryption system to send out sensitive data and avoid detection.

Rights Management

Another approach to prevent data leakage through email and other communications channels such as IM is rights management.

Rights management systems are usually client/server products used to define and control policy from a central system that then dictates to the email client (typically Microsoft Outlook) how content can be viewed, shared and distributed.

Used properly, rights management systems can provide a very high level of control and can work to prevent both intentional and unintentional data leakage. For example, a human resources employee could use rights management capabilities within the email client to send out a message where forwarding and reply-all capabilities are disabled. Or, the HR user could determine that the message cannot be sent to external email addresses.

Rights management can also extend beyond the mail client to turn off other system capabilities, such as the ability to print a message or take a screen shot. Some rights management systems even include time bomb capabilities—a message and its content will be sent to an external user, but the user loses access to the content after a certain amount of time has passed.

Rights management systems are extremely powerful and can be very effective, especially when it comes to the prevention of accidental data leakage. However, these systems are not foolproof. For example, while they make it possible to control how, say, a message from HR is distributed, the person from HR still needs to remember to enable the controls when he or she sends out the message. Also, rights management systems often do little to stop someone from crafting an email containing sensitive information and sending it to someone outside the company. And while turning off printing and screen-capture capabilities prevents one way of capturing sensitive data from a screen, there's little a company can do about a strategically aimed stand-alone digital camera or smartphone.

Email Gateways

Both encryption and rights management tools can work well to protect data, but they rely on the actions of individuals. And therein lies the catch. Many companies need a more automated system.

Over the years, security gateways have become popular for keeping the bad stuff from making its way into a company. These gateways typically sit in tandem with the mail server and scan incoming messages for viruses, spam, phishing attacks and other malicious payloads.

Figure 2

Theft or Illegal Access of Company Data and Other Resources

Cisco's "Data Leakage Worldwide White Paper: The High Cost of Insider Threats" included the results of a global security survey showing that:

6%	of end users have known someone at work who has accessed someone else's computer to look for unauthorized personal or corporate information.
5%	have accessed someone else's computer to look for unauthorized personal or corporate information.
3%	have known someone at work who has stolen computers or other equipment containing corporate data.
3%	have known someone at work who has sold corporate data to another party for profit.
1%	have stolen computers or other equipment containing corporate data.
1%	have sold corporate data to another party for profit.
89%	of respondents said "none of the above" applied to them.

Data: "Data Leakage Worldwide White Paper: The High Cost of InsiderThreats"

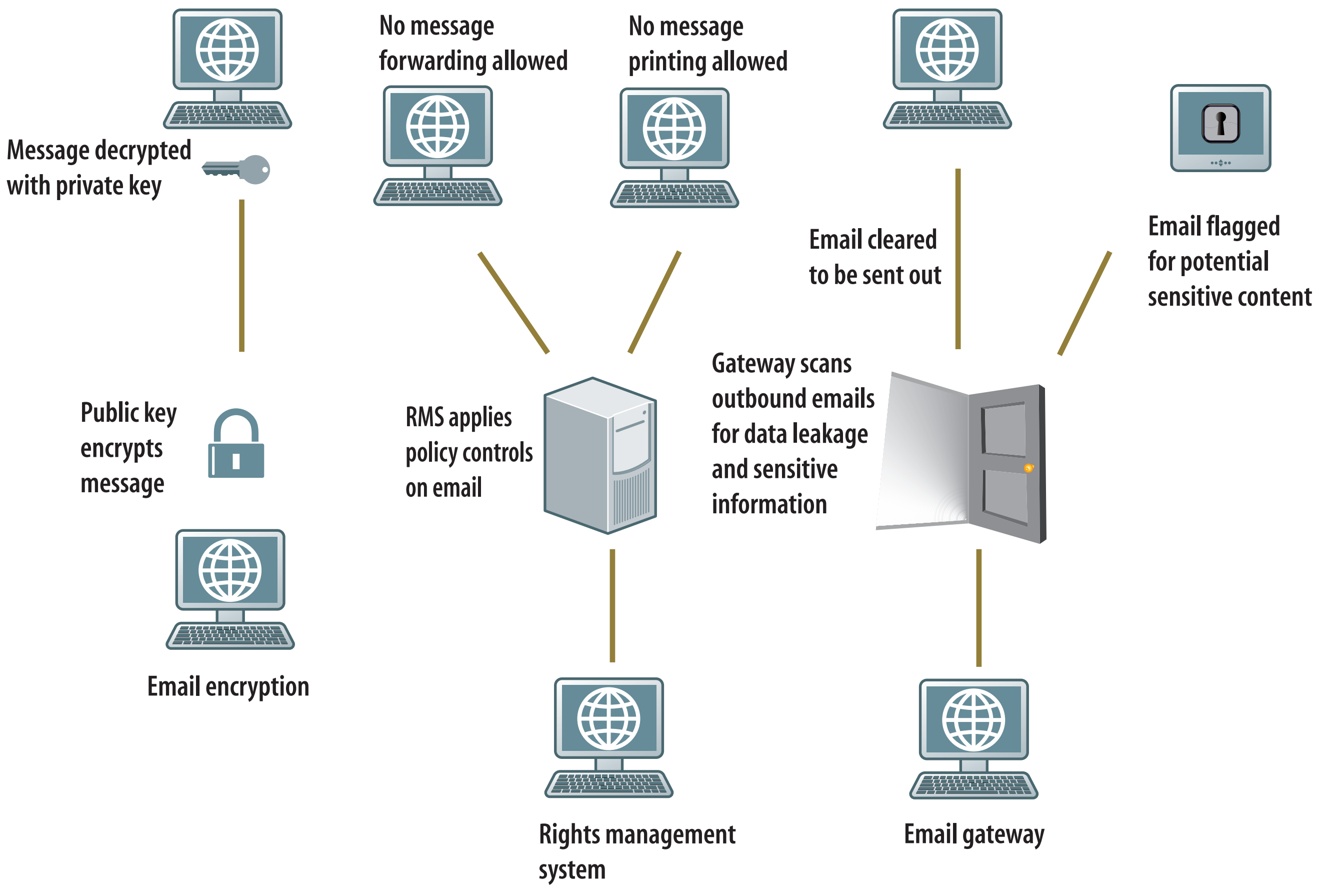
Of course, it didn't take long for vendors of these products to figure out that, if these gateways could scan the content of incoming messages, they could also scan the content of outgoing messages. And that's exactly what most email gateways now do. Businesses can configure them to check all outbound emails for certain keywords or file attachments. For example, words like "sensitive" or "secret" in the subject or body of certain messages might raise a red flag. The gateways could be set to scan attached Word or PDF documents for particular words or phrases. They can also be used to stop outbound emails containing profanity from leaving the company, and can look for common patterns in message content that may portend a security breach, such as credit card or Social Security numbers.

Depending on the system, when the gateway flags an email, it might send a reply to the sender to let him or her know there is a potential problem and even provide directions to solve it. Or it might hold the message in a quarantine area until a manager can approve it to be sent on or look into why the new guy in sales is sending a list of top clients to the firm's main competitor.

Figure 3

Three Approaches to Stopping Data Loss in Email

One of the oldest forms of securing email messages is encryption, the process of securing a message so only the sender and recipient can see its content. Rights management systems are typically client/server products that define and control policy from a central system that then dictates to the email client how content can be viewed, shared and distributed. Security gateways typically sit alongside the mail server and scan incoming messages for spam, phishing attacks and other malicious payloads.


Message decrypted with private key
Public key encrypts message
Email encryption
No message forwarding allowed
No message printing allowed
RMS applies policy controls on email
Rights management system
Email cleared to be sent out
Email flagged for potential sensitive content
Gateway scans outbound emails for data leakage and sensitive information
Email gateway

Data: *InformationWeek/Dark Reading*

REAL WORLD

Implications of Communications-Related Data Leaks

Sending sensitive information through unsecured email can be a problem for many businesses, but it isn't a matter of national security—except when it *is* a matter of national security.

This was the case when former Vice President Cheney was receiving treatment at George Washington University Hospital and a Secret Service agent accidentally sent detailed information on the vice president's visit through a clear-text, unencrypted email. Anyone monitoring the communications could have potentially learned everything about Cheney's visit, which would have affected the ability to keep him secure. The unencrypted message was discovered by the hospital's data loss prevention system.

In late November, a public relations professional accidentally leaked details of a PR strategy for the launch of Pottermore, the online followup project to J. K. Rowling's *Harry Potter* books. The PR pro inadvertently emailed a confidential memo outlining the top-secret event to nearly a dozen newspaper journalists. The information was included in a Word file attached to the bottom of invitations sent to the journalists for a press call.

Another problem with email data loss occurs when workers go outside accepted communications systems, often not because they want to leak information but simply because they find it an easier way to communicate.

Human resources firm TriNet found this to be the case when it brought in a data loss prevention system to monitor all communications. Many employees were using third-party webmail systems and cloud-based file services to share information because these services were more convenient than the company's secure communications system.

Of course, alternative communications channels can sometimes lead to data leaks, even when they aren't intended for sending out company data at all.

When information on President Obama's Marine One helicopter was found on a server in Iran, for instance, the data leak was traced to a worker's system at an avionics firm. The employee had installed a P2P program on his system to facilitate personal file sharing. Unfortunately, though, as many P2P programs tend to do, the application exposed much more then his music files.

This is another good example of why a system that can watch all forms of Internet-based communications can be a vital link for businesses aiming to prevent data loss. These systems can look beyond simple email to check all traffic for the presence of sensitive files and content.

—Jim Rapoza

FAST FACT

5%

Cisco survey respondents who have accessed someone else's computer to look for unauthorized personal or corporate data

Along with prevention of data leakage through email, these systems can be very useful for businesses following strict regulatory compliance requirements. In these situations, the gateway can, for example, be used to look for Health Insurance Portability and Accessibility Act violations of content leaving a medical facility.

Of course, email gateway systems have their drawbacks as well. Probably the biggest negative is a high incidence of false positives.

If a gateway is constantly blocking legitimate emails, security managers may reset the filters to stop false positives. This may, in turn, increase the possibility that sensitive information will make it past the gateway.

Or a business faced with false positives may choose to put the gateway in a monitor-only mode. In this case, suspicious emails are flagged but still sent on. In cases where there really was a security breach via email, you'll know who sent the message but the damage will already have been done.

Full-On DLP

When it comes to physical security, some businesses protect themselves by just locking the doors. Others use surveillance video or contract with an alarm firm. And some companies use all of the above, plus physical guards walking the company floors.

In much the same way, full-fledged DLP systems aim to provide near-total protection against data loss and intentional data leakage—or, as is often true in the case of total physical security, at least give businesses the feeling they are doing everything they can to protect their sensitive information.

Complete DLP systems will typically include many of the capabilities already covered in this report, including email encryption, rights management and gateway-based content scanning. They will also often include network policy management and next-generation firewall capabilities to control what Internet-based applications are used and limit what content is sent to these applications. In addition, these systems have the ability to block, monitor and/or control content sent to external email services and the use of other communication channels such as IM.

These DLP systems can also go beyond the actual communication channels themselves to control access to the content wherever it is kept within the company. So, for example, they can limit access to content in a storage system to just specific personnel or to viewing only within the company network. These systems also have physical system-level controls, such as blocking the use of USB ports.

Of course, you pay for this level of protection. Implementing a full DLP system in a large company can easily run well into six figures. Also, with the regular need for configuration, management, monitoring and alert handling, administering one of these systems can involve quite a bit of work and resources. Further, despite their breadth and depth of capability, full DLP systems are not bulletproof. An insider dedicated to leaking data can still find ways around these systems.

Challenges Ahead

You might think the constant progress of technology means more innovative DLP methods will be coming down the pike to prevent sensitive data from being leaked through email and other communications channels. But technology is advancing in ways that will make preventing data loss a much tougher task.

> “More innovative DLP methods may be coming, but technology is advancing in ways that will make preventing data loss tougher.”

Many companies are increasingly dealing with the demands of employees (and upper management) who want to use their own devices for business tasks. This lets workers take advantage of the latest smartphones and tablets—systems that are likely generations newer than the company could provide—but also adds considerable management headaches, especially in terms of security.

When employees use their own personal devices to send and receive emails, IMs and text messages, the ability to enforce rights management, encryption or email usage policies can disappear entirely. You can ban these devices from your company, but chances are good that employees will use them anyway—which only increases the possibility of data leakage.

The other technology trend adding complexity to DLP is the increased use of cloud computing for vital company applications and data storage. When sensitive data isn't located inside the company network, the ability to control access to that data can be limited.

Cloud's software-as-a-service sibling can make stopping data breaches nearly impossible. After all, how do you protect customer data when it is accessible from Salesforce.com and protected only by a user name and password?

For any business worried about data leaks, it can be tempting to simply give up. If nearly every system has a weakness and can be circumvented by a dedicated disgruntled insider, what's the point of investing in any of these security systems? But these systems—from email encryption to rights management to email gateways to DLP—all provide some level of protection against data leakage, and that's better than none.

Also, businesses should make sure that their usage policies for the transmittal of company information over email are regularly updated and disclosed to employees. In a recent study on the cost of data breaches from the Ponemon Institute, there was a drop in negligent insider data breaches. This decrease was attributed to improved user awareness and training.

While none of the technologies described here is perfect, using any one of them in combination with ongoing user training will take companies a long way toward preventing accidental or intentional data loss through email and other communications systems.

Previous

Table of Contents

MORE LIKE THIS

Want More Like This?

InformationWeek creates more than 150 reports like this each year, and they're all free to registered users. We'll help you sort through vendor claims, justify IT projects and implement new systems by providing analysis and advice from IT professionals. Right now on our site you'll find:

Research: Identity Management: Just 27% of the 438 business tech pros responding to our 2011 identity management survey say their firms have comprehensive IdM deployments. Will the consumerization of IT and the adoption of SaaS-based applications spur an IdM renaissance? Download our research and analysis.

Strategy: In-House Malware Analysis: Vulnerability management identifies and closes exploitable holes in your enterprise network. But some systems remain vulnerable, and traditional antivirus and perimeter defenses are proving less effective against sophisticated malware, targeted attacks and zero-day exploits. We show you how malware analysis is an essential complement to enterprise vulnerability management programs.

Strategy: Malware War: It's a never-ending battle as security labs work 24/7 to analyze malicious code and the bad guys design ingenious ways to thwart their efforts and evade detection. Find out what goes on behind enemy lines.

PLUS: Find signature reports, such as the *InformationWeek* Salary Survey, *InformationWeek* 500 and the annual State of Security report; full issues; and much more.