The Case for Outbound Content Management

An Osterman Research White Paper

Published April 2010

SPONSORED BY

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

Executive Summary

NOTES FROM THE "I WISH I HADN'T DONE THAT" DEPARTMENT

- In January 2009, an employee of public relations firm Ketchum used Twitter to post some very unflattering comments about the city of Memphis shortly before presenting to the worldwide communications group at FedEx – Memphis' largest employer. An employee of FedEx discovered the tweet, responded to the tweeter, and then copied FedEx's senior managers, the management of FedEx's communication department and the powers that be at Ketchum[1].

- During April 2010, a Microsoft Excel worksheet that contained the names of 10,006 individuals, their occupations and other information was emailed to a journalist by someone in the Gwent (Wales) police department. Nearly 900 of the individuals identified in the worksheet had a criminal record[2].

- During March 2010, a gubernatorial candidate in Massachusetts sent a fundraising email to members of the state's Senate and House in violation of Massachusetts' campaign finance laws[3].

- In March 2010, about 100 police officers in the state of Victoria, Australia, were under investigation for their role in the internal distribution of an email that contained an offensive image and racist comments[4].

A soldier in the Israeli army used Facebook to post the details of an upcoming Israeli Defense Forces operation; the operation was cancelled as a result.

- Also in March 2010, a soldier in the Israeli army used Facebook to post the details of an upcoming Israeli Defense Forces operation; the operation was cancelled as a result, and the soldier was subsequently court-martialed and jailed for 10 days[5].

- In July 2009, an employee of LA Fitness sued the company after being propositioned by three of her supervisors via text message. She was fired after she complained to her supervisors' managers[6].

- Three employees of Highlands County, Florida were fired and 11 other employees were disciplined for sending highly inappropriate instant messages. The three terminated employees brought a wrongful termination lawsuit against the County, but the suit was dismissed in February 2010[7].

- In January 2009, an email sent from an office at Missouri State University inadvertently contained the names and Social Security numbers of 565 international students at the university[8].

- In July 2008, an employee with the California Department of Consumer Affairs emailed a file with the names and Social Security numbers of more than 5,000 staff members to her personal Yahoo! account – on her last day of employment[9].

- In 2005, a former employee of Kaiser Permanente, the largest HMO in the United States, posted confidential information about 140 patients on her blog[10].

MOST LEAKS ARE INADVERTENT

It is very important to note that the vast majority of data leaks are caused by inadvertent actions on the part of employees: an employee may mistakenly send the wrong attachment, accidentally include sensitive data in an email, forward an email that contains confidential information buried deep in the discussion thread, etc. While malicious users may be successful in thwarting even very sophisticated content filtering capabilities, good outbound content management will help organizations to stop the 98% of sensitive and confidential content breaches that are not intentional.

KEY TAKEAWAYS

Email, instant messaging, text messaging, social networking and other tools are a double-edged sword: they are extraordinarily valuable as a means of boosting employee productivity, generating revenue and creating brand awareness; but they also pose enormous risks if their use is not monitored and managed properly. Organizations that do not sufficiently monitor and manage communications face enormous problems, as the examples above – and this white paper – clearly demonstrate.

At its core, managing content is about managing risk – the risk that an organization could lose trade secrets, quash an acquisition, have its senior management embarrassed or face heavy fines – if it does not properly manage the content that leaves its organization. Managing outbound content, therefore, needs to be viewed as a primary capability in any organization's security arsenal.

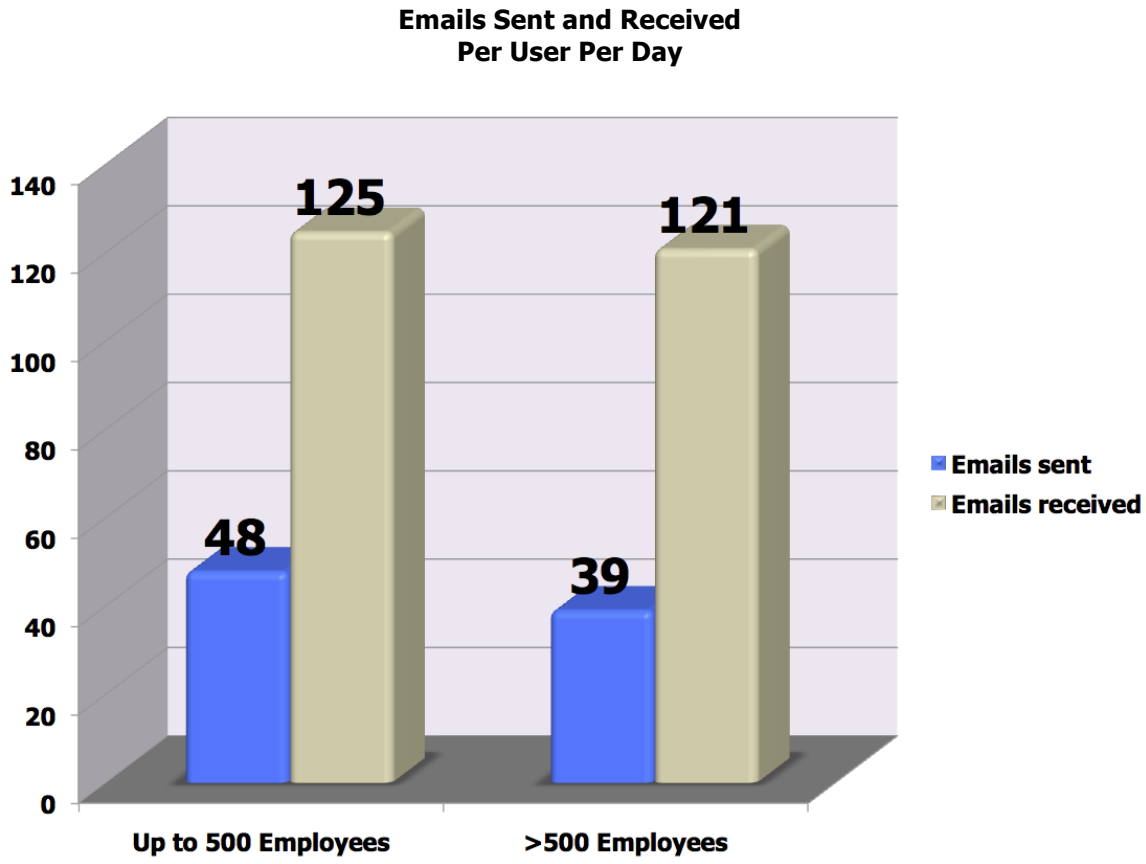
ABOUT THIS WHITE PAPER

This white paper focuses on the critical need to manage outbound content sent using email, instant messages, text messages, tweets, Facebook posts and the growing number of other venues from which damaging content might be sent. It also provides an overview of the relevant offerings from GWAVA, the sponsor of this white paper.

The State of Outbound Communications

EMAIL IS STILL THE PRIMARY MEANS OF COMMUNICATION…

Despite the growth of new communications and social networking tools, email still reigns as king. For example, in a March 2010 Osterman Research survey, we found that the average user sends 44 emails on a typical day and receives 123 emails, as shown in the following figure[11]. That means that during a normal workyear, the average user will send 11,360 emails and receive 31,940 emails. At this usage level, an organization of 1,500 users will generate traffic of 64.9 million emails in just one year.

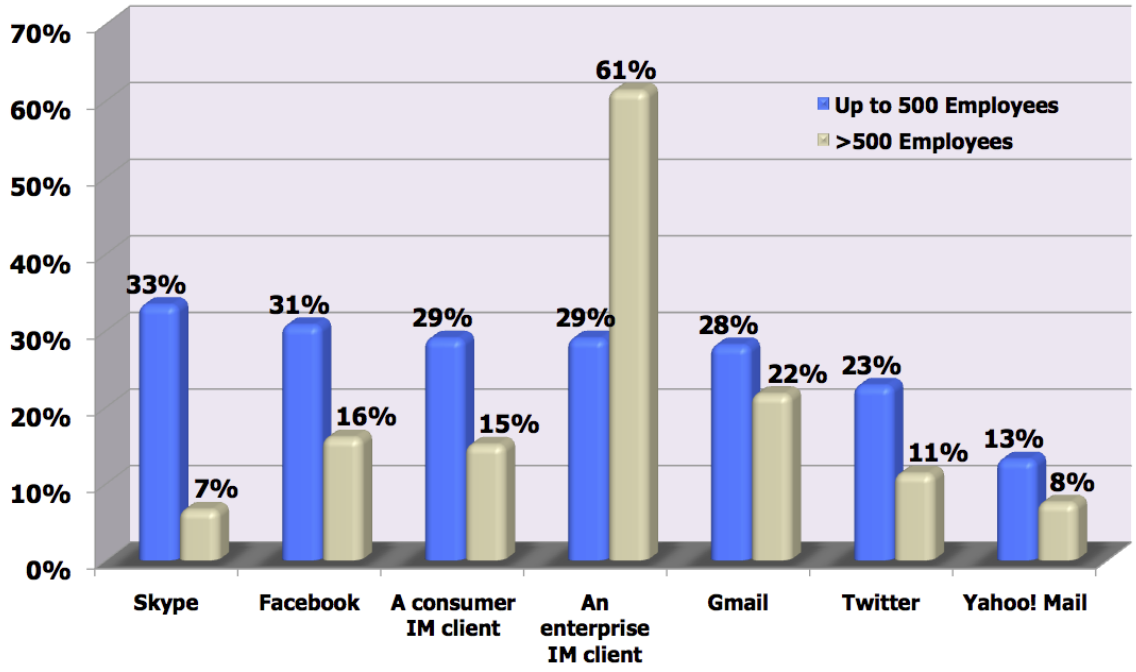


....BUT OTHER TOOLS ARE BEING ADDED TO THE MIX

That said – and despite Osterman Research's view that email will remain the dominant medium for sending and receiving business content for at least the next several years – there are a number of other tools that are becoming increasingly important in the context of collaboration, communications and information sharing. For example, the survey noted above found that Skype is used at work or for work-related purposes by 33% of users in smaller organizations (up to 500 employees) and by 7% of them in larger ones. Facebook is used by 31% of users in smaller organizations and by 16% in larger ones, while Twitter is used by 11% to 23% of users, as shown in the following figure.

Despite Osterman Research's view that email will remain the dominant medium for sending and receiving business content for at least the next several years – there are a number of other tools that are becoming more important in the context of collaboration, communications and information sharing.

Communications and Social Networking Tools in Use in the Workplace or for Work-Related Purposes
Proportion of Email Users Employing



In addition to the tools noted above, there are a variety of capabilities in use, including blogs, wikis and smartphones. For example, BlackBerry devices are in use by 58% of users in larger organizations and by 31% in smaller ones. The iPhone – use of which has grown rapidly in the workplace – is employed by 17% of users in larger organizations and by 27% of users in smaller organizations.

THE FUTURE OF INFORMATION FLOWS

The bottom line with regard to the future of communications, social networking, collaboration, information sharing and other tools boils down to four key points:

- **The Consumerization of IT**
  The workplace will increasingly be influenced by tools that may start in the consumer space but quickly migrate to the workplace. Initially, IT and senior business managers may resist their use, but the tools will be used anyway.

- **The Variety of Tools Will Grow**
  This will lead to a larger number of different tools used in the workplace, creating more egress points for content to leave the organization.

- **The Move to the Cloud**
  More organizations are moving key parts of their communication infrastructure to the cloud, meaning that their customers will be dependent on these providers to react appropriately to the problem of managing outbound communications.

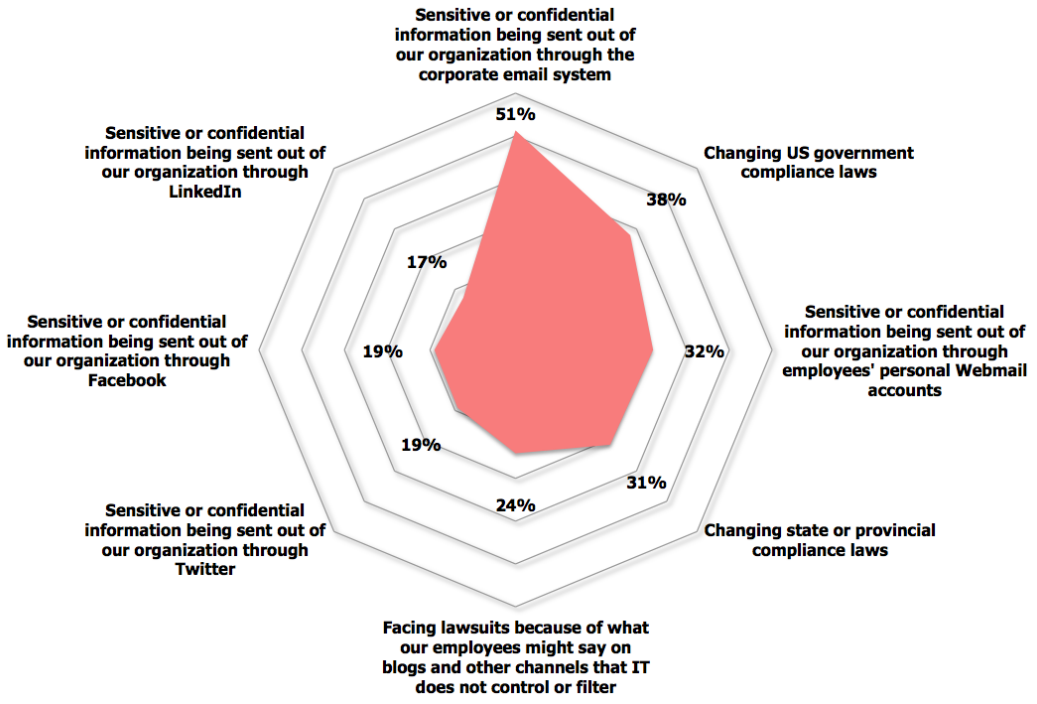
- **IT Will Have Less Direct Control**
  The growing number of employees who work from home/remotely, as well as the growing number of younger employees, will mean that IT will not be able to dictate the use of only "approved" tools – younger and more independent employees, aided by their lack of proximity to IT staff, will simply use what they want.

You Need to Focus on What Leaves Your Organization

DECISION MAKERS EXPRESS CONCERN ABOUT THE PROBLEMS

Many decision makers are at least intellectually aware of the problems associated with inadvertent and malicious data leaks, the use of consumer-oriented tools to send and receive corporate data, and related issues. For example, as shown in the following figure from an Osterman Research study conducted in February 2010[12], a large proportion of decision makers are concerned or extremely concerned about a variety of issues related to content that leaves their organizations.

Concern About Various Outbound Content Issues
% Responding Concerned or Extremely Concerned



In addition to the problems noted above, there are a number of other problems that organizations of all sizes experience:

- **Lack of encryption**
  A significant proportion of corporate data is sent outside the firewall in clear text

without encryption. Although decision makers and others understand that sensitive information should be encrypted before it is sent outside the firewall, most often it is not.

- **FTP and non-secure file transfer systems**
  Many organizations use FTP and other legacy file transfer capabilities that represent major security holes. Because users will often share FTP login credentials and/or leave sensitive content on FTP servers indefinitely, organizations leave themselves vulnerable to data breaches.

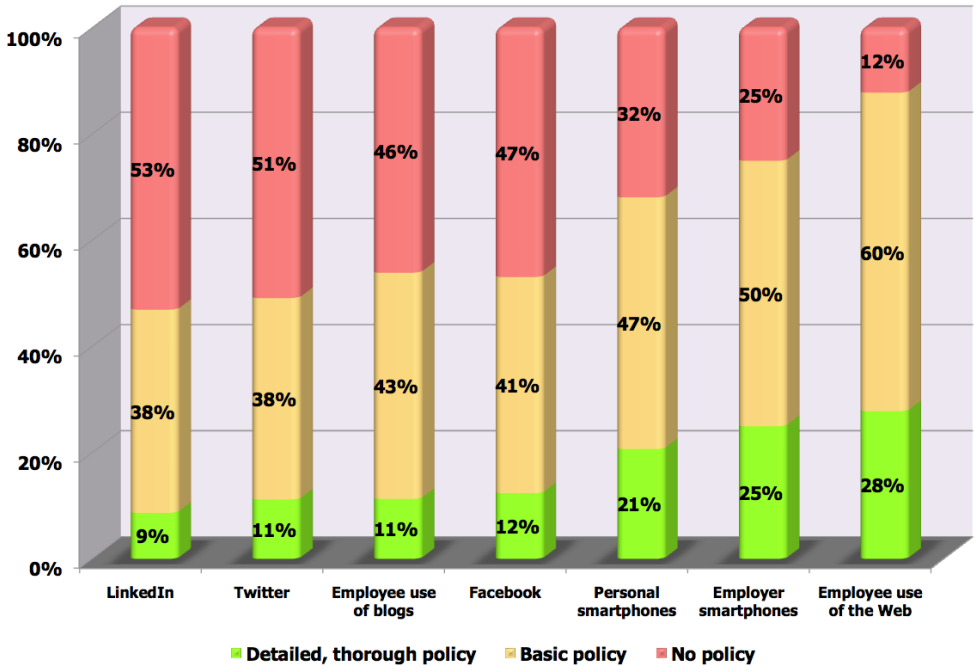
- **Attachments that contain sensitive information**
  Much of the sensitive content the leaves an organization does so in attachments – spreadsheets that contain sensitive financial information, word processing documents that contain Social Security numbers or health information and other content that users create as a normal part of their work. The key here is that many data leaks are not the result of users directly leaking this content, but instead sending sensitive content that others may have created.

- **Corporate data on home computers**
  A significant proportion of corporate data is stored on employees' home computers. In a study published by Osterman Research in September 2009[13], we found that 81-82% of users (depending on the size of the company) regularly check their work-related email from home on weekdays and 78% do so on weekends.

MOST ORGANIZATIONS' POLICIES ARE NOT KEEPING PACE

One of the fundamental problems in dealing with the issue of inadequate management of outbound content is that corporate policies are simply not keeping pace with the growing scope of the problem. For example, the February 2010 Osterman Research survey cited above found that although 98% of mid-sized and large organizations in North America have some sort of a policy focused on the use of email, only 31% have a *detailed and thorough* policy about appropriate use of email. Further, only a small proportion of organizations have a detailed and thorough policy about the use of other tools, as shown in the following figure.

Types of Policies in Place for Various Tools



Because detailed and thorough policies are really the first (but certainly not the last) line of defense in protecting against damaging content that is sent within or outside of an organization, most organizations are quite vulnerable to the potentially nasty consequences that could result from inappropriate, illegal or otherwise injurious content that is sent over their networks.

In addition to the embarrassment, damaged reputation and possibly lost revenue that could result from breaches of this type and sensitive or confidential information, there are many regulatory obligations that could also be violated.

WHAT COULD HAPPEN?

The consequences from inappropriate use of communications can be fairly significant. For example, in the example cited at the beginning of this white paper in which a Ketchum employee made inappropriate comments about Memphis just before presenting to senior management at FedEx, a senior manager at FedEx had this to say, in part:

> *"….everyone participating in today's event, including those in the auditorium with you this morning, just received their first paycheck of 2009 containing a 5% pay cut…*
>
> *….many of my peers and I question the expense of paying Ketchum to produce the video open for today's event; work that could have been achieved by internal, award-winning professionals with decades of experience in television production."*

Clearly, the implication is that the company may certainly be less likely to work with Ketchum in the future, potentially resulting in the loss of millions of dollars in future revenue.

WHAT ELSE COULD HAPPEN?

In addition to the embarrassment, damaged reputation and possibly lost revenue that could result from breaches of this type and sensitive or confidential information, there are many regulatory obligations that could also be violated. For example:

- **Payment Card Industry Data Security Standard (PCI DSS)**
  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.

- **Gramm-Leach-Bliley Act (GLBA)**
  GLBA requires that financial institutions protect information collected about individuals, including names, addresses and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers. The Act gives authority to eight federal agencies and the states to administer and enforce the Financial Privacy Rule (16 CFR Part 313) and the Safeguards Rule (16 C.F.R. Part 314). The wide-ranging Safeguards Rule mandates what companies should include in their written information security plan and how to secure this information, including using tough-to-crack passwords and encrypting sensitive customer information when it is transmitted electronically via public networks.
  GLBA also addresses steps that companies should take in the event of a security breach, such as notifying consumers, notifying law enforcement if the breach has resulted in identity theft or related harm, and notifying credit bureaus and other businesses that may be affected by the breach.

- **Health Insurance Portability and Accountability Act (HIPAA)**
  HIPAA addresses the use and disclosure of an individual's health information. It defines and limits the circumstances in which an individual's protected health information (PHI) may be used or disclosed by covered entities, and states that covered entities must establish and implement policies and procedures to protect PHI. Penalties for violations are up to $25,000 and $1.5 million, depending on when the violations occurred. Further, an individual who knowingly obtains or discloses individually identifiable health information may face a criminal penalty of up to $50,000 and up to one-year imprisonment. There is a specification for encryption of health information communicated over any network for which the transmitter cannot control access (45 CFR Part 142.308[d][1][ii].

  It is also important to note that if an unencrypted email that contains PHI is sent across the Internet, a violation of HIPAA may have occurred even if the email was not intercepted. The mere fact that this content is available for review by an Internet service provider or another third party can expose an organization to

penalties under HIPAA.

- **American Recovery and Reinvestment Act of 2009 (ARRA)**
  As part of ARRA, the provisions of HIPAA have been significantly expanded. A key component of ARRA is the Health Information Technology for Economic and Clinical Health Act (HITECH) that includes the following:

  - The reach of HIPAA has now been expanded to encompass business partners of entities already covered by HIPAA like pharmacies, healthcare providers and others. The new HIPAA will now include attorneys, accounting firms, external billing companies and others that do business with covered entities.

  - While these business associates were accountable to the covered entities with which they did business under the old HIPAA, these associates are now liable for governmental penalties under the new law.

  - Now for the really serious part: if you're subject to HIPAA requirements, one provision of HITECH is that the proceeds from HIPAA civil penalties will now be given directly to the Office of Civil Rights Enforcement (OCRE) within the US Department of Health and Human Services (HHS). What that means is that those who enforce HIPAA now have a direct financial incentive to levy fines and make them as large as possible, since these fines go directly into OCRE's budget. Further, individuals and lawyers can now collect fines for violations of the HIPAA Security Rule, dramatically increasing the incentive to sue privately when data is breached.

  - Related to the point above is that penalties for HIPAA violations have been expanded dramatically. For example, the US Department of Health and Human Services (HHS) issued *Breach Notification for Unsecured Protected Health Information* that became effective on September 23, 2009[14]. The HHS requires individuals to be notified of breaches of their PHI, logging of all such breaches with notification to HHS annually and notification of breaches of more than 500 individuals in one state to a prominent media outlet. Fines for violations can now reach as high as $1.5 million per calendar year.

The HHS requires individuals to be notified of breaches of their PHI, logging of all such breaches with notification to HHS annually and notification of breaches of more than 500 individuals in one state to a prominent media outlet. Fines for violations can now reach as high as $1.5 million per calendar year.

What this means for organizations that choose to remain in the healthcare industry or do business with them is that encryption and archiving become of paramount importance to a much larger group of companies. All of these organizations will need to appoint individuals to manage security policies. They will need to deploy appropriate technologies to protect data at rest and during transmission, and they

will need to dramatically beef up their security posture for messaging, managed file transfer, real-time communications, data preservation and other parts of their infrastructure.

- **State encryption requirements**
  California, with S.B. 1386, led the way for many states and some countries to pass data breach notification and disclosure acts. By the end of 2008, 44 U.S. states had enacted data breach notification laws and 25 countries, to varying degrees, have similar rules. A paper published in 2009 by the University of New South Wales ("Data Breach Notification Law Across the World from California to Australia"[15]) notes that the European Union and Australia have tabled data breach disclosure bills or passed acts. It also found that many of the laws and proposals from the 25 countries it examined are modeled on the California law.

  In Oct. 1, 2008, a Nevada law (Nev. Rev. Stat. § 597.970 [2005]) went into effect stating that: "A business in this State shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission." Such personal information includes an individual's first name or first initial and last name, along with details like a Social Security number, driver's license number or credit card number with security code. Law experts say that since the Nevada law doesn't define a "customer", the rules could be interpreted as applying to customers regardless of where they reside.

  A much broader law, Standards for the Protection of Personal Information of Residents of the Commonwealth (201 CMR 17.00), took effect in Massachusetts in early 2010. The law mandates that personal information – a combination of a name along with a Social Security number, bank account number or credit card number – be encrypted when stored on portable devices, when transmitted wirelessly or when transmitted on public networks. The law affects "persons who own, license, store or maintain personal information" about Massachusetts residents.

- **Personal Information Protection and Electronic Documents Act (PIPEDA)**
  PIPEDA is a Canadian privacy law that applies to all private companies operating in Canada. Like many other privacy laws, it requires that personal information be stored and transmitted securely. Canada's Privacy Act, in place since 1983, protects the personal information collected by government institutions.

- **UK Data Protection Act (DPA)**
  The DPA 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.

LOSS OF INTELLECTUAL PROPERTY

Although somewhat dated, a study by ASIS/PriceWaterhouseCoopers in 1999 found that about 70% of US firms' market value consists of their intellectual property and trade

secrets. An inability to protect outbound communications can lead to the loss of intellectual property, sometimes costing a company millions of dollars. For example:

- In 2007 a former employee of Duracell downloaded trade secrets about the company's AA batteries and then emailed that content to his home computer. Edward Grande, the former employee, pled guilty to theft of trade secrets in federal court[16].

- In the case of *Nilfis-Advance, Inc. v. Mitchell*, 2006 WL 827073 (W.D.Ark. Mar 28, 2006), the defendant was accused of sending emails containing trade secrets and other confidential information in zip files to his personal email account.

- In 2005, Oracle USA alleged that proprietary trade secrets had been posted by a former employee in a Google Groups posting[17].

- In *New South Communication Corp. v. Universal Telephone Co.*, 2002 WL 31246558 (E.D. La. Oct. 4, 2002), New South filed suit against an employee who had given notice he was leaving the company and then emailed confidential financial information about New South to his personal email account.

- In *United States v. Stephen R. Martin* 228 F.3d 1 (1st Cir. 2000), a researcher for IDEXX disclosed confidential information, files and other information about IDEXX trade secrets with the CEO of another firm[18].

The bottom line here is that any communication venue can represent an opportunity for an employee to inadvertently or maliciously leak trade secrets and that these leaks can cost an organization dearly.

EXPENSIVE REMEDIATION EFFORTS

There are a variety of very expensive remediation efforts that can ensue after confidential information has been disclosed. For example, the Ponemon Institute has calculated the cost of a data breach to be $204 per breached record (up from $138 in 2005), most of which ($144) is associated with indirect costs like lost revenues[19]. However, there are a variety of other costs associated with remediating data breaches:

- If an employee steals trade secrets or confidential information and the employer opts to sue that employee, the costs can be enormous. One source, for example, estimates the cost of litigating a trade secret case all the way through the completion of a trial to be in excess of $700,000[20]. For a small company, this cost can be prohibitive.

The first step that decision makers should take is to audit the current state of electronic communication, collaboration tools, social networking tools, etc.

- Notifying individuals whose data has been breached, as when an email that contains confidential information on individuals is sent unencrypted, can be relatively expensive. For example, if 100 individuals must be notified that their data was breached and a total of 16 hours of staff time is involved in creating the letter,

posting it, responding to inquiries, etc., a very conservative estimate of the cost of each letter sent will be nearly $7.00 per individual whose data was breached. The Ponemon Institute estimates the direct costs (detection and escalation, notification and ex-post response) to be much higher – $69 per record.

- Other costs associated with a data breach can vary depending on the extent of the breach, the industry in which an affected organization operates, the specific compliance obligations that have been violated and so forth. For example, a merchant whose data is suspected to have been breached in violation of PCI DSS compliance standards can expect to undergo a thorough policy review, manual computer inspection, wireless security testing and the like, resulting in thousands of dollars of staff time and potentially lost revenues. Discovery of an actual breach will result in costs that are substantially higher[21].

What Steps Should You Take?

STEP 1: UNDERSTAND THE PROBLEMS YOU FACE

The first step that decision makers should take is to audit the current state of electronic communication, collaboration tools, social networking tools, etc. Doing so will reveal the extent of the risks that an organization faces and will help to make real the problem to IT management, as well as senior line-of-business decision makers. In many cases, this will help an organization to realize that the risks and problems it faces are not merely a potential or theoretical problem but are instead a real and present business danger that the business must address. While this is not always a necessary step given the abundance of evidence that exists for the data breach problem, it may be required by some organizations in order to convince senior managers of the severity of their own problems.

Audits of communication and other tools can be conducted in a variety of ways. For example, monitoring tools can be used to archive email communication, instant messages, blog posts, tweets and other employee communication. Searches can then be performed 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, profanity, financial statements, racially or sexually inappropriate comments, and other information.

The purpose of such an audit is 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.

STEP 2: ESTABLISH DETAILED AND THOROUGH POLICIES

After the audit has been completed and digested by senior managers (and after they have been sufficiently scared by it), an organization should establish detailed and thorough corporate policies that focus on all of the issues related to the use of electronic communication, social networking and other tools. These policies should include:

- What constitutes appropriate and inappropriate employee use of email, Twitter, Facebook, instant messaging and other tools. This should include not only the content of emails and posts but also parties to whom email should not be sent, the types of content that should be encrypted, how email should be used on mobile devices, whether or not email should be checked from home and so forth.

- The extent to which corporate systems of any kind may be employed for personal use.

- Use of personal Webmail accounts over company-owned networks and/or use of these accounts during work hours.

- 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. Such a policy might also dictate the extent to which personal political, religious or other viewpoints can be expressed through tools like Twitter or Facebook.

- The types of communications that constitute business records, how long business records should be preserved, and when and how they should be deleted.

- Limits on the type of tools that may be used. For example, a company may want to prevent the installation and use of consumer-oriented instant messaging clients, or it may want to limit use only to a specific client.

- Organizations must understand any regulations that govern monitoring polices, particularly in countries that place restrictions on how monitoring practices may be carried out.

An Osterman Research survey found that only 29% consider their training programs to be effective or extremely effective in ensuring policy compliance. By contrast, 52% consider their automated policy compliance systems to be this effective.

Further, 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. This is important not only to protect organizations from the consequences of improper employee behavior but to also serve as a guide to delivery of time-sensitive communications.

STEP 3: TRAINING AND PROPER DATA MANAGEMENT

Before technology is deployed, employees need to be trained on the policies established in Step 2. Training is, in reality, the first line of defense in ensuring that data is not leaked in inappropriate ways. Part of the training process, however, focuses on technology solutions. 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 and/or other corporate policies. Further, 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.

That said, employee training can go only so far in ensuring that outbound communications are managed properly. For example, in a policy management study that Osterman Research conducted in February 2010, we found that organizations are slightly more dependent on training than on automated technologies to ensure messaging policy compliance[22]. However, the same survey found that only 29% consider their training programs to be effective or extremely effective in ensuring policy compliance. By contrast, 52% consider their automated policy compliance systems to be this effective.

STEP 4: DEPLOY THE RIGHT TECHNOLOGIES

The critical next step is to deploy the technologies that will enforce the corporate policies that have been established. While policies are necessary to establish what an organization needs to protect, they will be ineffective at solving all of the data breach problems an organization might experience.

Any system that an organization deploys should:

- **Identify the leak points**
  Focus on the leak points that are important to the organization, including email, instant messaging systems, Twitter, Facebook, other Web 2.0 applications, removable storage, laptops, FTP systems and other potential sources of data leaks. This does not necessarily have to be an exhaustive list of everything that could happen, but should focus on at least the most important communication tools that your organization uses. For example, if email is the primary method for sending data – which is the case for most companies – focus on email first. If instant messaging is used to share information with members of the supply chain, focus on that, as well. It's very acceptable to start small with only the most important communication tool, like email, and then build from there, or even end there if that solves the data leak problem.

- **Include capabilities to meet current and future requirements**
  It is important to deploy a technology that will meet the large and growing number of potential data leaks an organization might encounter. This includes inspecting for file metadata, industry-specific keywords and phrases, regular expressions (e.g., email addresses), exact file matches and performing statistical analysis to detect specific types of content, such as employee resumes sent out through email.

- **Deploy systems that will manage data properly**
  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 employeee'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, requiring encryption, archiving them, etc.

Not every content management system needs to rely on automated technologies that will inspect content at the gateway level. Some companies may wish to rely on individual users to classify content based on its sensitivity and mark this content appropriately. For example, some data leak prevention systems will classify emails by their sensitivity, the department that should manage it or some other parameter. Such a scheme may opt to classify every email or just those that contain sensitive content. Further, some systems will mark email visually so that senders and recipients can be made aware of the sensitivity of the content or how it should be classified. These systems help users to identify the sensitivity of particular emails and also help them to organize their content.

- **Perform the appropriate level of inspection**
  Incident management is a key component of any 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. Further, the real time nature of some tools, such as Twitter, make real-time inspection of outbound content almost impossible to accomplish without undermining the value of those tools.

- **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.

  Because most data breaches will occur through established messaging channels, such as email, outbound content inspection should be integrated with email and other IT-established communication channels.

  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. However, inspecting content flowing through

key threat vectors, such as Facebook or encrypted Webmail channels, might be critical.

It is also important to note that content inspection can occur at many places in the network. Some organizations may opt for a gateway-based tool or one in the cloud, while others will opt for client-side tools that will help individual users to remediate any problems before the offending content is sent.

- **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. It is also useful to retain copies or actual email, attachments, tweets or files being copied to USB devices.

STEP 5: INTEGRATE MESSAGING AND SECURITY

Because most data breaches will occur through established messaging channels, such as email, outbound content inspection should be integrated with email and other IT-established communication channels. Organizations might want to consider adding intelligence to the MTA and other points in the system to ensure that reliable content inspection takes place without imposing an undue burden on message delivery performance.

STEP 6: OTHER ISSUES ON WHICH YOU SHOULD FOCUS

It is important to conduct regular audits of, and perform regular reporting for, outbound content. For example, a weekly or monthly report showing attempted or inadvertent data breaches can help decision makers to refine policies to include additional elements or to keep up with new laws and regulations. These audits and reports can also help senior management to identify the weak points in employee training. They can also help to identify employees that might need additional counseling about appropriate use of communication, social networking and other tools.

Summary

Email, instant messaging, Twitter, Facebook, collaboration tools, wikis, blogs, smartphones and other systems used in organizations of all sizes are incredibly useful as a means of boosting employee productivity, increasing corporate revenue, speeding the decision-making process and improving the operation of business in a number of other ways. However, these tools and systems also represent an enormous risk to an organization because they allow employees to send sensitive, confidential or inappropriate content out of an organization, sometimes with damaging consequences.

As a result, every organization – regardless of its size or the industry in which it operates – must not allow communication and other tools to be employed without appropriate oversight. Corporate policies should be established to help employees

understand how and when these tools should be used, but training and automated systems are necessary to ensure compliance with these policies.

Sponsor of This White Paper

GWAVA, Inc.
100 Alexis Nihon Road
Suite 500
Montreal, QC
H4M 2P1
Canada
+1 514 639 4850
www.gwava.com

Since its beginning in September of 2001, weeks after 9/11, GWAVA has had a single focus; to meet the challenging needs that are forced upon our customers.

Why the Bug? Our logo is a bug for a reason. This image represents an ever present promise to those who trust us with their collaboration needs. The bug represents our understanding of the unpleasant tasks that IT departments are faced with. These include government compliance and regulation for archiving email, text, and instant messaging. It includes the catastrophic disasters that can literally destroy a company when email can't be accessed. It represents the constant threat of spam and viruses that are continually increasing in sophistication and complexity.

The solutions developed include Retain for Email, Retain for BlackBerry Enterprise Server, and Retain for Instant Messaging with Office Communicator. Other solutions are Reload for Disaster Recovery and GWAVA SMTP for anti-spam and anti-virus.

The bug is our promise to you that we understand your challenges and we are there with you to protect your organization, company, customers and employees.

GWAVA knows messaging.

---

[1] http://shankman.com/be-careful-what-you-post/
[2] http://www.policeprofessional.com/news.aspx?id=10245
[3] http://www.dailynewstranscript.com/news/x38423667/Cahill-camp-calls-capitol-campaign-solicitations-a-mistake
[4] http://www.independent.co.uk/news/world/australasia/racist-email-scandal-engulfs-australian-police-1928039.html
[5] http://www.allheadlinenews.com/articles/7018132756
[6] http://www.examiner.com/x-22217-Raleigh-Workplace-Issues-Examiner~y2009m9d18-Virtual-sexual-harassment-is-now-a-workplace-reality
[7] http://www2.highlandstoday.com/content/2010/feb/17/la-county-wins-e-mail-lawsuit-with-3-ex-workers/
[8] http://www.privacyrights.org/ar/ChronDataBreaches.htm
[9] http://www.privacyrights.org/ar/ChronDataBreaches.htm
[10] http://www.privacylawyer.ca/blog/2005/03/incident-disgruntled-employee-said-to.html
[11] Results of an End User on Email and Other Tools, published by Osterman Research, April 2010
[12] *Policy Management Trends, 2009-2012*, Osterman Research, Inc.
[13] *Results of an End User Survey on the Use of Communications Tools*, Osterman Research, Inc.
[14] http://www.aad.org/pm/compliance/hipaa/documents/BreachNotificationFactSheet.pdf
[15] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1412063
[16] http://wombletradesecrets.blogspot.com/2007_02_01_archive.html
[17] http://www.chillingeffects.org/tradesecret/notice.cgi?NoticeID=2096
[18] http://openjurist.org/228/f3d/1
[19] 2009 Annual Study: Cost of a Data Breach, Ponemon Institute, LLC
[20] https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&doctype=cite&docid=50+B.C.+L.+Rev+1425&srctype=smi&srcid=3B15&key=ac677f1ecd5269b45bc4efb326aed015
[21] http://www.pcicomplianceguide.org/merchants-20090416-cost-data-breach.php
[22] *Policy Management Trends, 2009-2012*, Osterman Research, Inc.