

# Why Your Organization Needs to Focus on Outbound Content

An Osterman Research White Paper

*Published May 2007*

**SPONSORED BY**



## Why This White Paper Will Be Worth Your Time

---

Electronic communication tools can provide enormous productivity benefits for an organization's employees and can provide distinct competitive advantages for organizations of all sizes. These tools can speed decision-making; minimize the impact of distance between employees, business partners and customers; and can help an organization to generate new business.

However, electronic communication carries with it the substantial risk that employees might communicate in ways that violate corporate policies, various statutes or best practices. For example, the ease with which an email or instant message can be sent means that trade secrets or other sensitive information can inadvertently or intentionally be sent in ways that are contrary to the best interests of an organization.

**For the most part, organizations in North America have almost universally deployed systems that protect against inbound threats, such as viruses, worms and spam. Far fewer organizations have deployed systems that monitor outbound content.**

For the most part, organizations in North America have almost universally deployed systems that protect against *inbound* threats, such as viruses, worms and spam. Far fewer organizations have deployed systems that monitor *outbound* content. However, the growing use of email and instant messaging, coupled with the growing variety of other communication tools available to employees, makes the monitoring and management of outbound content increasingly important.

This white paper focuses on the need to monitor and manage outbound content, discusses the key drivers that are making it necessary and discusses the steps that an organization should take to mitigate the risks it faces from employee use of communication tools. Also included in this document are brief descriptions of the companies that have co-sponsored it.

## There is a Growing Need to Focus on Outbound Content Management

---

Organizations large and small are well aware of the critical need to monitor inbound communications. According to an Osterman Research survey of mid-sized and large organizations completed in March 2007, virtually 100% have deployed anti-virus systems, 94% have deployed anti-spam capabilities and 83% have deployed anti-spyware capabilities. Most organizations are on their second or later generation of both anti-virus and anti-spam systems.

However, far fewer organizations have deployed systems that will monitor outbound electronic communications, either for simple post-send review of outbound content or for more proactive, pre-send review. For example, in the survey noted above, we found that **47% of North American organizations have not yet deployed an outbound content compliance solution.**

#### **Many are Not Aware of the Problems**

One of the primary reasons that organizations have not yet deployed systems that can monitor or take specific actions on outbound content is simply that management and employees are not aware of the potential risks that some content can create, nor are they aware of the specific instances in which data breaches might occur. For example, employees will often mistakenly send confidential data in an email – such as Social Security Numbers or other sensitive information – without realizing that the data needs to be encrypted. There are many instances in which confidential data is buried in an email thread that is forwarded to others without being read thoroughly. A study by Pertemps found that two-thirds of email users had mistakenly sent email to the wrong person, often resulting in embarrassment or the leak of confidential information.

#### **Data Loss Prevention is Critical Serious**

Data breaches are becoming increasingly numerous and more serious. For example, the Privacy Rights Clearinghouse has tracked data breaches since early 2005 and has recorded numerous instances in which data breaches were caused by mistakenly sent emails; thefts of laptops and servers; loss of backup tapes, CD-ROMs and hard drives; the discarding of printed email content in dumpsters or at the curb for trash pickup and other instances in which sensitive data was compromised.

**An Osterman Research survey conducted in 2006 found that if a data breach were to occur in which disclosure of the breach would have to be made to customers and other external contacts, nearly two-thirds of organizations estimated that a single such breach would cost their organization at least \$100,000, not to mention other operational costs, damage to their brand and other problems.**

There are a variety of risks that organizations know about and often do not address, such as employees who use corporate email systems in violation of stated policies. There

**One of the leading reasons that organizations have not yet deployed systems that can monitor or take specific actions on outbound content is simply that management and employees are not aware of the potential problems that some content can create, nor are they aware of the specific instances in which data breaches might occur.**

are also a variety of unknown risks, such as spyware that can infect corporate computers and distribute confidential data to hackers and others.

A distinction also needs to be made between authorized and unauthorized data breaches. For example, an employee who is authorized to post information on a company Web site can inadvertently post confidential or sensitive information. By contrast, a terminated employee who is no longer authorized to send email can use the system to send trade secrets to competitors or others. Whether inadvertent or intentional, the damage caused by such breaches can be significant.

### **Some Organizations Have Tried Ineffective Techniques**

Many organizations have attempted to solve the problem of data breaches by locking down the network or restricting access to various data stores or particular services. While sometimes effective, doing so is often cumbersome, difficult to manage and often prevents employees from performing legitimate work functions, not to mention that many of these approaches are simply ineffective much of the time.

### **Failure to Manage Outbound Content Can Lead to Problems**

Organizations that fail to adequately protect themselves from the inadvertent or intentional distribution of confidential or sensitive information can suffer a variety of problems:

- **Loss of reputation**

If an electronic communication system is used in violation of corporate policy, an organization can suffer serious damage to its reputation. For example, Harry Stonecipher, the former CEO of Boeing, used the company's email system to send personal emails to women with whom he was having extramarital affairs. His firing which resulted from this activity was highly publicized and embarrassing to the company. Similarly, two employees of a North American bank sent an email via the corporate email system that depicted a photo of a US senator's face superimposed on a nude body. The two employees were fired for violating corporate policy and filed a wrongful termination suit in response.

- **Damaging legal judgments**

Unmonitored and unmanaged use of email by employees can lead to significant and adverse legal judgments. For example, employees of British insurance company Norwich Union sent rumors using Norwich's

**Organizations that fail to adequately protect themselves from the inadvertent or intentional distribution of confidential or sensitive information can suffer a variety of problems.**

email system falsely claiming that a competitor, Western Provident Association, was undergoing a government investigation and was experiencing financial problems. After Western Provident filed suit, Norwich Union publicly apologized for its employees' behavior and paid a judgment of £450,000 (~\$900,000) in court costs and damages.

- **Loss of intellectual property**

Email, instant messaging, blogs, wikis, file transfer systems and other tools can be used to send confidential information in violation of corporate policy or the law. This means that designs, trade secrets, proprietary processes and other knowledge assets can all be compromised if not managed properly. For example:

- In 2006, an employee of Duracell Corporation emailed confidential company information to a personal email account and then sent this information to two competing companies.
- In 2005, Oracle alleged that proprietary trade secrets had been posted by a former employee in a Google Groups posting.
- In 1998, an employee of IDEXX Laboratories repeatedly emailed a competing firm (with whom she was seeking employment) information about IDEXX's customers, confidential reports, manufacturing documents and information on negotiations that IDEXX was having with a firm the company sought to acquire.

- **Compromise of corporate security**

Failure to adequately monitor outbound communications can lead to a variety of security-related problems, including compromised PCs acting as zombies for sending spam and consumer instant messaging clients that can spread worms and malware. There are a variety of tools commonly used in the workplace that bypass conventional security defenses, including Skype, peer-to-peer file-sharing software and chat tools.

- **Violation of statutes and compliance requirements**

By not adequately monitoring and managing outbound content, organizations can run afoul of a wide variety of statutes that require data to be protected and retained.

*Email, instant messaging, blogs, wikis, file transfer systems and other tools can be used to send confidential information in violation of corporate policy or the law. This means that designs, trade secrets, proprietary processes and other knowledge assets can all be compromised if not managed properly.*

A small sampling of these statutes – but by no means an exhaustive list – include the following:

- The **Health Insurance Portability and Accountability Act (HIPAA)** requires that Protected Health Information (PHI), such as an employee's identity and his or her health condition or medications, remain confidential. For example, if an email that contains PHI is sent from a supervisor to an external benefits administrator, it must be encrypted. There are a variety of areas within HIPAA that must be addressed, including archiving of data, but protection of patient confidentiality is of paramount importance for all electronic communication.
- **National Association of Securities Dealers (NASD) Rule 3010** requires that relevant securities dealers' correspondence with the public must be supervised, reviewed and retained. The goal of NASD 3010 is to ensure that registered representatives are not making inappropriate claims to their customers, such as sending an email to a customer that guarantees that a stock will increase in value.
- The **Gramm-Leach-Bliley Act (GLBA)** requires financial institutions that hold personal information to transmit and store this information in such a way that its integrity is not compromised. GLBA requires financial institutions to comply with a variety of Securities and Exchange Commission and NASD rules.
- The **Payment Card Industry Data Security Standard (PCI DSS)** encompasses a set of requirements for protecting the security of consumers' and others' payment account information. It includes provisions for building and maintaining a secure network, encrypting cardholder data when it is sent over public networks and assigning unique IDs to each individual that has access to cardholder information.
- Section 215 of the **Patriot Act** allows a federal judge to issue an order permitting the FBI to obtain a business' records that are deemed relevant to a terrorist investigation. The net impact of the Patriot Act has been to limit the types and quantity of information that an organization will retain on its customers so as to minimize the quantity of information that might have to be turned over to the

*The Gramm-Leach-Bliley Act (GLBA) requires financial institutions that hold personal information to transmit and store this information in such a way that its integrity is not compromised.*

US government in the event such a demand for records is received.

- **Federal Information Processing Standard 140-2 (FIPS 140-2)** is a US government standard for IT products that are used to send sensitive information. While not a statute per se, FIPS 140-2 certification is critical for selling IT-related products to the US Federal government.
  - California's **SB1386** is a far reaching law that requires any holder of personal information about a California resident to notify each resident whose information may have been compromised in some way. This requirement makes it extremely important to retain and transmit records in an encrypted form, since doing so exempts an organization from the reporting requirement in the event of a breach.
  - The **Personal Information Protection and Electronic Documents Act (PIPEDA)** is a privacy law that applies to all Canadian companies. Like many other privacy laws, it requires that personal information be stored and transmitted securely.
  - The **UK Data Protection Act** imposes requirements on businesses operating in the United Kingdom to protect the security of personal information and to preserve information only as long as it necessary to do so. The Act requires, at least by implication, requirements for encrypted transmission of personal information and its secure retention.
  - The UK's Information Commissioner issued **The Employment Practices Data Protection Code** in June 2005 which includes, among other things, limits on the extent to which employee communication can be monitored.
  - Japan's **Personal Data Protection Law** is designed to protect consumers' and employees' personal information. It includes provisions for ensuring the security and disclosure of databases that contain this information, among other provisions.
- It is important to note that the list above represents only a limited set of regulations and that it is important to view regulations at a variety of levels: geographically

*The UK Data Protection Act imposes requirements on businesses operating in the United Kingdom to protect the security of personal information and to preserve information only as long as it necessary to do so. The Act requires, at least by implication, requirements for encrypted transmission of personal information and its secure retention.*

(state/provincial, Federal and global) and by industry sector. For example, some industries, such as certain sectors of the financial services industry, have specific requirements to which they must adhere. Some regulations, however, are cross industry and apply more generally.

### Other Problems

There are a variety of other problems and risks to which organizations are subject if they do not adequately monitor outbound communications from email and other systems. For example, employees who send sexually harassing, racist or other offensive content can put an organization at significant risk. Chevron Oil settled a sexual harassment lawsuit for \$2.2 million after four women received offensive email from a fellow employee. Morgan Stanley settled a \$60 million lawsuit filed by two employees after they received racist jokes sent through the company's email system.

**Chevron Oil settled a sexual harassment lawsuit for \$2.2 million after four women received offensive email from a fellow employee. Morgan Stanley settled a \$60 million lawsuit filed by two employees after they received racist jokes sent through the company's email system.**

Further complicating the issue is that laws, policies and best practices for monitoring various systems differ widely by geography. For example, laws in Germany and France make it more difficult to monitor employees' email use than in the United States. A 2003 report by Sweden's Data Protection Authority concluded that employers must obtain the voluntary consent of employees in order to monitor their communication. New Zealand's Privacy Act 1993, on the other hand, allows an employer to monitor its employees' communication if it has clearly informed them it will do so.

While some of the statutes noted above focus more on archiving, discovery or reporting requirements rather than monitoring, there is an implied need to monitor outbound communications for potential data breaches. For example, while SB1386 requires an organization only to *report* breaches of data for California residents, organizations that hold this data should *monitor* its outbound content to prevent these breaches.

**In short, data breaches and unmanaged use of electronic communication tools can be quite damaging to an organization and can lead to loss of reputation, the loss of customers and can create substantial regulatory and legal risk.**

### **There are Many Systems That Need to be Managed**

There are a variety of avenues through which confidential or sensitive information can be breached:

- Corporate email systems used on desktops, laptops, mobile devices and home computers
- Personal Webmail accounts used at work
- Consumer and enterprise instant messaging systems
- Skype and other consumer-oriented VoIP tools
- File transfer protocol (FTP) tools
- Chat tools
- Peer-to-peer file-sharing tools
- Message boards and forums
- Blogs
- Wikis

*There are a large number of data sources and communications tools that organizations must monitor and manage in order to protect corporate data from accidental or unauthorized distribution.*

**There are a large number of data sources and communications tools that organizations must monitor and manage in order to protect corporate data from accidental or unauthorized distribution, although email and IM are clearly the most important channels to monitor given their pervasive and much more frequent use by employees than other tools.**

### **What Should Organizations Do?**

---

There are three basic steps that any organization should undertake with regard to the risks it faces from unmanaged use of electronic communication tools:

- Understand the scope of the problem and its particular situation.
- Establish detailed and thorough corporate policies about use of electronic communication tools. Osterman Research has found that the vast majority of organizations have only a basic set of policies around the use of email, for example.

- Implement capabilities that will ensure compliance with these policies.

### **Understand the Scope of the Problem**

The first step that must be undertaken is to audit the current state of electronic communication in the organization. Doing so will reveal the risks that an organization faces and will help to qualify the problem to IT and senior business management. In most cases, **this will help an organization to realize that the risks and problems it faces are not merely a theoretical abstract, but are instead a real and present business problem that it must solve.**

Audits can be conducted in a variety of ways. For example, monitoring tools can be used to archive email communication, instant messages, blog posts and other employee communications. Searches can then be conducted on this content to look for credit card numbers, Social Security numbers, emails that are sent to competitors' domains, specific violations of statutes or corporate policies and other information. Another method is to draw a random sample of emails and then search the content for similar types of information.

The goal of any audit should be to identify and to quantify the problem of unmanaged communication so that senior management, legal counsel, HR and others can understand the extent of the risk the organization faces.

### **Establish Detailed and Thorough Corporate Policies**

After the audit, an organization should established very detailed and thorough corporate policies that focus on a variety of issues related to the use of electronic communication, including:

- Appropriate use of email by employees and what constitutes inappropriate use.
- Use of personal Webmail accounts over company-owned networks or on company time.
- The types of information that should be sent through various media. For example, a company may want to establish a policy that allows attachments to be sent only through email and not instant messaging systems.
- Limits on the type of tools that may be used. For example, a company may want to prevent the

**The goal of any audit should be to identify and to quantify the problem of unmanaged communication so that senior management, legal counsel, HR and others can understand the extent of the risk the organization faces.**

installation and use of consumer-oriented instant messaging clients, or it may want to limit use only to a particular client.

- The extent to which corporate systems may be employed for personal use.
- The types of information that should be sent via encrypted communication channels and which may be sent without encryption.
- What types of communications constitute business records and so must be preserved and for what lengths of time.
- Organizations must understand any regulations that govern monitoring policies, particularly in countries which place restrictions on how monitoring practices may be carried out.

**While policies are an important step in managing employee use of communications facilities, automated management systems are necessary to ensure complete and consistent adherence to these policies.**

In addition, corporate policies should include provisions that will set employee expectations about the use of electronic communication tools. For example, part of any corporate policy should include a statement that some types of electronic communication do not provide guaranteed delivery of content.

### **Implement the Appropriate Systems**

Perhaps the most critical step in managing the use of electronic communication is the deployment of systems that will enforce corporate policies. **While policies are an important step in managing employee use of communications facilities, automated management systems are necessary to ensure complete and consistent adherence to these policies.** These systems should:

- **Focus on the potential leak points that are important to your organization**  
As noted above, there are a variety of tools that put an organization at risk. As part of the evaluation process, you should determine which information channels (e.g., email, instant messaging, etc.) present a significant risk to your organization in order to guide your selection process.
- **Promote correct employee handling of data**  
For example, if an employee sends an inappropriate message to a co-worker or a confidential document to a

competitor's domain, a monitoring system should remind employees of corporate policies that may exist regarding the appropriateness of the communications vehicle they have chosen or other corporate policies.

- **Perform the appropriate level of inspection**

Based on corporate policies, the role of the employee in the organization and other factors, content should be inspected based on the appropriate policies. For example, certain employees may require different levels of outbound content inspection and data retention than others – a broker/dealer's email to a client may trigger a different set of policies compared to a clerical staff member's email to the same client. Certain recipients of an email may trigger different policies based on the company's history with those recipients. A CEO's email to an external auditor should trigger different inspection and retention requirements than those triggered by a marketing staff member's email.

It is important to expend the appropriate level of computing resources necessary to satisfy corporate and other policies in order to maximize the performance of electronic communication and management systems. For example, performing very deep content inspection on every message that flows through the corporate network is simply not necessary in many cases.

- **Deploy systems that will take appropriate action**

Based on the suspected level of data breach, the systems that monitor outbound communication should take the appropriate action. For example, an employees' instant message that contains what looks like a Social Security number may warrant nothing more than a popup window on the sender's display that reminds them of a corporate policy against sending this information through an instant messaging client. On the other hand, an email that contains an attachment with proprietary information sent through an employee's personal Webmail account may warrant immediate redirection of the message to a compliance officer or supervisor for further review before the message is sent. In short, suspected data breaches should trigger only the appropriate actions of discarding messages, quarantining them for further review, copying them to a supervisor, archiving them, etc.

Incident management is a key component of any

*It is important to have a consistent set of policies for all forms of outbound communication. For example, instant messaging should be treated no differently than email in the context of what types of communications are allowed or disallowed.*

system, since each suspected data breach should be handled with the right level of enforcement. For example, in a large organization it would be impractical to route every suspect email to a compliance officer or supervisor for review.

- **Train and make employees aware of corporate policies**  
Employees should receive regular training on corporate policies and good data management practices and should continually be made aware of appropriate ways to send information.
- **Implement forensics capabilities**  
Organizations may want to implement forensics capabilities in order to check on how data has been handled after it has been sent, either for legal purposes or simply to understand how its data is being managed. The ability to learn about how outbound content was sent and processed is just as important in many cases as monitoring this content prior to its being sent.
- **Implement a sender authentication scheme**  
While not an outbound content scanning mechanism, it is important for any organization to implement an authentication mechanism, such as SPF or DKIM, to ensure that recipients of its emails are given some level of assurance that the sending organization is valid.
- **Tight integration with existing infrastructure**  
In order to speed reduce costs, you should consider solutions that are well integrated with your IT infrastructure whenever possible. This approach will also speed implementation and lower on-going administration costs.

**Outbound electronic content in any organization must be monitored and managed in order to minimize risk and to ensure that electronic communication is appropriate and in compliance with an organization's policies, statutory obligations and industry best practices.**

### **Be Consistent**

It is important to have a consistent set of policies for all forms of outbound communication. For example, instant messaging should be treated no differently than email in the context of what types of communications are allowed or disallowed – i.e., an organization should not allow certain types of conversations to take place via instant messaging if they do not allow the same type of communication to be sent through email.

### **Maintain and Update Policies**

Even after organizations develop and implement a policy, there might be revisions or tweaks to the policies that need

to be made. How will a company implement the policies for new staff through acquisitions? What happens if new regulations are established? What trial and error might be necessary?

## Summary

---

Outbound electronic content in any organization must be monitored and managed in order to minimize risk and to ensure that electronic communication is appropriate and in compliance with an organization's policies, statutory obligations and industry best practices. Organizations should monitor all avenues through which employees may communicate, including email, instant messaging systems, blogs, wikis, personal Webmail accounts, message boards and other tools. The appropriate policies should be established and systems should be deployed so that an organization's risk from inappropriate use of electronic communication is reduced to the greatest extent possible.

## Sponsor of This White Paper

---

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at [www.symantec.com](http://www.symantec.com).



20330 Stevens Creek Blvd.  
Cupertino, CA 95014  
(408) 517-8000  
[www.symantec.com](http://www.symantec.com)

© 2007 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

THIS DOCUMENT IS PROVIDED "AS IS". ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.