

## EXCERPT

---

### **Worldwide Outbound Content Compliance 2005–2009 Forecast and Analysis: IT Security Turns Inside Out**

---

Brian E. Burke

#### **IN THIS EXCERPT**

This excerpt is taken from *Worldwide Outbound Content Compliance 2005–2009 Forecast and Analysis: IT Security Turns Inside Out*, by Brian E. Burke (IDC #34260, November 2005). It includes the sections IDC Opinion, Situation Overview, Market Drivers, a profile of Mirapoint, and Essential Guidance, as well as four figures.

#### **IDC OPINION**

Historically, information security solutions have focused on addressing external threats to corporate networks and endpoints. Viruses, hackers, worms, trojans, spam, blended threats and, most recently, spyware have wreaked havoc on corporate networks and users alike. In turn, enterprises have deployed an expanding array of perimeter security solutions, such as firewall, antivirus, antispam, intrusion detection/prevention, antispymware, and others, to protect against external threats. Today, there is an emerging threat to corporate security that comes from inside the organization. This concern has created a new market that IDC has defined as outbound content compliance (OCC). Outbound content compliance includes solutions that monitor, secure/encrypt, filter, and block outbound content contained in email, instant messaging (IM), peer-to-peer, file transfers, Web postings, and other types of messaging traffic. OCC solutions play a key role in enforcing corporate governance, which is defined by IDC as a combination of complying with both external regulatory requirements and internal corporate policies and best practices. These solutions help organization protect against:

- Violations of government and industry regulations (Health Insurance Portability and Accountability Act [HIPAA], Gramm-Leach-Bliley [GLB], Sarbanes-Oxley [SOX], etc.)
- Violations of corporate email policy and best practices
- Loss/leakage of intellectual property
- Loss/leakage of confidential or customer information
- Legal liability associated with inappropriate and offensive content

## SITUATION OVERVIEW

---

### **The Emergence of Outbound Content Compliance**

For years, organizations have focused security efforts on external threats posed by the explosive growth of viruses, spam, blended threats, and spyware. The situation is now beginning to change, especially in light of new information-intensive government and industry regulations that require organizations to protect the integrity of customer and employee personal information and corporate digital assets. As noncompliance may result in substantial fines and executive liability, organizations are realizing that information leakage by insiders is a threat that can no longer be underestimated.

Addressing the insider threat, however, is turning out to be a complex challenge. The increasing use of corporate email, Web email, instant messaging, peer-to-peer, and other channels for distributing data and the proliferation of mobile devices that allow employees to carry sensitive information outside the organization's boundaries make the control of outbound content a substantial challenge.

Outbound content compliance includes solutions that monitor, secure/encrypt, filter, and block outbound content contained in email, instant messaging, peer-to-peer, file transfers, Web postings, and other types of messaging traffic. OCC solutions play a key role in enforcing corporate governance, which is defined by IDC as a combination of complying with both external regulatory requirements and internal corporate policies and best practices.

Additionally, IDC defines OCC as a "competitive" market. Competitive markets are combinations of whole or fractions of functional markets that reflect such market dynamics as the problem being solved or the technology on which the software is based. Competitive markets are typically more ad hoc because they are meant to reflect current market approaches, coalitions, standards, and software architectures. Some competitive markets have been modeled to address a broad solution market category. OCC is an emerging competitive market with several product areas, which are discussed in the sections that follow.

#### ***Outbound Email Filtering***

Over the past 10 years, email has dramatically transformed the way most corporations do business. Many organizations have elevated email, formerly a "lowly" application, to "mission critical" status in their support priorities. As email use grows, extending enterprise communications to partners and customers, the challenge to manage these messages increases in scope and complexity. As previously stated, most enterprises have developed up-to-date means of protecting against external threats. However, managing the insider threat as it relates to outbound email has become an even more challenging task.

Organizations began with simple content-filtering techniques around keywords. As regulatory requirements become more clearly defined and the impact to organizations' bottom lines more severe, these simple techniques are no longer enough to ensure property security. Today, the only effective means of ensuring the privacy of confidential data is via a policy-driven approach whereby enterprises can define their own policies by more than simple dictionaries (e.g., determining which regulatory requirements affect the organization, is there intellectual property that needs to be protected, etc.). Effective policy-based solutions coupled with sophisticated content filtering for keywords or dictionaries should correlate with multiple detection engines to eliminate false positives. Detection techniques include fingerprinting, contextual analysis, and search engine capabilities. Additionally, relying on end users to determine what should or should not be protected is no longer an option in today's heavily regulated environment.

A flexible policy engine can automatically enforce corporate policy and automatically stop/block, encrypt, carbon copy, route, or other method of protection based on workflow, roles, and policy violation. Clearswift, Entrust, and Tumbleweed were pioneers in addressing outbound email security through email filtering. The strong demand for outbound email filtering solutions has attracted traditionally "external threat" focused messaging security vendors as well. Antispam and antivirus vendors such as CipherTrust, IronPort, Proofpoint, Symantec, MailFrontier, Trend Micro, FrontBridge, Sendmail, Postini, and Sophos are all in the process of developing or have developed outbound scanning, filtering, and blocking features for their messaging security products. IDC expects other messaging security vendors to offer outbound scanning capabilities as the demand continues to grow.

### ***Secure Email: Encryption***

The ability to encrypt email has been available for many years. Many enterprise-level email products, such as Lotus Notes, inherently have email encryption. Products such as PGP and standards such as S/MIME have long histories. However, the uptake of email encryption has been historically slow. Many factors have contributed to this, including difficulty to use, the lack of a strong business case, and interoperability. However, due to industry and government standards and regulations, the growing importance of email, and improved email security technology, the market now appears poised for growth. The need to secure business communication such as financial statements, patient health information (PHI), intellectual property, and other confidential information has fueled the need for secure email solutions.

While encryption plays a key role in compliance, it is only a piece of the compliance puzzle. Determining what to encrypt is more than half the battle. Organizations must define their policies (based on corporate and regulatory requirements) and employ solutions to automatically enforce defined policies, including an integrated, policy-driven encryption capability with support for multiple technologies.

The enterprise environment seems to be most receptive to gateway-based secure email because it reduces user interaction, reduces the key management needs, and does not require desktop installations. IDC believes gateway-secure email solutions have high growth potential because they are much easier to deploy and often include other features beyond email encryption such as content filtering. Key players in the

gateway secure email market include Sigaba, Tumbleweed, Entrust, PGP, PostX, Voltage, CipherTrust, and ZixCorp. Other vendors such as Clearswift, IronPort, Proofpoint, SurfControl, and Sendmail benefit from offering encrypted email through an integrated third party.

### ***Multiprotocol Content Filtering***

The threats associated with outbound content compliance apply not only to email but also to instant messaging, peer-to-peer, file transfers, Web postings, and other types of messaging traffic. Protecting confidential information and sensitive data from leaving an organization is quickly becoming a business-critical mission for enterprises of all sizes, and they are starting to understand the need to secure Internet protocols beyond email. The need for real-time monitoring to reduce the risk of compliance violations, corporate governance concerns, internal policy infractions, information leaks, and unacceptable Internet use exposes organizations to financial and legal liabilities as well as damage to brand and reputation.

The demand to secure protocols beyond email has created an emerging set of new vendors and products. Vericept, Tablus, Vontu, PortAuthority, Reconnex, Fidelis, Verdasys, and Oakley Networks have quickly established themselves as key players in the outbound content compliance market. IDC expects strong growth from existing vendors in this market as well as market growth from traditional "email only" security vendors expanding their offerings to address additional protocols such as instant messaging and Web email. CipherTrust and Proofpoint, for example, recently announced multiprotocol content filtering solutions. We expect other email security vendors to follow suit. There is already tight integration through strategic partnerships between email filtering vendors and instant messaging vendors. We expect this trend to continue. Moreover, we believe multiprotocol solutions must evolve from monitoring and reporting on information loss/leaking to prevention of information loss/leakage.

### ***Enterprise Rights Management***

The demand for solutions that safeguard confidential and sensitive data has been fueled by recent high-profile data thefts and government regulations. Security officers, compliance officers, and IT departments alike are all struggling to control the dissemination of and access to sensitive data contained in email, Word documents, and other types of electronic document formats. An emerging set of solutions that IDC is defining as enterprise rights management (ERM) is being deployed to address a broad spectrum of customer needs, including:

- Controlling access to and usage of confidential and sensitive information
- Preventing confidential and sensitive information from leaving an organization
- Protecting documents outside of the corporate firewall
- Ensuring compliance with government and industry regulatory requirements such as Gramm-Leach-Bliley, HIPAA, Sarbanes-Oxley, and SB 1386
- Enforcing policies around content creation, editing, sharing, publishing, and distribution

Key players in the enterprise rights management market include Microsoft, Workshare, Authentica, Adobe, Liquid Machines, SealedMedia, and other emerging vendors.

### ***Instant Messaging Security***

Instant messaging is beginning to challenge email's monopoly on text messaging. The value of instant messaging's immediacy and presence awareness is being noticed more widely in the workplace, and the need for security and policy enforcement for instant messaging is on the rise, including not only the approved IM tool but also unapproved IM, P2P, or other communication tools that may be slipped in by delinquent or unknowing users. This is especially true in certain regulated industries, such as financial services, where businesses must now ensure instant messaging security and policy enforcement just as they do email. Compliance with regulations such as Sarbanes-Oxley, HIPAA, and Gramm-Leach-Bliley is forcing organizations to take notice of the instant messaging use inside their organizations.

Key players in the instant messaging security market include FaceTime, IMlogic, Akonix, IM-Age, and CipherTrust. In addition, many email security vendors have strategic partnerships and tight integration with instant messaging security vendors. IDC expects to see more traditional "email only" security vendors add instant messaging security to their product lines through partnerships and acquisitions.

## **MARKET DRIVERS**

---

### **Government and Industry Regulations**

Government and industry regulations have placed unprecedented pressure on corporations to secure the use of their electronic communications. A wide range of communication channels available to employees, such as instant messaging, chat, Webmail, and peer-to-peer file sharing, represents a serious threat to customer information and can expose organizations to reputation, compliance, legal, and financial risks. Organizations that manage patient health information, social security numbers, and credit card numbers are being forced by government and industry regulations to implement minimal levels of security to address leakage of personal information. The loss of confidential personal information can materialize into compliance infractions, lawsuits from customers and/or patients, potential identity theft, and significant and often irreparable harm to an organization's credibility and reputation.

Many organizations are still struggling to understand the numerous regulations that potentially affect their organizations and what that means from a business perspective. In today's increasingly information-intensive businesses, technology is becoming a key part of strategic compliance initiatives to ensure sustainability of compliance-related processes, mitigate risk, and manage ongoing costs. Examples of pressing regulations are discussed in the sections that follow.

### ***Health Insurance Portability and Accountability Act***

The Health Insurance Portability and Accountability Act of 1996 has two major objectives: making healthcare transactions simpler through the use of standards, common code sets, and unique health identifiers; and protecting the confidentiality of patients' health information. The act applies not only to healthcare service providers but also to all healthcare entities, including insurance companies and government agencies.

The HIPAA Privacy Rule defines administrative, physical, and technical safeguards for covered entities (CE), which include standards for keeping the privacy of electronic protected health information (ePHI). These standards deal with several requirements that are most relevant for OCC solutions, including the implementation of policies and processes on issues like assigning and controlling access to ePHI; reporting incidents; keeping track of ePHI moving in, out, and within CE; and securing the transmission of ePHI over networks. Noncompliance with the security rule requirements may carry criminal penalties of up to \$250,000 in fines and jail time of up to 10 years.

The HIPAA Privacy Rule became effective in April 2003, and the compliance date for most CEs was April 2005 (smaller CEs should be in compliance by April 2006). Although the rule does not require CEs to implement specific security technologies and solutions, desktop-based and network-based OCC should benefit from heightened demand in the healthcare industry as they can meet some of the core requirements of the Privacy Rule.

### ***Gramm-Leach-Bliley***

The Gramm-Leach-Bliley Act (GLB) was passed to protect customer information maintained by (or on behalf of) financial institutions from loss, unauthorized access, or misuse.

The GLB Safeguard Rule requires all financial institutions to "develop, implement and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards" to protect customer "nonpublic information" (account numbers and details, social security numbers, credit card numbers, and so on). It mandates different requirements for safeguarding NPI, including the establishment of access controls of IT systems on which NPI is stored, encryption of electronic records, and monitoring of systems to detect intrusion attempts and attacks. Noncompliance with the Safeguard Rule may carry severe penalties in fines and prison terms of up to five years for individuals.

In light of the above, and although GLB — as in the case of the HIPAA Privacy Rule — does not require the use of specific security solutions, intrusion detection systems and encryption are being implemented by most financial institutions, and IDC believes OCC solutions should also take their share of the market for GLB compliance.

### ***Sarbanes-Oxley***

The Sarbanes-Oxley Act of 2002 (SOX) was legislated in the United States in light of high-profile corporate scandals such as those of Enron and WorldCom. Defining new requirements regarding the financial management of publicly traded companies, the act is aimed at ensuring the integrity and the accuracy of reporting and preventing accounting errors and wrongdoings that may affect a company's shareholders and the general public. SOX lays responsibility on CEOs and CFOs, who must certify that their companies' financial reports are complete and do not contain any inaccurate or misleading statements. Noncompliance may lead to fines of up to \$5 million for individuals and up to \$25 million for entities and prison sentences of up to 20 years.

Section 404, which describes management's responsibility for establishing "internal control over financial reporting," is one of the key sections of SOX in terms of outbound content compliance. Under this liability, companies are required to "provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the registrant's assets that could have a material effect on the financial statements."

The broad category of "assets" includes digital assets such as source code, trade secrets, M&A information, patient records, and any other sensitive information the unauthorized disclosure of which may have a negative impact on the company's stock price and its financial performance. Thus, organizations are required to closely monitor the usage of those assets and be able to detect such events in real time or near real time. The above should foster greater demand for OCC solutions.

### ***California SB 1386***

Effective July 1, 2003, California SB 1386 requires "a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information ... to disclose in specified ways, any breach of the security of the data ... to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

The act defines "personally identifiable information" (PII) as social security number, driver's license number or California Identification Card number, account number, and credit or debit card number ("in combination with any required security code, access code, or password that would permit access to an individual's financial account"). The act allows California residents who have been injured by a violation of the act to undertake civil action to recover damages. In addition, it allows courts to enjoin violating businesses.

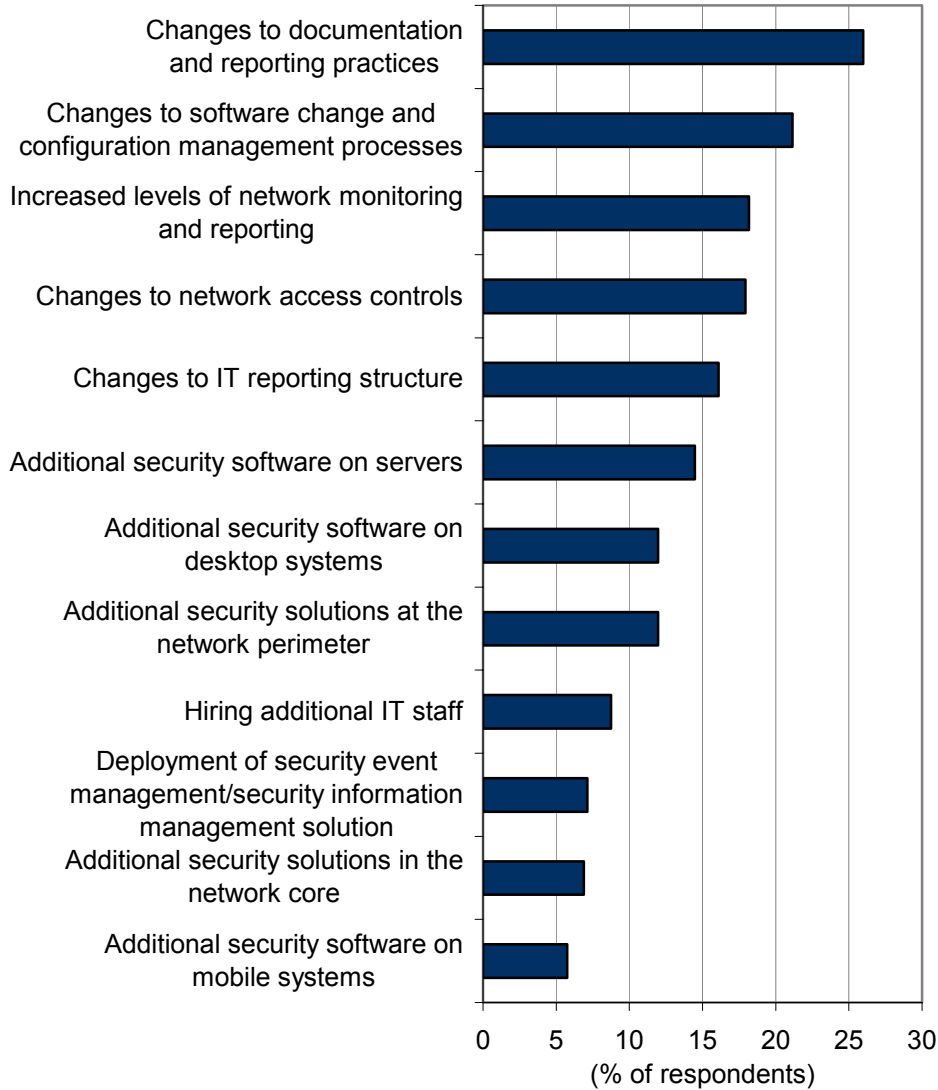
Practically speaking, organizations that are required to comply with this act should protect the IT systems in which they store and manage private information but also take appropriate measures to detect any unauthorized delivery thereof outside their boundaries. Thus OCC solutions could be relevant for that purpose and should benefit — especially considering 22 states have followed California's lead and federal legislation has been introduced.

### ***The Business Impact of Government and Industry Regulations***

As shown in Figure 1, government and industry regulations are impacting the way organizations deal with information security and staffing in many different ways. Increased levels of network monitoring and reporting are very close to the top of the list of concerns. IDC believes this is clearly driven by the pressure government and industry regulations have placed on corporations to secure the use of their electronic communications. We expect the risk of compliance infractions and lawsuits from customers and/or patients to continue to force organizations to implement network monitoring and reporting technologies.

**FIGURE 1**

Requirements Based on Impact of Regulations on Company Information Security and Staffing



N = 435

Source: IDC, 2005

### **Outbound Malicious Threats**

An increasing number of organizations is concerned about filtering their outbound email stream for threats such as spam, viruses, and spyware. These outbound malicious messages are generated by zombie PCs within their organizations. IDC believes the majority of spam sent today is sent from zombie PCs infected with spam trojans. Zombie PCs are computers that have been infected by malicious code that allow spammers to use them to send email. High-profile worms such as Sobig,

MyDoom, and Bagle are clear examples of threats containing malicious code that allow remote attackers to take over infected machines.

Many organizations are concerned that they will face legal liability if their customers or partners get "infected" by messages they generate, and they don't want to have their communications with customers and partners blacklisted because of malicious content coming from their domains. Moreover, organizations can face brand reputation damage when spam and viruses are sent from their networks. An organization's damaged reputation can be devastating to the credibility of the organization, leading to even greater negative financial impact. The Federal Trade Commission recently announced a plan that will leverage the agency's influence, along with that of 20 other governments across the globe, in an effort to reduce spam by targeting "zombie" PCs. The FTC and its partners have announced "Operation Spam Zombies," an international campaign to educate Internet service providers and other Internet connectivity providers about hijacked or "zombie" computers that spammers use to flood in-boxes here and abroad.

As antispam legislation and more sophisticated antispam products make it more difficult for traditional spammers to send junk email, spammers will increasingly look for other ways to send their messages. IDC believes spammers will continue to use techniques from virus writers and hackers to help them create more and more zombie PCs to send spam.

### ***High-Profile Incidents***

The growing awareness of outbound content compliance has been recently catalyzed by a series of corporate scandals in which customer records, confidential information, and intellectual property were leaked. As the vast majority of those cases demonstrate, such breaches are often not the result of malicious wrongdoing but rather employees who unknowingly put their companies at risk. This may occur as employees send out email messages that contain files or content they are not aware is confidential. Another example is employees delivering confidential files to their Web-based email boxes (or copying files to mobile devices) and thus exposing them to untrusted environments.

### ***Loss of Intellectual Property***

Protecting corporate intellectual property has also moved up the priority list of many IT departments. Organizations of various industry and company sizes are extremely concerned with protecting patents, trademarks, brands, trade secrets, designs, architectures, copyrights, algorithms, software code, hardware schematics, inventions, business processes, and many other corporate assets.

Gone are the days in which intellectual property and corporate secrets were kept safe in locked cabinets behind guarded doors. Today, nearly all corporate information exists in electronic form, accessible to almost any employee. Additionally, email has become the de facto filing system for much of this information, making it even more critical to protect the outbound flow of messages. The risks of inadvertent or deliberate disclosure of confidential information and intellectual property range from legal exposure to competitive disadvantage. Companies can risk losing serious

dollars when design documents and source codes are posted to Internet message boards or emailed outside the organization. Examples include:

- ☒ In February 2004, portions of the Windows 2000 and Windows NT 4 source code databases were leaked, apparently by one of Microsoft's outsourcers for code development.
- ☒ In December 2004, Apple filed a lawsuit against three members of its Apple Developer Connection network who allegedly distributed a prerelease version of "Tiger," the company's next major Mac OS X release, through the P2P file-sharing network BitTorrent.
- ☒ In October 2002, an internal Dell Computer document regarding Dell's plan for entering the PDA market was leaked and posted on a French Web site.

### ***Loss of Customer Records and Confidential Information***

A privacy failure, even a merely perceived failure to protect customer data, can result in loss of consumer trust, affect customer retention, and cause significant damage to brand and company reputation. Online privacy practices must be consistent with offline irreparable damage to brand, reputation, consumer retention, and customer-focused business strategy. There have been several high-profile incidents in which customer records and/or confidential information have been leaked, including:

- ☒ In June 2001, an Eli Lilly employee emailed the users of Medi-messenger, an email service that reminded subscribers to take their medications, to announce the termination of the service. Because of a human error, the message disclosed the names and email addresses of all the service subscribers in the "To:" line.
- ☒ Data collector ChoicePoint has mistakenly given private information on up to 145,000 U.S. residents to identity thieves. ChoicePoint reached an agreement in February 2005 with 19 state attorneys general to tell the 145,000 potential victims that identity thieves may have gained access to personal information such as social security numbers and credit reports.
- ☒ In September 2004, a former help desk employee at Teledata Communications pleaded guilty to a scheme to steal and sell 30,000 of the company's customers' consumer credit reports.
- ☒ In May 2000, Michael Eisner, then Walt Disney's CEO, accidentally emailed Disney's quarterly earnings press release to an ABC News employee prior to Disney's public earnings announcement. Luckily, the employee realized the mistake, alerted Eisner of the error, and prevented a possible SEC insider trading investigation.
- ☒ In June 2002, parts of Cisco's quarterly report were leaked via email, which forced the company to publish it ahead of its scheduled financial release.
- ☒ In October 2002, an email was sent from Merrill Lynch to Standard & Poor's; Merrill Lynch's request for an assessment of Commerzbank was leaked, causing the latter to issue a statement regarding its financial robustness.

Although in some of the above cases email usage policies were established, violations still occurred, which demonstrates that policies alone are not enough. Organizations are realizing that to prevent such incidents from happening, dedicated solutions that provide better control and enforcement mechanisms over electronic communications are becoming essential.

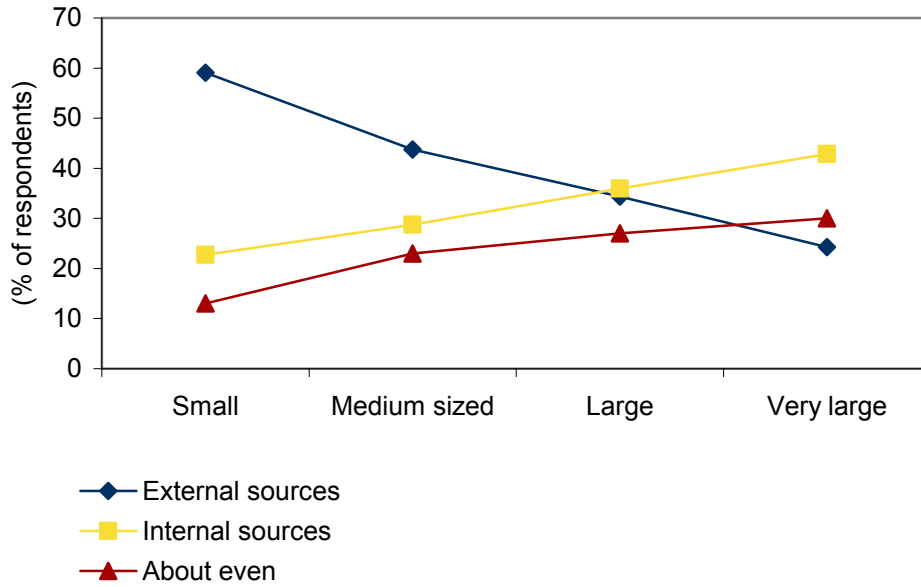
### ***Internal Versus External Threats***

According to a recent IDC survey of 435 North American organizations, internal threats are much more of a concern in large enterprise environments, as shown in Figure 2. Moreover, internal violations happen at a much higher degree in larger organizations, as shown in Figures 3 and 4. The growing concern with internal security threats comes as no surprise to IDC. In fact, there are several data points that lead us to believe the internal security threat will continue to rise:

- ☒ According to the latest CSI/FBI Computer Crime and Security Survey, 80% of respondents reported security incidents involving insider abuse in 2004 (up from 64% the previous year).
- ☒ According to IDC's 2004 Security Survey, 31% of organizations have terminated employees or contractors for internal security violations.
- ☒ According to IDC's 2005 Security Survey, employees following security policies was rated as the second-highest security challenge organizations will face over the next 12 months.

**FIGURE 2**

Internal Versus External Security Threats to Enterprise Security by Company Size

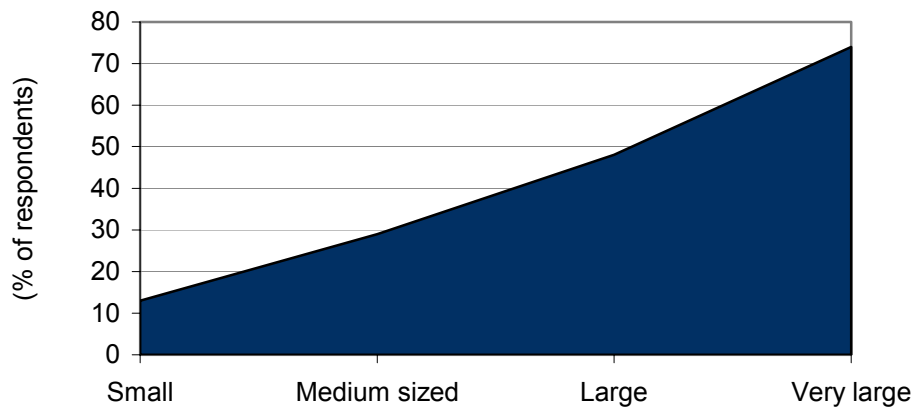


N = 435

Source: IDC, 2005

**FIGURE 3**

Internal Security Violations by Company Size

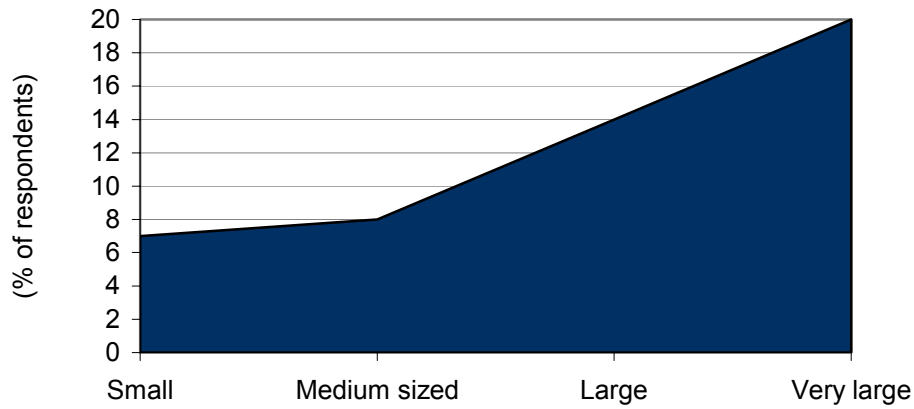


N = 435

Source: IDC, 2005

**FIGURE 4**

Exposure of Confidential Information by Company Size



N = 435

Source: IDC, 2005

## VENDOR PROFILE: KEY PLAYER IN OUTBOUND CONTENT COMPLIANCE

### Mirapoint

#### **Overview**

Mirapoint, founded in 1997, offers messaging and security solutions through purpose-built appliances designed to protect data networks. Mirapoint has 230 employees and is headquartered in Sunnyvale, California.

#### **Outbound Content Compliance Products**

Mirapoint offers the following OCC products:

- Mirapoint Razorgate and Message Store provide functionality to ensure outbound content compliance. This functionality includes:
  - Enforce envelope security through SSL/TLS.
  - Enforce envelope identity through directory-enabled SMTP authentication.
  - Require outbound connections to come from an internal network or VPN.

- ❑ Outbound content filters, which allow the identification of outbound messages based on header or body matches to known character strings, regular expressions, and word lists. Filter actions include quarantine (to be reviewed by a compliance officer), wiretap (for archiving purposes), redirection, and rejection that indicate exactly what happened to every message traversing the system. Combinations of these features, together with a functional firewall, provide the enterprise with the ability to protect the Internet from zombie PCs within the network — the major source of spam distribution on the Internet today.

### ***Strategic Direction***

Mirapoint is focused on the continued sales of Message Server to key service provider, education, government, and enterprise customers. Mirapoint's Message Server is an alternative to more traditional enterprise messaging products and is a versatile solution for a variety of employee segments. Message Server offers Webmail and collaboration features, as well as email, group calendaring, and address book functionality. Mirapoint's RazorGate offers a standalone email security appliance, which complements existing email servers (both Mirapoint and non-Mirapoint). Mirapoint continues to focus on building solutions that can prevent and filter out email threats.

## **ESSENTIAL GUIDANCE**

IDC believes the greatest challenge in terms of protecting customer records, confidential information, and intellectual property comes from unstructured content. Electronic documents, emails, instant messages, paper documents, calendars, Web conference proceedings, voicemail, electronic discussions, Web content, and inter-application transactions are either covered today or will soon be covered under one or more regulations and can certainly be included as part of evidence discovery. While financial, employee, and customer records are usually safe and sound in a secure database, unstructured content is frequently scattered across hundreds or even thousands of email and file servers. Unlike the records managed in the database, this unstructured content is typically not well organized, not easily found, controlled only under ad hoc security and access control policies, and generally not maintained in a way that provides any kind of context for the embedded information. Whether with regard to regulatory compliance or discovery, the unstructured content in most organizations represents a time bomb waiting to go off.

---

## **Copyright Notice**

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit [www.idc.com](http://www.idc.com) to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit [www.idc.com/offices](http://www.idc.com/offices). Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or [sales@idc.com](mailto:sales@idc.com) for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2006 IDC. Reproduction is forbidden unless authorized. All rights reserved.