Why Your Organization Needs to Implement DLP

An Osterman Research White Paper

Published February 2011

SPONSORED BY

Why This Document Will Be Worth Your Time

The typical email user sends 41 emails during a normal workday, or roughly 10,250 emails each year. That means than in an organization of 2,000 users, 20.5 million emails will be sent. Add to this the large and growing proportion of email users who also use instant messaging clients, wikis, post content to blogs, use personal Webmail accounts for business purposes, check email from home, send files through FTP systems, take work home on USB thumbdrives, work from coffee shops and hotels, transport corporate data on mobile devices, and use collaboration tools of various types. Plus, add in the growing number of iPads, iPhones, Smartphones and other corporate and personal devices that are used in the workplace and to access corporate data resources.

Now, consider that most of these communications and fileshares sent and transported without any sort of monitoring, encryption or oversight, and that many of the devices used are not secured by IT. The result is that

> *Organizations must implement DLP systems to protect themselves against the growing array of threats they face from inadvertent and malicious data leaks.*

organizations are deploying a growing array of tools and endpoints for employees to become more efficient. And, at the same time, they are creating a growing number of opportunities for information to leak out of an enterprise in unauthorized and potentially damaging ways.

There are many well-publicized (and some not-so-well publicized) examples of sensitive data that has been sent through email and other tools in an authorized or mistaken manner. The vast majority of these data breaches are inadvertent, but the opportunity exists for malicious users to send confidential and sensitive data, as well.

THE CONSEQUENCES OF DATA LEAKS CAN BE SERIOUS

The consequences of a data breach can vary widely: a confidential memo sent by a senior manager to the wrong client may carry with it no negative ramifications; the client may simply delete the email and the breach will simply be forgotten. However, data breaches can carry with them very serious consequences, such as the revelation in February 2008 that that the Hannaford Brothers chain of supermarkets lost more than four million debit and credit card numbers to hackers. The most recent study on data breaches by the Ponemon Institute found that the loss of customer records costs $204 per record, and that the average business loss for a large organization that suffers a data breach is $6.65 million[1].

The bottom line is that organizations must implement Data Loss Prevention (DLP) systems to protect themselves against the growing array of threats they face from inadvertent and malicious data leaks from email, instant messaging and other systems.

---

[1] *2009 Annual Study: Cost of a Data Breach*, Ponemon Institute

This white paper is an update to a white paper we published on DLP issues in 2008 and is sponsored by Safend. Information on the company is included later in this white paper.

DLP is Becoming Much More Important

MANY ARE UNAWARE OF THE PROBLEMS WITH DATA LOSS

According to a 2010 study by Osterman Research, the vast majority of organizations have implemented robust inbound security capabilities focused on preventing infiltration by spam, viruses, malware and other threats. However, even using a fairly broad interpretation of data loss prevention (DLP) capabilities, which would include products that don't provide *true* DLP functionality, fewer than one-half of organizations have deployed systems that will protect against outbound threats.

Clearly, the data above suggests that organizations of all sizes are well aware of the need to monitor their inbound communications for spam and malware. However, they are not nearly as aware of the need to monitor outbound communications, or they are not taking the threat as seriously as they should. This, despite the fact that 27% of organizations in the same survey reported that during the previous 12 months data or information was accidentally or malicously leaked from their organization.

One of the key reasons that organizations have not yet deployed DLP systems can be explained by the fact that many decision makers are not aware of the potential risks they face, nor might they be aware of the data breach examples in their own industries. For example:

- Employees will often accidentally send confidential data in an email – such as credit card numbers, Social Security numbers or other confidential information – without realizing that the data needs to be encrypted during transmission.

- There are many cases in which confidential data, unbeknownst to the sender, is buried in an email thread that is forwarded to others.

- Email is sometimes sent to the wrong person, often resulting in the leak of confidential information.

- Some employees will send confidential data via personal Webmail accounts to others or to themselves to avoid file size limitations on attachments or so that they can work on documents at home.

- Web 2.0 applications represent a significant potential for data loss. For example, MySpace, Facebook and other social networking sites have been on the receiving end of healthcare-related data. Hidden malware installed on endpoints has harvested personal information like credit card numbers and quietly uploaded this content via HTTP/HTTPS.

- Memory sticks are ubiquitous and newer devices are entering the network at a rapid pace, including iPads, iPhones and a variety of other tools that are popular among consumers as well as among business customers. For example, a 2010 survey by ITIC[2] found that more than 80% of respondents use iPhones, iPads and Macs for both personal and work-related use.

BREACHES ARE BECOMING MORE NUMEROUS AND SERIOUS

Data breaches are becoming more numerous and more serious. For example, the Privacy Rights Clearinghouse has tracked data breaches since early 2005 and has recorded many examples in which data breaches were caused by emails sent mistakenly; cases in which laptops, CD-ROMs and backup tapes with confidential data were lost or stolen; employees discarding printed content in dumpsters or at the curb for trash pickup; and many other instances in which sensitive data was compromised.

There are many risks that organizations know about and often do not address, such as employees who use corporate email systems in violation of stated policies or who use personal Webmail accounts to send company data home – a 2007 Osterman Research survey found that 47% of organization allow employees to use personal Webmail for business purposes. There are also a variety of unknown risks, such as keystroke loggers that can infect corporate computers and distribute confidential data to hackers and others.

It is also important to distinguish between authorized and unauthorized data breaches. For example, an employee who is authorized to place information on a company Web site or a corporate wiki can mistakenly post confidential information. By contrast, a terminated employee who is no longer authorized to send email can still use the system to send trade secrets to competitors or others until their access credentials are removed. Whether inadvertent or intentional, the damage caused by such breaches can be enormous.

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

MULTIPLE VENUES THROUGH WHICH DATA LOSS OCCURS

There are many tools and systems from which confidential or sensitive information can be sent in violation of corporate policy:

- Corporate email systems used on desktops, laptops, mobile devices and home computers. Regarding the last venue, an Osterman Research survey found that the vast majority of employees check their work-related email from home on weekends, and slightly more check their work email from home after-hours.

- Consumer and enterprise instant messaging systems

- Personal Webmail accounts used at work

---

[2] http://goo.gl/yZIgS

- Thumbdrives and other portable storage devices

- Smartphones and tablets

- Social networking tools like Facebook and LinkedIn

- Other Web 2.0 applications, including wikis and blogs

- File transfer protocol (FTP) tools

- Chat tools

- Skype and other consumer-oriented VoIP tools

- Consumer-focused devices like the iPad and iPhone

- Peer-to-peer file-sharing tools

- Message boards and forums

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

PROBLEMS CAUSED BY NOT ADDRESSING THE DLP ISSUE

Data breaches can be *very* expensive: for example, an Osterman Research survey 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.

Organizations that do not properly address DLP can suffer a variety of problems, including:

- **Loss of intellectual property**
  Email systems, file transfer systems, instant messaging systems, blogs, wikis, Web tools, thumbdrives and other tools can be used to send confidential information in violation of corporate policy, common sense and the law. The result is that trade secrets, designs, proprietary processes and other knowledge assets can all be compromised if not adequately protected. For example:

  o In 2009, 76 million records on US veterans were breached by the National Archives and Records Administration because of an improperly discarded hard drive.

- o In 2008, an employee of Ivy Tech Community College (Bloomington, IN) intended to send student information to a single employee, but inadvertently sent an invitation to view the file to a much larger list.

- o In 2007, an employee of Pfizer installed file-sharing software for personal use on her company laptop. The result was that personal data for 17,000 Pfizer employees, including Social Security numbers, was exposed.

- o The leakage of a large number of US State Department documents, through multiple DVDs burned by a trusted analyst stationed in Iraq has been in the headlines in 2010 and will continue to be so in 2011.

- o In 2009, a laptop stolen from AvMed Health Plans resulted in the breach of 1.2 million records.

> *A failure to properly monitor outbound communications can lead to a variety of security-related 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, the former CEO of Boeing, Harry Stonecipher, used the corporate 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 embarrasing to the company.

  In another well-publicized case, two employees of a North American bank sent a message via the corporate email system that depicted a photo of Senator Hillary Clinton's face superimposed on a nude body. The two employees were fired for violating corporate policy and filed a wrongful termination suit in response.

- **Harmful legal judgments**
  Unfettered use of email by employees can lead to significant and adverse legal judgments. For example, several years ago employees of British insurance company Norwich Union sent rumors using the corporate email system that falsely claimed 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 (~US$780,000) in court costs and damages.

- **Compromise of corporate security**
  A failure to properly 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. A small sampling of these statutes – but by no means an exhaustive list – include the following:

  o California's SB1386 (the Database Security Breach Notification Act) 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 very 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.

  Since California passed its groundbreaking data breach notification law, most other US states have passed similar laws, as shown in the following figure. For example, Nevada put into effect a law (NRS 597.970) on October 1, 2008 that states, "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." Massachusetts has passed a similar, but more restrictive law that will go into effect on January 1, 2009. While the Nevada law focuses on electronic transmission of information, the Massachusetts law focuses on the portability of data. That means that any personally identifiable information data an entity has on a Massachusetts resident that is stored on a laptop, mobile device, thumbdrive, etc. must be encrypted. California's legislature sent Bill 1166, which would have tightened the state's existing data breach notification law, to the governor for signature, but the bill was returned to the legislature without being signed into law.

Status of Adopting Data BreachNotification Laws in the United States
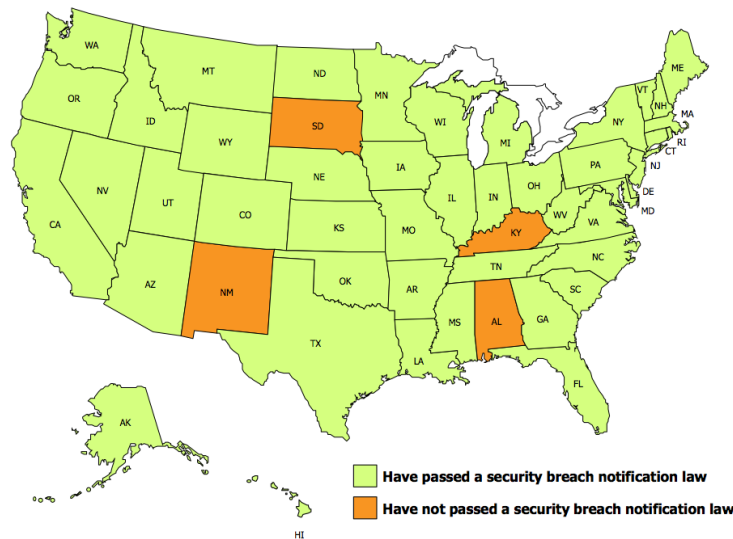
Data Source: National Conference of State Legislatures

o 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.

As part of the American Recovery and Reinvestment Act of 2009 (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). Now, business partners of entities already covered by HIPAA, such as pharmacies, healthcare providers and others, are required to comply with HIPAA provisions. This includes 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. Further, HIPAA violations have been expanded dramatically. For example, if a covered entity or one of their business associates loses 500 or more patient records, it must notify HHS and a "prominent media outlet" to let them know what has occurred. Section 13402 of HITECH requires that if a "covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected individuals likely reside."Fines for HIPAA violations can now reach as high as $1.5 million per calendar year.

o 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.

o 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.

o 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.

o Sensitive Data Discovery (SDD) – the practice of protecting sensitive information that may be stored or transmitted through corporate systems – is becoming

more important. For example, PCI DSS v2.0 highly recommends this practice for any PCI DSS compliance process. However, SDD is also necessary for a wide variety of other requirements, as well, including HIPAA and Sarbanes-Oxley.

o The Personal Information Protection and Electronic Documents Act (PIPEDA) is a Canadian privacy law that applies to all companies operating in Canada. Like many other privacy laws, it requires that personal information be stored and transmitted securely.

o 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.

o 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.

o 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 regulations identified above represent only a limited set of regulations and that it is important to view regulations at a variety of levels: geographically (state/provincial, Federal and global) and by industry sector. For example, some industries, such as some sectors of the financial services industry like broker-dealers, hedge fund managers and investment advisors, have specific requirements to which they must adhere. Some regulations, however, are cross industry and apply more generally, such as California's SB1386.

OTHER PROBLEMS ABOUND

There are a variety of additional risks and problems that organizations face if they do not properly monitor outbound communications from email, removable storage and other systems. For example:

- Employees who send sexually harassing, racist or other offensive content can put an organization at significant risk: in a well-publicized case, 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.

- Citing Title VII of the Civil Rights Act of 1964 and the New Jersey Law Against Discrimination, the New Jersey Supreme Court ruled that an employer can be liable for materials posted by its employees on electronic bulletin boards.

Making the issue more difficult 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.

- 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.

> *Employees who send sexually harassing, racist or other offensive content can put an organization at significant risk.*

- 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.

While some of the statutes noted above focus largely on archiving, e-discovery or reporting requirements and not monitoring per se, 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* their outbound content to prevent these breaches.

In short, data breaches and the unmonitored use of electronic communication tools can be very damaging to an organization of any size and can lead to loss of reputation, revenue, and customers; and can create substantial regulatory and legal risk.

What Should You Do?

STEP 1: UNDERSTAND JUST HOW SERIOUS THE PROBLEM IS

The first step that decision makers may want to take to solve the data breach problem is to audit the current state of electronic communication and file management in the organization. This may include the use of an auditing tool to learn how many external devices are used in the organization, as well as a discovery tool that can help identify the location of sensitive intellectual property, regulated data and other sensitive content.

Going through such a review 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, theoretical problem, but are instead a real and present business danger that it 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 extent of their own organization's problems.

Audits of communication and file management tools 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 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 POLICIES FOCUSED ON STOPPING BREACHES

After the audit has been completed and digested by senior managers, an organization should establish very detailed and thorough corporate policies that focus on all of the issues related to the use of electronic communication and file management capabilities, including:

- Appropriate and inappropriate use of email by employees and what constitutes inappropriate use. This should include not only the content of emails, 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.

> *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.*

- The extent to which corporate systems 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.

- 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 particular client.

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

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 can also serve as a guide to delivery of time-sensitive communications.

STEP 3: DEPLOY THE RIGHT TOOLS

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 potential leak points that are important to the organization, including email, instant messaging systems, Web-based systems, removable storage, laptops, FTP systems and other potential sources of data leaks.

- **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 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 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.

  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.

- **Promote appropriate 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. Copying of sensitive documents to removable storage devices should be monitored because of the high risk of data loss from these devices. Osterman Research surveys have found overwhelmingly that decision makers want to provide reminders and other "soft" types of enforcement rather than routinely sending potentially offending messages to compliance officers, supervisors or HR.

- **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. However, inspecting content flowing through key threat vectors, such as removable storage or encrypted Webmail channels, is critical.

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

- **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, organizations should consider solutions that are well integrated with their IT infrastructure whenever possible. This approach will also speed implementation and lower on-going administration costs.

WHAT WILL ORGANIZATIONS DO?

Osterman Research believes that most organizations are waking up to the fact that they need to implement DLP capabilities. For example, an Osterman Resesarch study published in August 2010 found that:

- 41% of organizations will likely or definitely deploy DLP systems in the 2010-2011 time frame

- 43% will likely or definitely deploy system to protect against consumer-oriented instant messaging threats

- 56% will likely or definitely deploy systems to manage and/or control Web access

Summary

Outbound content sent from any communications tools or stored on laptops and removable storage devices must be monitored and managed in order to minimize risk and to ensure that the content 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, wikis, blogs, personal Webmail accounts, USB devices, message boards and other tools. The appropriate policies should be established and systems should be deployed so that an organization's risk can be mitigated to the extent possible.

Sponsor of This White Paper

Safend, Inc.
2 Penn Center, Suite 301
Philadelphia, PA 19102
Tel: +1 215 496 9646
Fax: +1 215 496 0251

Safend Ltd.
32 Habarzel Street
Tel Aviv 69710
Israel
Tel: +972 3 644 2662
Fax: +972 3 648 6146
www.safend.com

Safend a leading provider of endpoint data protection, guards against corporate data loss and theft through its content discovery and inspection, encryption and comprehensive device and port control. Safend encrypts internal hard drives, removable storage and CD/DVDs and provides granular port and device control over all physical and wireless ports. Safend maps sensitive information and controls data flow through email, Web, external devices and additional channels. Safend ensures compliance with HIPAA, PCI, SOX, BASEL II and other regulatory data security and privacy standards. Safend solutions are deployed by multinational enterprises, government agencies and small to mid-size companies across the globe. For more information, visit www.safend.com.