proofpoint™

Control tomorrow's email risks today

Outbound Email and Data Loss Prevention in Today's Enterprise, 2010

Results from Proofpoint's seventh annual survey on outbound messaging and content security issues, fielded by Osterman Research during June & July 2010

Proofpoint, Inc.   892 Ross Drive   Sunnyvale, CA 94089   P 408 517 4710   F 408 517 4711   info@proofpoint.com   www.proofpoint.com

On behalf of Proofpoint, Inc., Osterman Research fielded an online survey of email decision makers at large US organizations. Respondents were asked about their concerns, priorities and plans related to the content of email leaving their organizations, as well as related concerns about the risks associated with mobile devices, blogs and message boards, social media sites, media sharing sites and other electronic communications technologies.

Osterman gathered a total of 261 responses from companies with 1,000 or more employees in June and July 2010. This report summarizes the findings of that study.

The latest version of this report is always available by visiting:

http://www.proofpoint.com/outbound

CONTENTS

This page intentionally left blank.

proofpoint

THE BOTTOM LINE: KEY FINDINGS, 2010

Selected "Fast Facts" from Proofpoint's *Outbound Email and Data Loss Prevention in Today's Enterprise, 2010* report, based on a June/July 2010 study of 261 email decision makers at large US enterprises (1000 or more employees). The latest version of this report is always available at http://www.proofpoint.com/outbound. For media inquiries, please email pr@proofpoint.com.

Who's Reading Your Corporate Email?

- More than a third (37%) of US companies with 1,000 or more employees surveyed employ staff to read or otherwise analyze outbound email. Additionally, 48% of companies surveyed perform regular audits of outbound email content.
- 38% of US companies with 20,000 or more employees surveyed employ staff whose *primary or exclusive* job function is to read or otherwise monitor outbound email content. Overall, one third (33%) of companies surveyed employ such staff.
- One fifth (20%) of companies surveyed said that employee email was subpoenaed in the past 12 months. The largest companies were affected more frequently, with more than a quarter (27%) of companies with 5001 to 20,000 employees and more than half (54%) of companies with more than 20,000 employees reporting that they were ordered to produce employee email.

How Common are Data Leaks in General? Via Email? Via Lost or Stolen Devices?

- More than one third (36%) of US companies surveyed say their business was impacted by the exposure of sensitive or embarrassing information in the last 12 months. Nearly one third (31%) said they had been impacted by improper exposure or theft of customer information. 29% said they had been impacted by the improper exposure or theft of intellectual property.
- 35% (down from 43% in 2009) of US companies investigated a suspected email leak of confidential or proprietary information in the past 12 months. 32% (slightly down from 34% in 2009) investigated a suspected violation of privacy or data protection regulations in the past 12 months.
- More than 1 in 5 of US companies surveyed (22%) investigated the exposure of confidential, sensitive or private information via lost or stolen mobile devices in the past 12 months. 56% of respondents are highly concerned about the risk of information leakage via email sent from mobile devices.

How Often are Employees Fired or Disciplined for Email Misuse?

- One fifth of US companies surveyed (20%) terminated an employee for violating email policies in the past 12 months (down from 31% in 2009). Half of US companies surveyed (50%) disciplined an employee for violating email policies in the past 12 months.

Data Leaks via Social Media: Facebook, YouTube and Twitter a Risk? Can it Get You Fired?

- 25% (up from 18%) of US companies surveyed investigated the exposure of confidential, sensitive or private information via a blog or message board posting. 24% (up from 17%) disciplined an employee for violating blog or message board policies in the past 12 months. 11% (up from 9%) reported terminating an employee for such a violation. 54% (up from 46%) are highly concerned about the risk of information leakage via blogs and message board postings.
- 20% (up from 17% in 2009) of US companies investigated the exposure of confidential, sensitive or private information via a posting to a social networking site (e.g., Facebook, LinkedIn). 20% have disciplined an employee for violating social networking policies in the past 12 months. 7% (down from 8%) reported terminating an employee for such a violation. 53% (up from 45%) are highly concerned about the risk of information leakage via posts to social networking sites.
- 18% of US companies investigated the exposure of confidential, sensitive or private information via video or audio media posted to a media sharing site (e.g., YouTube, Vimeo). 21% (up from 15% in 2009) have disciplined an employee for violating media sharing/posting policies in the past 12 months. 9% (up from 8% in 2009) reported terminating an employee for such a violation. 52% (up from 42%) are highly concerned about the risk of information leakage via media sharing sites.
- 17% (up from 13%) of US companies investigated the exposure of confidential, sensitive or private information via an SMS text or Web-based short message service (e.g., Twitter). 51% (up from 41%) are highly concerned about the risk of information leakage via Web-based short messaging (e.g., Twitter).

Is the Recession Increasing the Risk of Data Loss?

- 58% (up from 50%) of respondents say that budget constraints have negatively impacted their organization's ability to protect confidential, proprietary or sensitive information in the past 12 months.
- 48% (up from 42%) of respondents say that increasing numbers of layoffs at their organizations in the past 12 months have created an increased risk of data leakage.
- 21% (up from 18%) of US companies investigated a suspected leak or theft of confidential or proprietary information associated with an employee leaving the company (e.g., through voluntary or involuntary termination) in the past 12 months.

This page intentionally left blank.

OVERVIEW

Email remains the most important medium for communications both inside and outside the enterprise. But the convenience and ubiquity of email as a business communications tool has exposed enterprises to a wide variety of legal, financial and regulatory risks associated with outbound email. Enterprises continue to express a high level of concern about creating, managing and enforcing outbound messaging policies (for email and other communication protocols) that ensure that messages leaving the organization comply with internal rules, best practices for data protection and external data protection, encryption and privacy regulations. In addition, organizations remain very concerned about ensuring that email, the Web and social media tools cannot be used to disseminate confidential or proprietary information.

This report summarizes the findings of Proofpoint's seventh annual survey of enterprise attitudes about outbound email, content security and data protection. Its goal is to "take the pulse" of IT decision-makers with respect to outbound messaging and data loss issues and to help raise awareness of the policy, technology and cultural issues surrounding email and Web monitoring, data protection and information leaks.

The results of the 2010 survey show that while the corporate SMTP email server is no longer the number one source of data loss *concern* for messaging decision makers (respondents showed a higher level of concern about the physical loss of mobile devices, Web-based email and email sent from mobile devices), email remains the number one source of leaks of confidential or proprietary information in the enterprise.

And as new communication technologies—such as social media sites, short messaging services and other Web services—gain broader adoption in the enterprise, the level of concern about those technologies and the number of data loss events experienced via those technologies is growing.

In response to the increasing popularity of social media both inside and outside the workplace, this year's survey examined new policy areas, including how many large enterprises explicitly prohibit the use of various social media technologies, what types of inappropriate content are most commonly found in social media communications and how commonly companies train employees on their Web and social media policies.

With the economic environment continuing to be turbulent in the US and around the world, this year's survey (as in the 2009 edition) includes a look at how the economic downturn continues to affect organizations' abilities to protect confidential and proprietary data.

About the 2010 Study

This report summarizes findings from Proofpoint's 2010 study of outbound email and content security issues in the enterprise. This effort was started in 2004 when enterprise attitudes about inbound messaging issues (e.g., spam and viruses) were much better understood than concerns about outbound email content (e.g., data protection, privacy, regulatory compliance and intellectual property leak protection).

This study was designed to examine (1) the level of concern about the content of email (and other forms of electronic messaging) leaving large organizations, (2) the techniques and technologies those organizations have put in place to mitigate risks associated with outbound messaging, (3) the state of messaging-related policy implementation and enforcement in large organizations and (4) the frequency of various types of policy violations and data security breaches.

Over time, the scope of this survey has expanded from a pure focus on email to an examination of other message streams including Web-based email, mobile email, blogs and message board postings, media sharing and social networking sites. Beginning in 2009, Proofpoint added questions related to security concerns around SaaS/cloud computing, declining budgets and employee layoffs and these questions were asked again in 2010.

For the 2010 survey, Proofpoint commissioned Osterman Research to field an online survey of email decision makers at large enterprises in the US. Respondents were asked about their concerns, priorities and plans related to email, the Web, social media and other technologies that potentially create data loss risks. During June and July 2010, Osterman gathered responses from enterprises with 1,000 or more employees. In total, 261 valid responses were received, comprised of 190 companies with 1000-5000 employees, 45 with 5001-20,000 employees and 26 with more than 20,000 employees. Respondents were qualified based on their knowledge of their organization's email and messaging policies and technologies. In all cases, respondents were either IT decision-makers or IT influencers of their organizations' messaging technologies and policies.

Complete demographic information about the respondents and their organizations can be found in the appendix to this report.

Media and Analyst Use of this Report

Media and analyst firms are welcome to cite statistics and findings from this report with proper attribution.

The source of this data is Proofpoint, Inc., an email security and compliance vendor based in Sunnyvale, CA, http://www.proofpoint.com.

In online citations, a link to the download page for this report:

http://www.proofpoint.com/outbound

is always appreciated.

Proofpoint researchers and executives are available for commentary on this report, its findings and related issues around email, social media, data loss, information security and technology in the workplace.

For media inquiries, please email:

pr@proofpoint.com

CONCERNS ABOUT OUTBOUND EMAIL COMPLIANCE AND CONTENT SECURITY

As in previous years, respondents were asked to rate their current level of concern around a variety of compliance, data protection and security issues related to the content of email leaving their organizations. The survey asked about level of concern around seven different outbound email topics. The specific question asked was, "Please rate your current level of concern around the following compliance and security issues related to the content of email leaving your organization (outbound email messages)":

Complying with internal email policies

Respondents were asked to rate their level of concern around "ensuring compliance with internal corporate email policies."

Complying with healthcare privacy regulations and guidelines

Respondents were asked to rate their level of concern around "protecting the confidentiality of private healthcare information."

Complying with financial privacy regulations and guidelines

Respondents were asked to rate their level of concern around "protecting the confidentiality of personal identity and financial information."

Complying with financial disclosure and corporate governance regulations

Respondents were asked to rate their level of concern around "ensuring compliance with financial disclosure or corporate governance regulations."

Guarding against leaks of valuable IP and trade secrets

Respondents were asked to rate their level of concern around "ensuring that email cannot be used to disseminate company trade secrets or valuable intellectual property."

Guarding against leaks of confidential memos

Respondents were asked to rate their level of concern around "ensuring that email cannot be used to disseminate confidential internal memos."

Guarding against inappropriate content and attachments

Respondents were asked to rate their level of concern around "monitoring email for offensive or otherwise inappropriate content and attachments."

Top Outbound Email Concerns

Figure 1 shows the percentage of respondents who reported being "very concerned" or "concerned" about each of the topic areas. As in previous years, respondents demonstrated a high level of concern across all categories—in each one, more than 60% of all respondents reported being "concerned" or "very concerned."

One interesting finding from the 2010 survey is that respondents from organizations with 5001 to 20,000 employees reported noticeably lower levels of concern versus their counterparts in smaller and larger organizations. This trend can be observed across other survey areas as well. As can be seen later in the report, these organizations tend to be more likely to have formal policies in place, have conducted more training on email-related policies, report lower rates of policy violations that result in employee discipline or termination and are less concerned about data loss risks in general.

For 2010, ensuring compliance with financial disclosure and corporate governance regulations was the area of greatest concern, with 74% of respondents reporting that they are "concerned" or "very concerned". Protecting the confidentiality of personal identity and financial information in outbound email was the second most important issue, with 72% of US respondents reporting a high level of concern. Tied for third place, 71% of respondents said they were "concerned" or "very concerned" about "ensuring that email cannot be used to disseminate company trade secrets or valuable intellectual property" and "ensuring that email cannot be used to disseminate confidential internal memos."

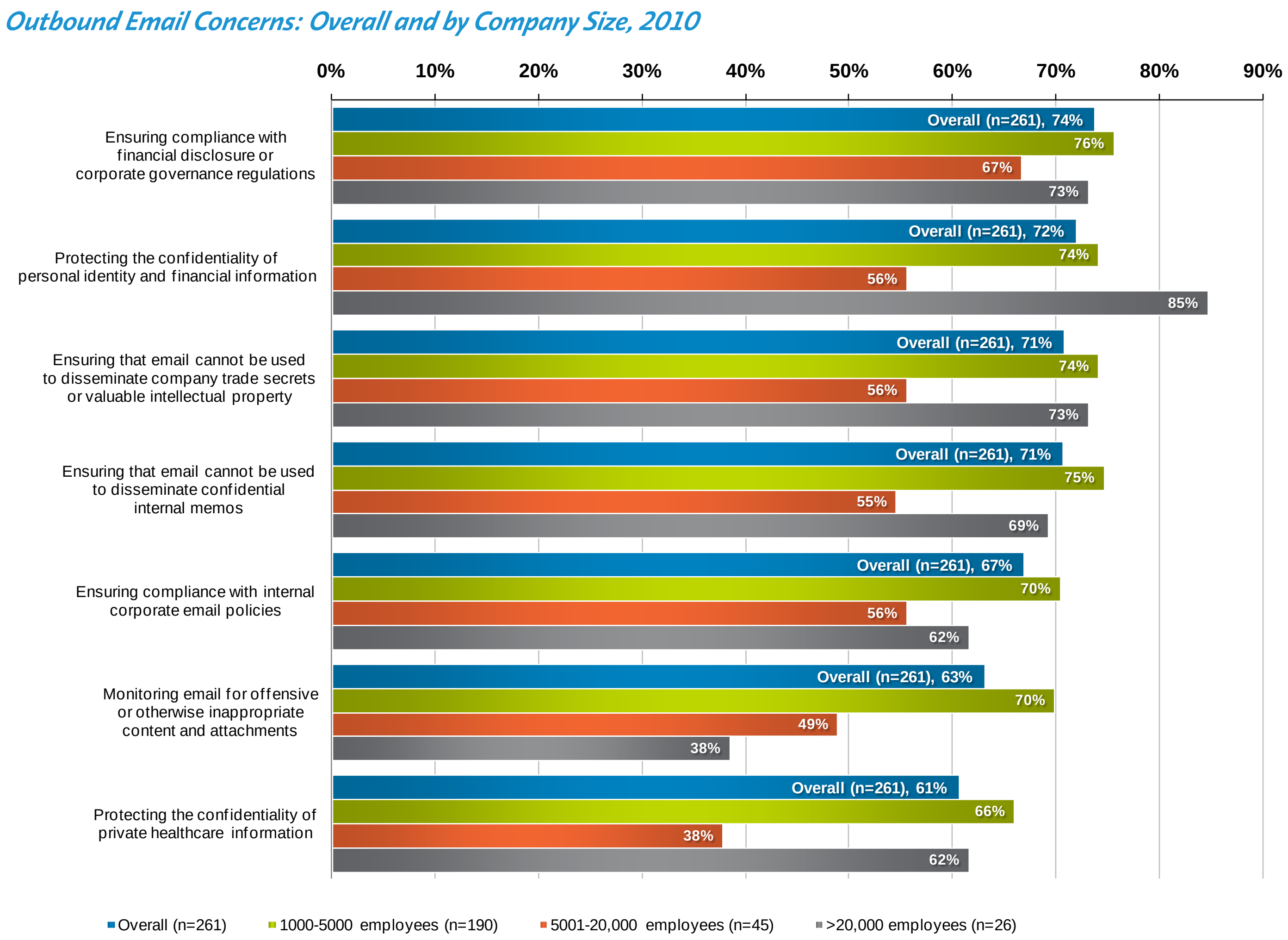

Figure 1: Percentage of respondents who reported being "very concerned" or "concerned" about various outbound email security issues.

HOW RISKY IS OUTBOUND EMAIL AND IM/SOCIAL MEDIA CONTENT?

As a way of estimating the magnitude of the problem posed by non-compliant email messages in today's enterprise, respondents were asked three questions. First, they were asked how common it is for various forms of inappropriate content to be found in email leaving their organizations. Second, they were asked how common it is for various forms of inappropriate content to be found in instant messages or social media content leaving their organizations. Respondents were also asked to estimate what percent of their organizations' outbound email contains content that poses a legal, financial or regulatory risk.

Most Common Forms of Inappropriate Content in Outbound Email

Respondents were asked, "On a scale of 1 to 5, how common is it to find the following types of inappropriate content in email leaving your organization, where 1 is 'almost never happens' and 5 is 'this is very common'?"

Figure 2, below, charts the distribution of answers (across all respondents) for four different types of inappropriate content in outbound email:

- **Adult, obscene or potentially offensive content.** 18% of respondents say this type of content is "common" or "very common" in outbound email.

- **Confidential or proprietary business information** about your organization. 21% of respondents say this type of content is "common" or "very common" in outbound email.
- **Valuable intellectual property or trade secrets** which should not leave the organization. 23% of respondents say this type of content is "common" or "very common" in outbound email.
- **Personal healthcare, financial or identity data** which may violate privacy and data protection regulations. 27% of respondents say this type of content is "common" or "very common" in outbound email.

Most Common Forms of Inappropriate Outbound Email Content, 2010

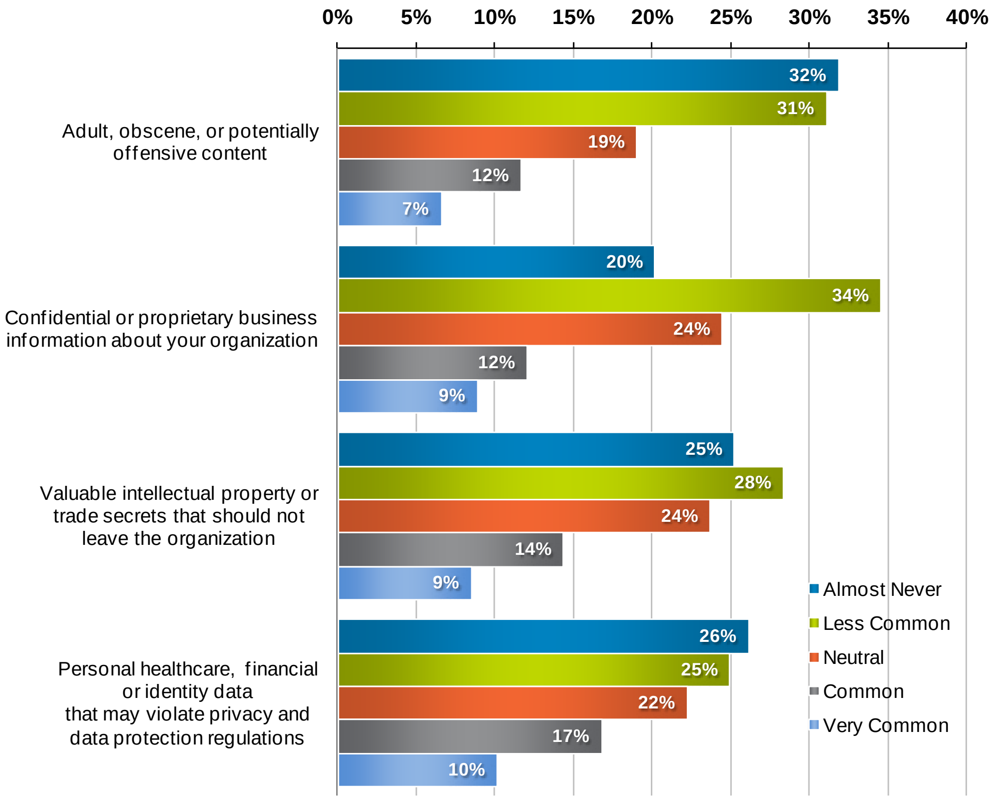

Figure 2: Four different categories of inappropriate content. Respondents rated how common it is to find each type of content in email leaving their own organizations.

As Many as 1 in 5 Outbound Emails May Pose a Risk

Asked "Using your best estimate, what percent of your organization's outbound email contains content that poses a legal, financial or regulatory risk to your organization?", the *mean* (average) answer for all respondents who provided an estimate (212 respondents) was that 1 in 5 (20% of) outbound email messages poses a risk.

Not all survey respondents provided an estimate in answer to this question, with 19% of respondents answering that they "don't know." Responses also varied widely and were skewed toward the lower end of the scale. The median answer was that 1 in 10 (10%) email messages contains risky content (that is, half of respondents estimated less than 10%, while the other half estimated more than 10%).

Most Common Forms of Inappropriate Content in Outbound IM and Social Media

Respondents were also asked, "On a scale of 1 to 5, how common is it to find the following types of inappropriate content in instant messaging or social media tools leaving your organization, where 1 is 'almost never happens' and 5 is 'this is very common'?"

Figure 3, below, charts the distribution of answers (across all respondents) for four different types of inappropriate content in outbound instant messages and social media communications:

- **Adult, obscene or potentially offensive content.** 20% of respondents say this type of content is "common" or "very common" in outbound IM and social media.
- **Confidential or proprietary business information** about your organization. 22% of respondents say this type of content is "common" or "very common" in outbound IM and social media.
- **Valuable intellectual property or trade secrets** which should not leave the organization. 22% of respondents say this type of content is "common" or "very common" in outbound IM and social media.
- **Personal healthcare, financial or identity data** which may violate privacy and data protection regulations. 25% of respondents say this type of content is "common" or "very common" in outbound IM and social media.

Most Common Forms of Inappropriate Outbound IM and Social Media Content, 2010

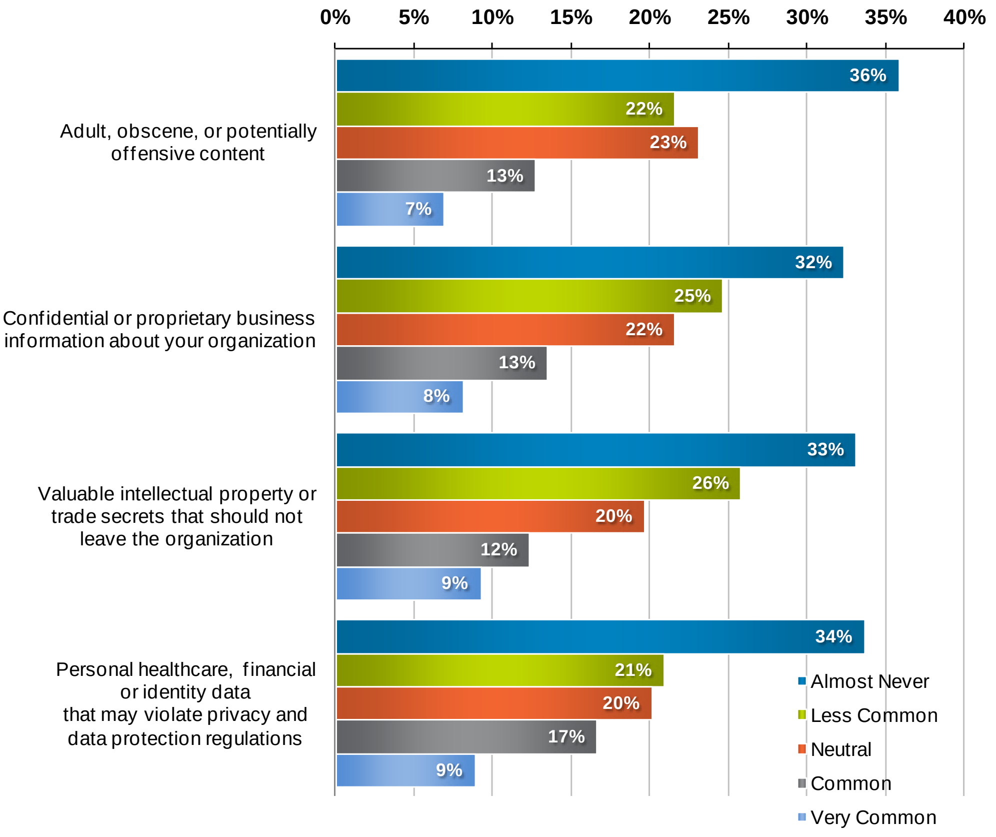

Figure 3: Four different categories of inappropriate content in outbound instant messaging and social media content. Respondents rated how common it is to find each type of content in IM or social media communications leaving their own organizations.

HOW DO COMPANIES REDUCE OUTBOUND EMAIL RISKS TODAY?

The survey also asked respondents about their organization's deployment of a variety of techniques and technologies to mitigate risks related to outbound email content, compliance and security. As we saw in the 2009 sample, the 2010 results show that only a small subset of technologies (specifically, email archiving and outbound spam and malware detection) has achieved more than 50% penetration in large enterprises.

Manual processes—such as conducting regular audits of outbound email content and employing staff to read outbound email—continue to be relatively common.

Figure 4 shows the techniques and technologies the survey asked about and the percentage of companies that report having already deployed each (overall results as well as a breakout by company size are shown).

Reading Employee Email and Other Manual Processes are Still Common

As in previous years, one of the most interesting results of the survey was the high percentage of organizations that reported they employ staff to read or otherwise analyze the contents of outbound email messages (see Figure 4).

In this year's survey, more than a third of all US respondents—37% (down slightly from the all-time high of 38% in the 2009 survey)—reported that they employ staff to monitor (read or otherwise analyze) outbound email content. An additional 26% of companies surveyed said that they intend to deploy such staff in the future. In previous years, the largest organizations (those with more than 20,000 employees) were much more likely to use this technique. However, 2010 results show companies in the 1000 to 5000 employee and more than 20,000 employee ranges reporting the same frequency. Organizations in the 5001 to 20,000 employee range were less likely to employ this, and other, manual techniques for monitoring outbound email as can be seen in Figure 4.

Overall, the number of US companies that say they employ staff to monitor the contents of outbound email has remained fairly consistent from year to year at roughly one-third (e.g., 38% in 2009, 29% in 2008, 32% in 2007, 38% in 2006, 36% in 2005 and 31% in 2004).

In previous years, these findings generated a great deal of interest and a common question that was raised was, "How many of these staffers monitor outbound email content as their main job function?"

To address this issue, starting in 2007 and continuing this year, the survey asked companies if they "employ staff whose *primary* or *exclusive* job function is to read or otherwise analyze outbound email content." The 2010 findings stayed at the same high level hit in 2009, with 33% of US companies surveyed saying they employ such staff. An additional 25% say that they intend to employ such staff in the future.

The survey also asked respondents if they perform regular audits of outbound email content. Overall, 48% of surveyed companies perform such audits (up slightly from 46% in 2009).

Adoption of Techniques and Technologies for Mitigating Outbound Messaging Risks, Overall and by Company Size, 2010

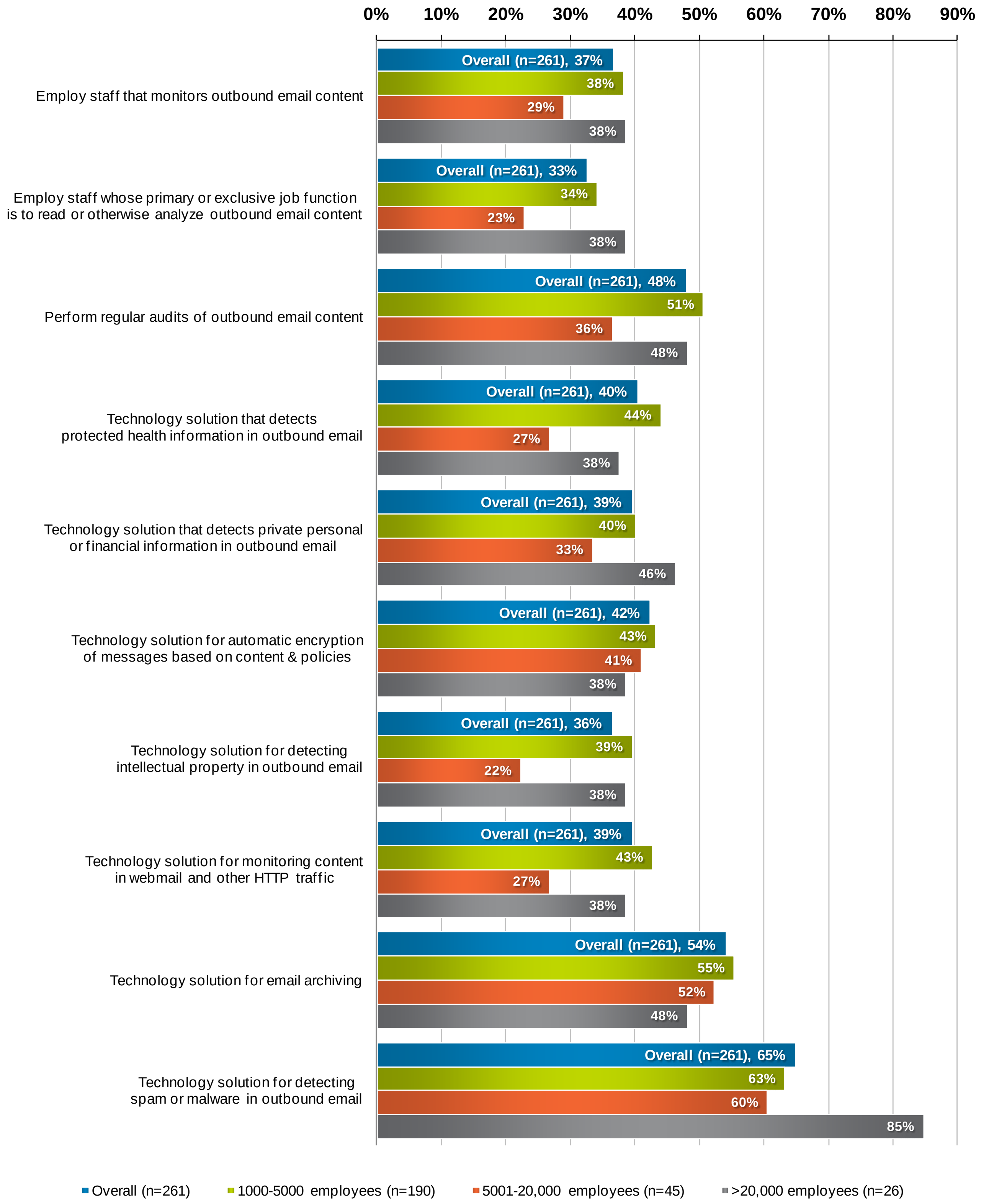

Figure 4: Percentage of respondents, overall and by company size, who report having deployed or used various techniques and technologies for mitigating outbound messaging-related risks.

Adoption of Technology Solutions for Mitigating Outbound Messaging Risks

In addition to the manual processes described previously, the survey asked respondents about their deployment plans for a variety of outbound content security technologies. Note that the survey did not ask for details, such as vendor or product name, associated with these deployments—it simply asked whether these broad classes of technology had been deployed. See again Figure 4.

Adoption of solutions for detecting protected healthcare information in outbound email

Respondents were asked if they have deployed a technology solution that detects protected health information in outbound email. 40% (up from 36% in 2009) of US companies reported using such technology.

Adoption of solutions for detecting identity or financial information in outbound email

Respondents were asked if they have deployed a technology solution that detects private personal or financial information (such as social security numbers) in outbound email. 39% (up from 36% in 2009) of US companies reported using such technology.

Adoption of content aware / policy-based email encryption

Respondents were asked if they had deployed a technology solution for automatic encryption of messages based on message content and policies ("content aware" encryption). Content-aware encryption solutions are commonly used for compliance with data protection regulations such as HIPAA in the US (which specifies that private healthcare information cannot be transmitted in an unencrypted form). An increasing number of US states have also adopted data privacy regulations that require or imply that companies should use encryption technology to protect their residents' personal information. 42% of companies surveyed this year (down slightly from 43% in the 2009 sample) say they have deployed such a solution.

Adoption of solutions for detecting intellectual property in outbound email

Respondents were asked if they had deployed a technology solution for detecting intellectual property in outbound email. 36% (up slightly from 35% in 2009) of US respondents say they have deployed such a solution.

Adoption of solutions for webmail / HTTP monitoring

Respondents were asked if they had deployed a technology solution for monitoring content in webmail (i.e., HTTP email services such as Hotmail, Gmail, etc.) and other HTTP traffic leaving the organization. 39% (up from 35% in 2009) of US respondents said they have deployed such a solution.

Adoption of email archiving technology

Respondents were asked if they had deployed a technology solution for email archiving. 54% (down from 58% in the 2009 sample) of US respondents said they have deployed such a solution.

Adoption of technology for outbound spam and malware detection

Respondents were asked if they had deployed a technology solution for detecting spam or malware in outbound email. This question is new to the 2010 edition of the survey. One trend that industry analysts and email security firms have observed is that enterprises are increasingly concerned about infected machines on their internal networks that may be used to send spam or malware (malicious software such as computer viruses). Machines compromised in this way are the top source of spam and malware today.

Overall, 65% of US organizations say they have deployed technology that can detect spam or malware in outbound email (and a very high percentage of organizations with more than 20,000 employees—85%—report having such a solution in place).

OTHER CONDUITS FOR EXPOSURE OF CONFIDENTIAL INFORMATION

Though this survey primarily explores concerns about the corporate email system, email is not the only technology that poses a potential risk to organizations. Other communication protocols, Web-based services, social media tools, messaging devices and file transfer mediums can also be conduits for confidential information exposure or sources of regulatory risk.

Respondents were asked to rate their current level of concern about a variety of outbound data streams, including various forms of email, as conduits for the exposure of confidential or proprietary information. The key findings, overall and broken out by company size, are summarized in Figure 6 which shows the percentage of respondents who reported being "concerned" or "very concerned" about each outbound data stream.

In previous years' surveys (2006 through 2009), most conduits were rated as a concern by 40% or more of US respondents and this continues to hold true in 2010 as can be seen in Figure 6. More than half of respondents expressed a high level of concern about all but two categories (FTP and peer-to-peer networks). As noted previously, when looked at by company size, respondents in the 5000 to 20,000 employee category demonstrated a somewhat lower level of concern than their counterparts in other size categories.

For every category, the 2010 results showed a higher level of concern than 2009. While Figure 6 shows the relative levels of concern about different data loss conduits, Figure 10 (later in this document) shows how frequently organizations investigated different types of data loss events.

Level of Concern about Lost Mobile Devices and Storage Media

While previous editions of this survey have asked about the frequency of suspected data loss events due to lost or stolen mobile devices and storage media, they did not ask respondents to rate their level of concern about this issue. New for 2010, respondents were asked to rate their level of concern around the "physical loss of laptops, smartphones and other devices that contain corporate data" as a conduit for exposure of confidential or proprietary information.

This turned out to be the category that causes IT decision makers the most concern with 64% of respondents saying they were "concerned" or "very concerned." While this topic *worries* respondents more than any other category (including various types of email, other communication protocols and social media), it's interesting to note that respondents *investigated* more data loss events caused by email (35% reported such an investigation) and blogs/message boards (25% reported such an investigation) than data losses caused by lost or stolen mobile devices and storage media (22% reported such an investigation). See Figure 10, later in this report for the frequency of data loss events by category.

Level of Concern about Web-based Email as a Conduit for Data Loss

Of all types of email, Web-based email services (e.g., services such as Google Gmail, Hotmail and Yahoo! Mail) causes IT decision makers the most concern. This year, 60% (up from 50% in 2009) of respondents said they were "concerned" or "very concerned" about Web-based email services as a conduit for the exposure of confidential information.

Level of Concern about Mobile Email as a Conduit for Data Loss

Respondents were asked about their level of concern about email sent from mobile devices (such as smartphones or other wireless, Internet-connected devices). More than half (56%, up from 51% in 2009) respondents said they are "concerned" or "very concerned" about the potential for data loss via mobile email.

The survey also asked respondents to provide their best estimate for what percentage of their organization's employees have mobile access to the corporate email system via smartphones or other wireless handheld devices. The overall mean estimate was that approximately one third (32%) of employees have such access.

For statistics on the number of data loss incidents associated with *lost or stolen* mobile devices and storage media (as well as other categories), please see "Policy Enforcement and Investigations of Suspected Violations" and Figure 10, later in this document.

Level of Concern about Outbound Corporate Email as a Conduit for Data Loss

Email sent from the organization's SMTP email system (corporate email) was once again cause for a high level of concern for more than half of respondents (55%, up from 51% in 2009). Larger organizations (those with more than 5000 employees) expressed slightly more concern about SMTP email than they did about email sent from mobile devices.

Level of Concern about Blog/Message Board Postings as a Conduit for Data Loss

As in previous years, blogs and message boards were also considered a significant source of data loss risk. More than half of respondents (54% up from 46% in 2009) expressed a high degree of concern about blog and message board postings as conduit for exposure of confidential or proprietary information.

Level of Concern about Social Networking Site Postings as a Conduit for Data Loss

For the third year, survey respondents were asked to rate their level of concern about postings to social networking sites (e.g., Facebook, MySpace, LinkedIn, etc.) as potential conduits for the exposure of confidential or proprietary information. As awareness and use of social networking sites has become ubiquitous, it's no surprise to see the level of concern about these communication channels increasing.

This year, 53% of respondents said they were "concerned" or "very concerned" about posts to social networking sites as a potential conduit for data loss (up from 45% in 2009 and 44% in 2008).

Level of Concern about Media Sharing Sites as a Conduit for Data Loss

The continuing popularity of video and audio media sharing sites (e.g., YouTube, Vimeo, etc.) and the proliferation of digital media creation in the workplace continues to be a source of data loss risk in large organizations. This year, 52% (up from 42% in 2009) of respondents expressed a high level of concern about postings to media sharing sites.

Level of Concern about Short Messages Sent from Mobile Devices as a Conduit for Data Loss

For the second year, the survey asked respondents to rate their level of concern about short messages sent from mobile devices (e.g., SMS text messages or similar) as a potential source of data loss. 51% (up from 44% in 2009) of respondents said they were "concerned" or "very concerned."

As can be seen from Figure 6, respondents from companies with 1000 to 5000 employees expressed a greater level of concern around this category than their counterparts in larger organizations.

Level of Concern about Short Messages Sent Via Web-based Short Messaging Services as a Conduit for Data Loss

For the second year, the survey asked respondents to rate their level of concern about short messages sent from Web-based short messaging and notification services (e.g., Twitter, Friendfeed, etc.). The increasing popularity of services like Twitter is clearly driving an increase in concern as 51% (up from 42% in 2009) of respondents said they were "concerned" or "very concerned" about the potential for data loss via these channels.

Level of Concern about Instant Messaging (IM) as a Conduit for Data Loss

Data loss for Instant Messaging (IM) continues to be a concern for IT decision makers with half (50%, up from 45% in 2009) of respondents expressing a high level of concern about IM as a conduit for data loss.

Level of Concern about FTP (File Transfer Protocol) as a Conduit for Data Loss

In previous years, respondents had expressed the lowest level of concern about the venerable FTP (File Transfer Protocol). The 2010 survey finds that just under half (49%, up from 39% in 2009) of respondents expressing a high level of concern about FTP as a potential source for data loss.

Level of Concern about Peer-to-Peer (P2P) Networks as a Conduit for Data Loss

Though respondents expressed the least amount of concern about peer-to-peer networks (commonly used for both legitimate distribution and rights-infringing sharing of digital files), a significant, and increasing, number of respondents (46%, up from 40% in 2009) said they were "concerned" or "very concerned" about P2P networks as potential conduits for data loss.

Level of Concern about Potential Conduits for Exposure of Confidential Information, Overall and by Company Size, 2010

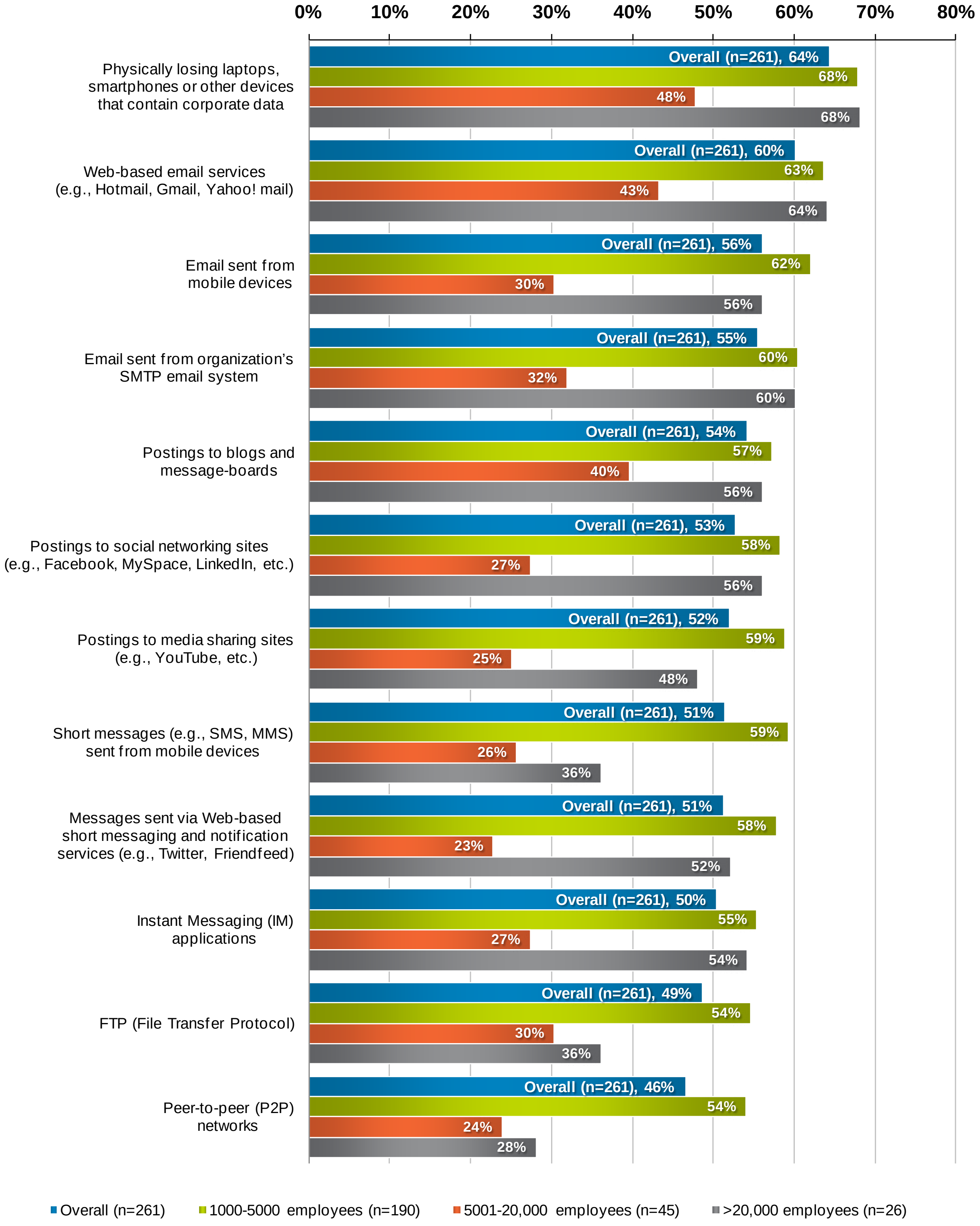

Figure 6: Percentage of respondents who reported being "concerned" or "very concerned" about various protocols that may serve as conduits for exposure of confidential info.

THE MESSAGING POLICY ENVIRONMENT IN TODAY'S ENTERPRISE

An important part of mitigating outbound messaging risks is the implementation of well-defined company policies related to the use of email and other forms of electronic communication. Some of these policies are specifically email-related and others relate to broader corporate governance and IT security issues.

Prohibitions on Personal Use of Email and Web, Social Media Sites

New in the 2010 survey, respondents were also asked if their organization's policies explicitly prohibit various activities including personal use of email and the Web at work, use of popular social media sites and use of media sharing services. These findings (overall and by company size) are summarized in Figure 7.

In brief, the majority (63%) of large enterprises surveyed explicitly prohibit the use of peer-to-peer file sharing sites.

Roughly half of large enterprises explicitly prohibit the use of popular social network Facebook (53%), media sharing sites such as YouTube (53%), and short message service Twitter (49%).

Roughly 40% of organizations explicitly prohibit the use of personal Webmail at work (40%), personal use of the Web at work (39%) and personal use of corporate email during company time (38%).

Nearly a third of organizations prohibit use of popular "professional" social network LinkedIn (31%).

Prohibitions on Use of Web, Social Media and Personal Email at Work, Overall and by Company Size, 2010

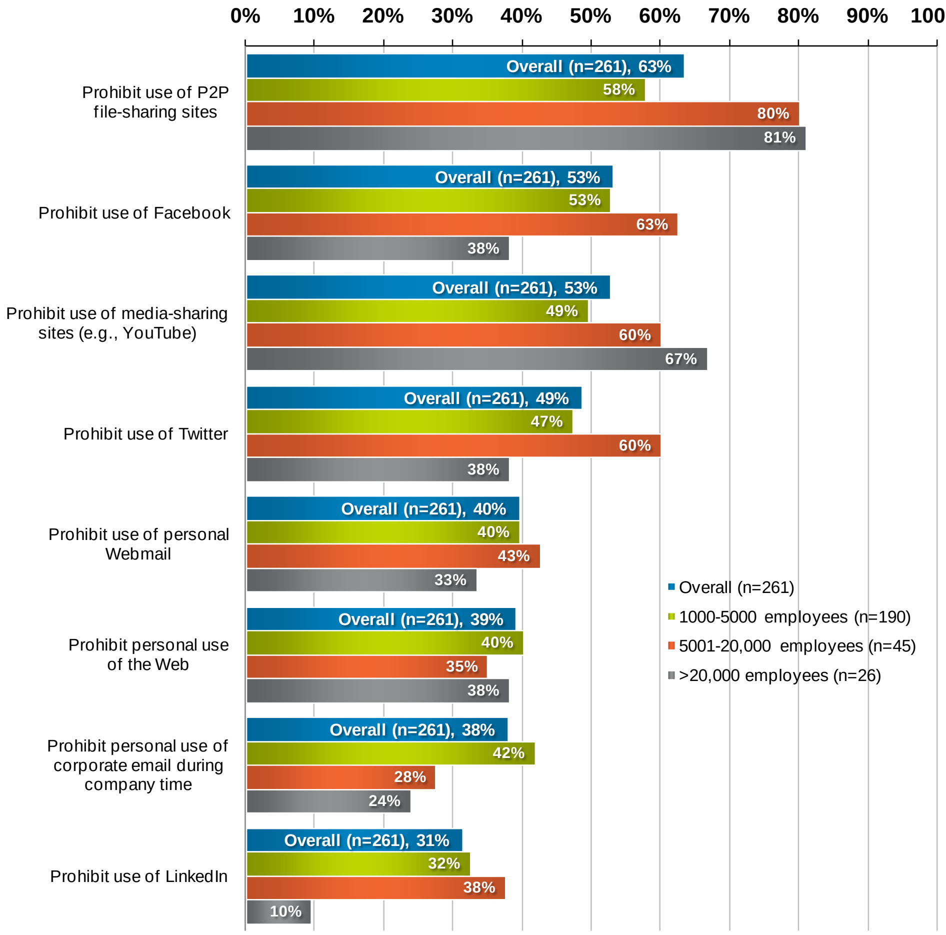

Figure 7: Percentage of respondents who report that their organization's policies explicitly prohibit personal use of email and webmail, and various social media and web technologies at work.

Adoption of Various Email, Compliance and Security-related Policies

As in previous years, our survey inquired about the sophistication of the policy environment in large companies by asking respondents "at what stage is your organization in defining, implementing and enforcing" a wide variety of email, compliance and content security-related policies (18 different types in the 2010 survey).

For each policy type, respondents were asked if they had either a simple written policy (e.g., a note appears in an employee handbook or similar document), a detailed written policy (e.g., a separate policy document), no formal policy or "don't know".

The responses overall and broken out by company size are summarized in Figure 8, which shows the percentage of companies that reported having some sort of formal policy (whether "simple" or "detailed"). The policies themselves are described below in order of highest to lowest overall adoption:

Acceptable use policy for email

A policy that defines appropriate uses for company email systems and may include personal use rules, monitoring and privacy policies, offensive language policies, etc. Overall, 94% of large US companies surveyed reported having formalized an acceptable use policy for email.

Ethics policy

A policy that defines ethical and unethical business practices to be adhered to by employees and executives and may include disclosure rules, conflict of interest rules, communication guidelines, etc. Overall, 92% of US companies reported having a formal ethics policy.

Remote access – mobile computing and storage devices policy

A policy that establishes an authorized method for controlling mobile computing and storage devices that contain or access corporate information resources. Such policies are essential for reducing the risks associated with data loss via Internet-connected mobile devices and removable/portable storage media. Overall, 91% of large US companies reported having formal policy of this type.

Information sensitivity policy or content classification policy

A policy that defines requirements for classifying and securing the organization's information in a manner appropriate to its sensitivity level. Such policies are essential to reducing the risk of leaks of confidential information via email. Overall, 88% of US companies reported having formalized such a policy.

Email policy focused on potential data loss / focused on potential time wasted by employees

One question frequently asked by readers of previous editions of this report was whether organizations are more concerned about the potential for data loss or the potential for employee inefficiency and wasted time with respect to email, the web and social media.

As a way of shedding more light on this issue, the 2010 survey added this policy category along with "email policy focused on potential time wasted by employees" as well as similar categories that relate to Web and social media usage.

For the email category, 86% of companies report having an email policy focused on potential data loss while 80% reported having an email policy focused on potential time wasted by employees, indicating that email policies tend to be more focused on the risk of data loss versus the risk of employee inefficiency.

Email retention policy

A policy that defines what information sent or received by email should be retained (archived) and for how long. In certain highly-regulated industries, email retention is required by law. Overall, 86% of US companies reported having a formal email retention policy.

Web surfing policy focused on potential data loss / focused on potential time wasted by employees

As a way of determining whether companies are more concerned about data loss risks versus time wasted by employees when it comes to use of the Web, the 2010 survey added these two policy categories.

With respect to Web surfing, 83% of companies report having a policy focused on potential data loss while 86% reported having a policy focused on potential time wasted by employees, indicating that Web policies are likely intended to address both risks, with a slight bias toward the issue of employee inefficiency.

Acceptable encryption policy

A policy that defines what types of encryption may be used within the organization and when such techniques can or should be applied. These policies are essential to compliance with regulations, such as the US's HIPAA regulations and a growing number of US state regulations, that include encryption requirements. Overall, 82% of US companies reported having a formal acceptable encryption policy.

Risk assessment policy

A policy that defines requirements and provides authority for the information security team to identify, assess and remediate risks to the organization's information infrastructure. Overall, 82% of US companies reported having a formal risk assessment policy.

Social networking policy

An acceptable use policy that specifically addresses the use of social networking sites (e.g., MySpace, Facebook, etc.). Overall, 81% of US companies reported having a formal acceptable use policy for social networking sites. The 2010 finding is significantly higher than what was reported in 2009, when formal policies for social networking use were reported by just 67% of respondents.

Automatically forwarded email policy

A policy that governs the automatic forwarding of email to external destinations. Overall, 80% of US companies reported having a formal policy for automatically forwarded email.

Social networking policy focused on data loss / focused on potential time wasted by employees

As a way of determining whether companies are more concerned about data loss risks versus time wasted by employees when it comes to use of social networking sites, the 2010 survey added these two policy categories.

With respect to social networking, 80% of companies report having a policy focused on potential data loss while 79% reported having a policy focused on potential time wasted by employees, indicating that social networking policies are likely intended to address both risks, with a slight bias toward the issue of employee inefficiency.

Acceptable use policy for blog and/or message board postings

A policy that defines appropriate uses of internal and external Web log (blog) or message board systems and may include personal use policies, confidentiality rules, monitoring and privacy policies, etc. Overall, 80% of US companies reported having a formal policy for acceptable use of blogs and message boards.

Audit vulnerability scanning policy

A policy that provides authority for the information security team to conduct audits and risk assessments to ensure integrity of information systems, investigate incidents, ensure conformance to security policies, monitor user/system activity, etc. Overall, 79% of US companies reported having a formal audit vulnerability scanning policy.

Media sharing/posting policy

An acceptable use policy that specifically addresses the use of video or audio content sharing sites (e.g., YouTube, Vimeo, etc.) as well as P2P (peer-to-peer) networks and technologies (e.g., BitTorrent, etc.). Overall, 78% of US companies reported having a formal media sharing/posting policy.

Adoption of Outbound Messaging-related Security Policies, Overall and by Company Size, 2010

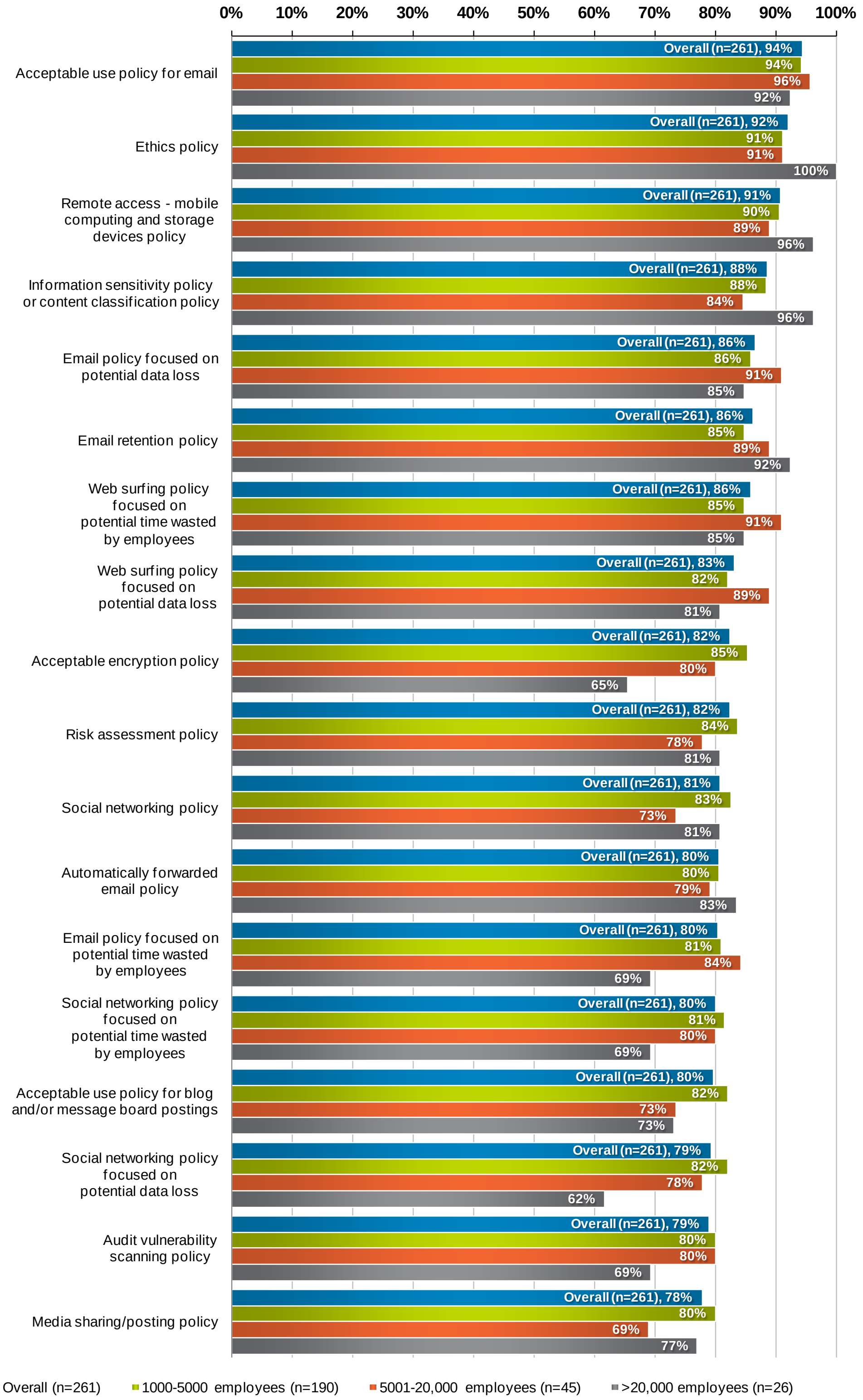

Figure 8: Percentage of companies reporting that they have formalized various security-related policies, by company size.

INVESTIGATIONS OF DATA LOSS INCIDENTS, EMPLOYEE TRAINING AND POLICY ENFORCEMENT ACTIONS

In addition to assessing the level of concern around various conduits for data loss and the state of related policies, survey respondents were asked whether their organization had experienced any of 20 different policy enforcement-related events in the past 12 months.

Respondents were asked about formal training for employees, investigations of data loss events and any employee discipline or termination actions they may have taken. Responses are summarized in Figures 9 through 11 on the following pages.

Formal Email and Web/Social Media Policy Training

Respondents were asked if their company had conducted formal training for employees about its email security policies, training about external regulations that apply to the organization's use of email or training about the organization's Web/social media policies in the past 12 months. The results, overall and broken out by company size category, are summarized in Figure 9, below.

- **Email security policy training:** Overall, more than half (55%) of respondents said their organization had conducted a formal training for employees about their email security policies in the past 12 months. Among the largest companies (those with more than 20,000 employees), such training was less common.
- **Email regulation training:** Overall, 42% of respondents said their organization had conducted a formal training of employees about external regulations that apply to that organization's use of email in the past 12 months. Again, the largest companies were less likely to have conducted such training.
- **Web/social media policy training:** Overall, 31% of respondents said their organization had conducted a formal training for employees about the organization's Web/social media security and acceptable use policies. Companies in the 1000 to 5000 employee range were most likely to conduct such training.

Formal Email and Web/Social Media Policy Training, Overall and by Company Size, 2010

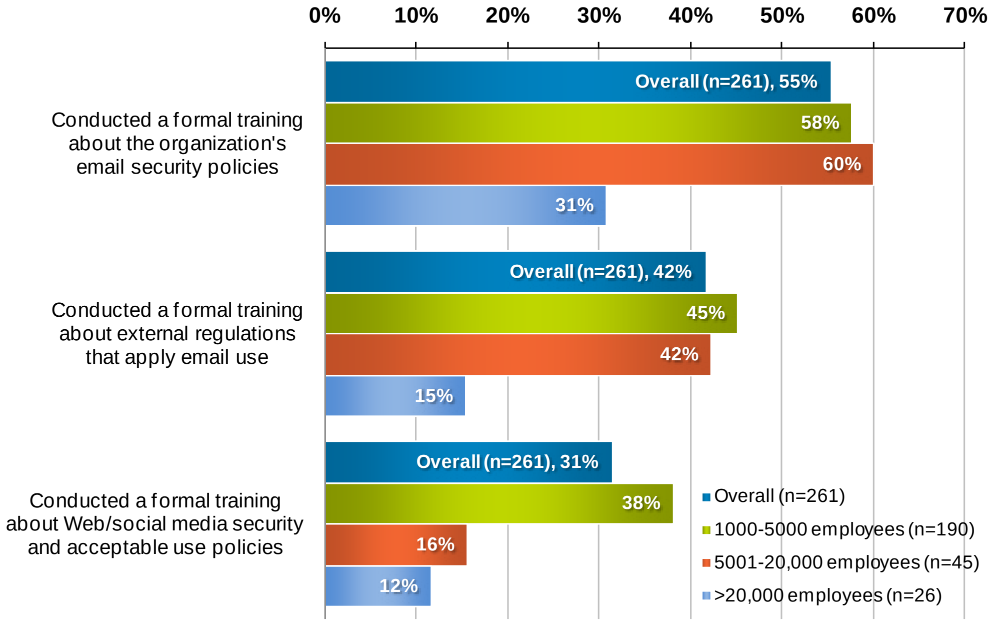

Figure 9: Percentage of companies that reported conducting formal training for employees about that organization's email security, email compliance and Web/social media policies in the past 12 months.

Investigation of Data Leaks and Compliance Violations in the Last 12 Months

As in previous years, our research shows that large organizations are justifiably concerned about the risks associated with outbound email content and other electronic messaging protocols, based on the large number that say they have investigated various types of leaks of confidential information and regulatory compliance violations in the past 12 months.

Key findings are summarized in Figure 10, which shows the percentage of companies that investigated various types of data leaks in the past 12 months. Both overall findings and findings by company size are shown. In general, the larger the organization, the more likely it is that a given type of data loss event or compliance violation was investigated.

Leaks of Confidential Information via Email

Overall, leaks of confidential information via email seem to be down from previous years, but remain the most frequently cited source of data loss events, as can be seen from Figure 10. This year, more than a third (35%) of respondents reported that they investigated a suspected leak of confidential or proprietary information via email (down from 43% in 2009).

Looking at these investigations by company size shows fairly wide variability. More than half of the largest companies (54%) investigated an email-based leak of confidential information, while 44% of organizations with 5001 to 20,000 employees and 30% of organizations with 1000 to 5000 employees report likewise.

Potential Violations of Privacy and Data Protection Regulations via Email

Overall, nearly a third (32%) of large US companies surveyed report that they investigated a suspected violation of privacy or data protection regulations related to email in the past 12 months. This is slightly down from the 2009 finding of 34%.

Leaks of Confidential Information Via Blog or Message Board Postings

Blogs and message board postings continued to be a significant source of risk. Overall, one quarter (25%) of organizations reported that they had investigated the exposure of confidential, sensitive or private information via a blog or message board posting in the past 12 months (up from 18% in 2009).

More than a third (35%) of surveyed companies with more than 20,000 employees reported investigating such a leak.

Leaks of Confidential Info Via Lost or Stolen Mobile Devices or Storage Media

Respondents were asked if they had investigated "the exposure of confidential, sensitive or private information via lost or stolen mobile devices (e.g., laptop, smartphone, mobile email device) or storage media." Lost or stolen devices and storage media have often been the root cause of high-profile data breaches (and, as shown previously, cause IT decision makers a great deal of concern), so it's interesting to compare the risk of this type of "physical" data loss to the risks presented by electronic channels such as email, blogs and social media.

This year's survey found that more than 1 in 5 (22%) of large US organizations investigated the exposure of confidential information via lost or stolen mobile devices or media, essentially unchanged from 2009.

Employee Terminations as a Source of Data Loss Risk

For the second consecutive year, respondents were asked if they had investigated "a suspected leak or theft of confidential or proprietary information associated with an employee leaving the company (e.g., through voluntary or involuntary termination)" in the past 12 months.

Overall, 21% of respondents (up from 18% in 2009) said they investigated such a leak or theft.

Leaks of Confidential Info Via Social Networking Site Postings

Respondents were asked if they had investigated the exposure of confidential, sensitive or private information via a posting to a social networking site (e.g., Facebook, MySpace, LinkedIn, etc.) in the past 12 months. Investigations of data loss events related to social networking sites increased once again over previous years.

Overall, 20% of organizations surveyed reported that they had investigated the exposure of confidential, sensitive or private information via a posting to a social networking site in the past 12 months (up from 17% in 2009 and 12% in 2008).

Leaks of Confidential Info Via Video or Audio Posted to Media Sharing Sites

Respondents were asked if, in the past 12 months, they had investigated the exposure of confidential, sensitive or private information via video or audio posted to a media sharing site. Overall, 18% of respondents to this year's survey reported such an investigation (unchanged from 2009). Companies with 5001 to 20,000 employees were less likely to report such an investigation (just 11%).

Exposure of Material Financial Info Via Blog or Message Board Postings

Respondents were also asked if, in the past 12 months, they had investigated "the exposure of material financial information (such as unannounced quarterly results or significant deals) via a blog or message board posting."

This question is aimed at publicly-traded companies (who are most concerned with protecting "material" financial information). 19% of public companies surveyed (there were 123 of them in this year's sample, or 47% of the total respondents) said that they investigated the exposure of material financial information via a blog or message board posting (up from 15% of public companies in the 2009 survey).

Among non-public companies, 16% (up from 10% in 2009) reported such an investigation. Note that, in Figure 10, the aggregate results for all companies (both public and non-public) are shown.

Leaks of Confidential Info Via Short Message Services (Mobile and Web)

For the second consecutive year, respondents were asked if they had investigated the exposure of confidential, sensitive or private information via short message service (e.g., SMS, MMS or Web-based short message systems such as Twitter) in the past 12 months.

Overall, 17% of organizations reported such an investigation (up from 13% in 2009).

Investigations of Potential Data Leaks and Compliance Violations, Overall and by Company Size, 2010

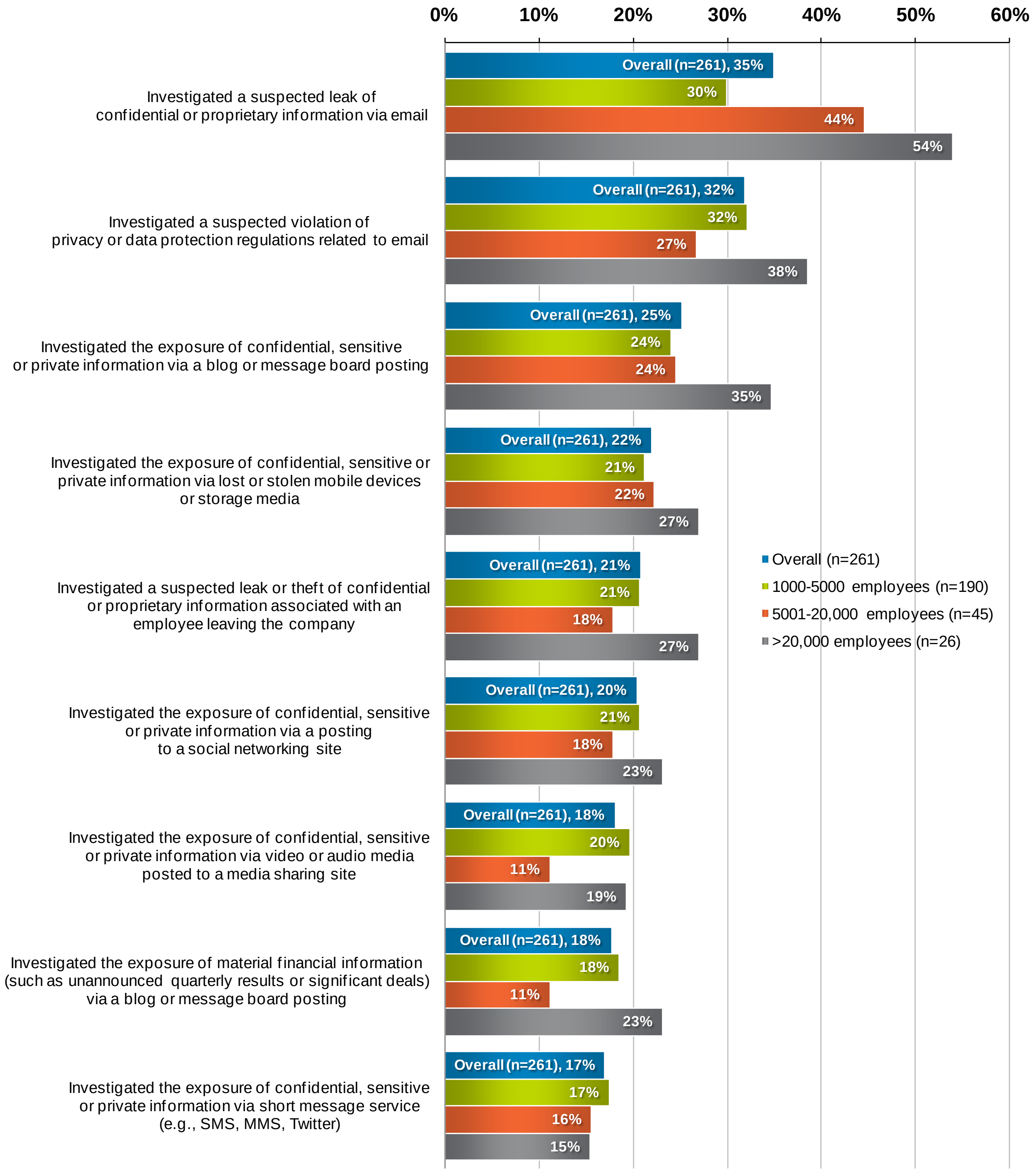

Figure 10: Percentage of large US companies reporting that they investigated various types of data loss events in the past 12 months.

Disciplinary Actions Taken Against Employees for Policy Violations in the Past 12 Months

As in past years, the 2010 survey asked respondents about various disciplinary actions, including termination, that they took against employees for violations of various messaging-related policies in the past 12 months. The key findings are summarized in Figure 11.

In previous years, findings had shown that, in general, larger organizations were more likely to take some form of disciplinary action. Findings from this year do not show that trend (in fact, 2010 results showed that smaller organizations were somewhat more likely to take disciplinary actions for web and social media-related policy violations).

Discipline and Termination of Employees for Violating Email Policies

Violations of email policies continue to be the most common source of messaging-related discipline and termination actions covered in this survey.

This year, we found that half (50%, slightly down form 52% in 2009) of companies surveyed had disciplined an employee for violating email policies in the past 12 months. These results have stayed roughly constant for several years (e.g., in 2008, 51% US companies reported this type of disciplinary action; in 2007 the finding was 52%).

Terminations for violations of email policies were less frequent this year. Overall, 20% of companies reported that they terminated an employee for violating email policies in the past 12 months (down from 32% in 2009 and 26% in 2008).

Discipline and Termination of Employees for Violating Blog and Message Board Policies

Respondents were asked if employees had been disciplined or terminated for violating the company's blog or message board policies in the past 12 months. Overall, 24% (up from 17% in 2009) of companies surveyed said they had disciplined an employee for blog or message board policy violations in the past 12 months.

Terminations were less frequent, with 11% (up from 9% in 2009) of companies reporting that they had terminated an employee for violating blog or message board policies in the past 12 months.

Discipline and Termination of Employees for Violating Media Sharing/Posting Policies

Respondents were asked if their companies had disciplined or terminated an employee for violating the company's media sharing/posting policy in the past 12 months. Overall, 21% of companies (up from 15% in 2009) reported disciplining an employee for violating media sharing/posting policies. 9% of companies (up from 8% in 2009) reported terminating an employee for this sort of violation.

Discipline and Termination of Employees for Violating Social Networking Policies

Respondents were asked if their companies had disciplined or terminated an employee for violating the company's social networking policy in the past 12 months. Overall, 20% of companies reported having disciplined an employee for violating social media policies, double the 2009 finding of 10%.

Terminations for violations of social networking policies did not increase by the same amount, however, with just 7% (down from 8% in 2009) of companies reporting that they took such actions in the past 12 months.

Discipline and Termination Actions Taken by Companies, Overall and by Company Size, 2010

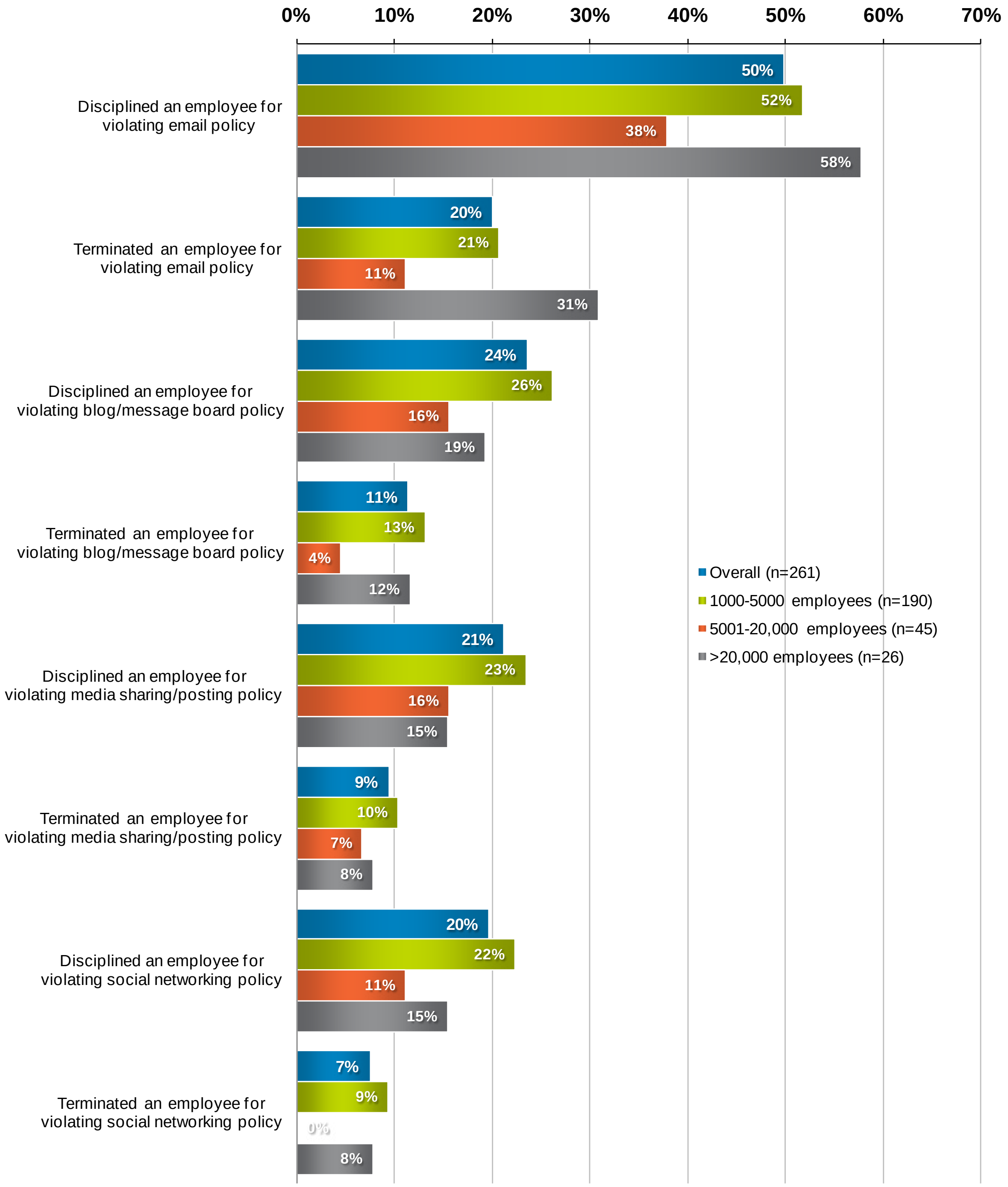

Figure 11: Percentage of respondents who reported various types of disciplinary actions against employees for messaging-related policy violations in the past 12 months.

EXPOSURE, THEFT AND DISCOVERY OF SENSITIVE INFORMATION

In addition to the questions about *investigations* of various types of content security breaches, respondents were asked if their business had been impacted by the *improper exposure or theft* of different types of information including customer information, intellectual property and other "sensitive or embarrassing" information in the past 12 months.

Organizations were also asked if they were ordered to produce employee email or other electronic content in response to an order by a court or other regulatory body.

Findings are summarized in Figure 12.

Exposure of Sensitive or Embarrassing Information

Overall, more than a third (36%, slightly up from 34% in 2009) of companies surveyed reported that their business had been impacted by the exposure of sensitive or embarrassing information in the past 12 months. The largest organizations were more likely to say that they were impacted in this way (47%).

Improper Exposure or Theft of Customer Information

Nearly a third (31%, slightly down from 33% in 2009) of companies reported that they had been impacted by improper exposure or theft of customer information in the past 12 months. The largest companies were less likely to report being impacted in this way (13%).

Improper Exposure or Theft of Intellectual Property

Overall, 29% (slightly up from 27% in 2009) of companies reported that they had been impacted by improper exposure or theft of intellectual property in the past 12 months.

Litigation Concerns: Subpoenas of Employee Email and Other Electronic Content

Exposure of confidential information can also occur when, in the course of civil or criminal investigations, a company's email messages and other electronic content are subpoenaed. Respondents were asked if, in the past 12 months, their organization had "been ordered by a court or regulatory body to produce employee email (i.e., has employee email been subpoenaed?)." They were also asked if they had been ordered to produce other electronic content.

Overall, 1 in 5 (20%, down from 24% in 2009) of companies reported having to produce employee email in the past year. Larger companies were more likely to be subject to this type of discovery event (e.g., 54% of companies with more than 20,000 employees reported doing so as can be seen in Figure 12).

Email is not the only form of content that is subject to electronic discovery requests, of course. Overall, 16% of companies reported that they were ordered to produce other types of electronic content in the past 12 months. Again, larger companies were subject to this type of discovery event more frequently (50% of companies with more than 20,000 employees reported doing so). This is the first year that survey respondents were asked about discovery requests for non-email electronic content.

Exposure or Theft of Sensitive Information, Overall and by Company Size, 2010

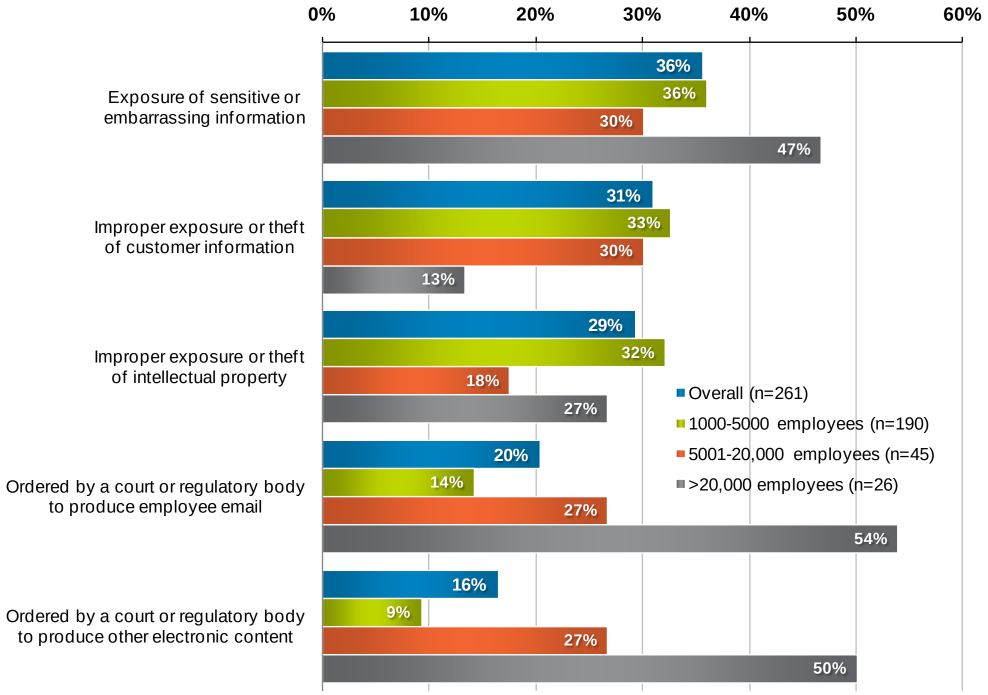

Figure 12: Percent of respondents who reported that their organization had been impacted by theft or exposure of various types of sensitive information in the past 12 months.

IMPORTANCE OF REDUCING THE RISKS ASSOCIATED WITH OUTBOUND EMAIL

As in previous years, the survey attempted to assess organizations' level of urgency around reducing the risks associated with outbound email. To assess this level of urgency, survey respondents were asked, "How important to your organization is reducing the legal and financial risks associated with outbound email in the next 12 months?"

Overall, 70% of respondents (up from 62% in 2009) said that it is "important" or "very important" for their organizations to reduce the legal and financial risks associated with outbound email in the next 12 months.

Note that just 10% of respondents feel that this issue is "somewhat unimportant" or "very unimportant."

The responses, also broken out by company size, are summarized in Figure 13, below.

Importance of Reducing Risks Associated with Outbound Email, Overall and by Company Size, 2010

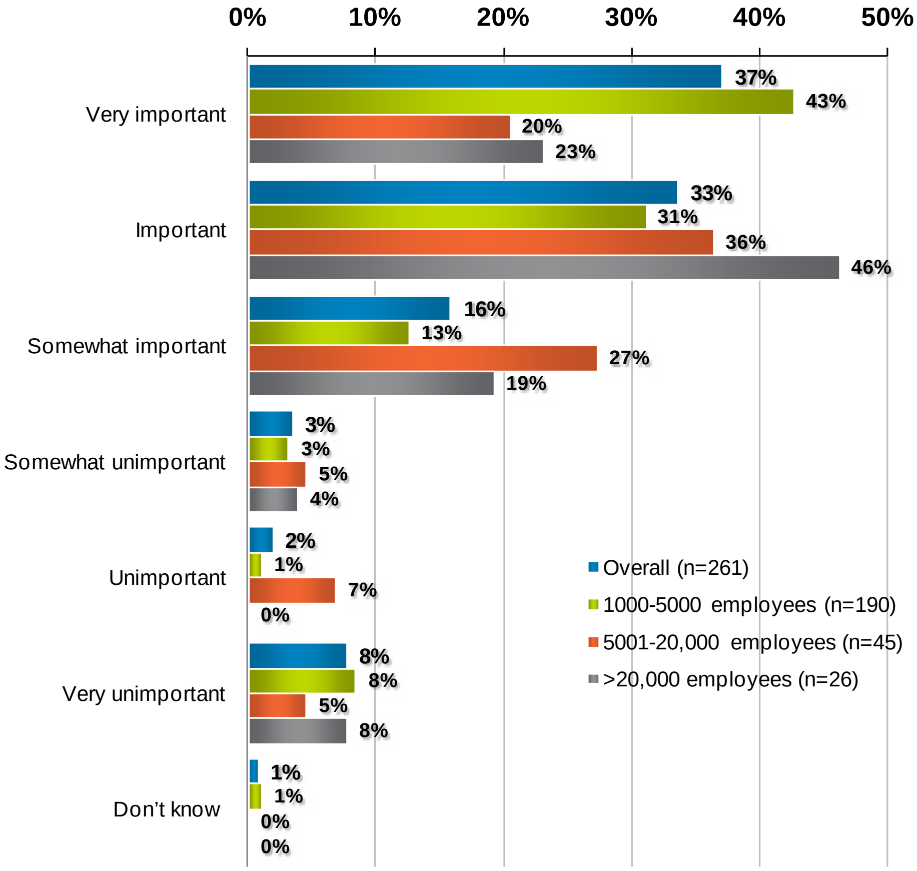

Figure 13: Importance of reducing the legal and financial risks associated with outbound email in the next 12 months.

IMPORTANCE OF REDUCING OUTBOUND HTTP CONTENT RISKS

Organizations were also asked about their urgency around reducing the risks associated with outbound HTTP transmissions. To assess this level of urgency, survey respondents were asked, "How important to your organization is reducing the legal and financial risks associated with outbound HTTP traffic (e.g., webmail, blog postings) in the next 12 months?"

Overall, 67% of respondents (up from 56% in 2009) said that it is "important" or "very important" for their organizations to reduce the legal and financial risks associated with outbound HTTP traffic in the next 12 months.

Note that only 8% of respondents feel that this issue is "somewhat unimportant" or "very unimportant."

The responses, also broken out by company size, are summarized in Figure 14, below.

Importance of Reducing Risks Associated with Outbound HTTP Content, Overall and by Company Size, 2010

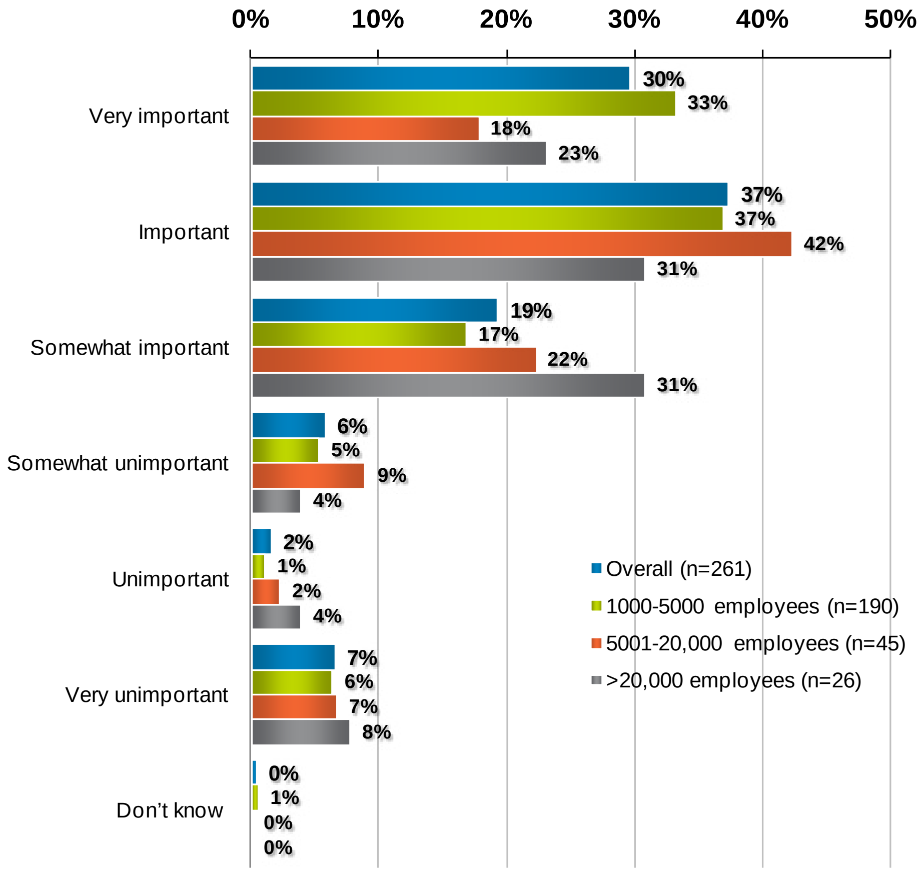

Figure 14: Importance of reducing the legal and financial risks associated with outbound HTTP content (e.g., webmail, blog and message board postings, etc.) in the next 12 months.

ECONOMIC CONSIDERATIONS: BUDGET, LAYOFFS AND DATA SECURITY

As part of our continuing look at how the ongoing economic recession is affecting data security in large enterprises, we once again asked respondents to assess their agreement with several statements about the impact of budget constraints, layoffs of IT staff and layoffs in general on the state of their organization's ability to protect sensitive data.

The 2010 findings show that IT decision makers are still feeling the pinch of budget constraints and an increasing number feel that staff reductions and layoffs in the past 12 months have negatively impacted their organizations' ability to protect confidential, proprietary and sensitive data. Responses to this question are summarized in Figure 15, below.

Respondents were asked, "How would you assess the following statements as they apply to your organization's messaging security policies, practices and technology deployments?" Topics were as follows:

- "Budget constraints have negatively impacted my organization's ability to protect confidential, proprietary or sensitive information in the past 12 months." Overall, more than half of respondents (58%, up from 50% in 2009).
- "Reductions in the size of our IT staff due to layoffs have negatively impacted my organization's ability to protect confidential, proprietary or sensitive information in the past 12 months." Overall, 53% (up from 47% in 2009) of respondents agreed or strongly agreed with this statement.
- "An increasing number of layoffs at my organization in the past 12 months has created an increased risk of data leakage." Overall, 48% (up from 42% in 2009) of respondents agreed or strongly agreed with this statement.

Budget and Economic Trends Issues, Overall and by Company Size, 2010

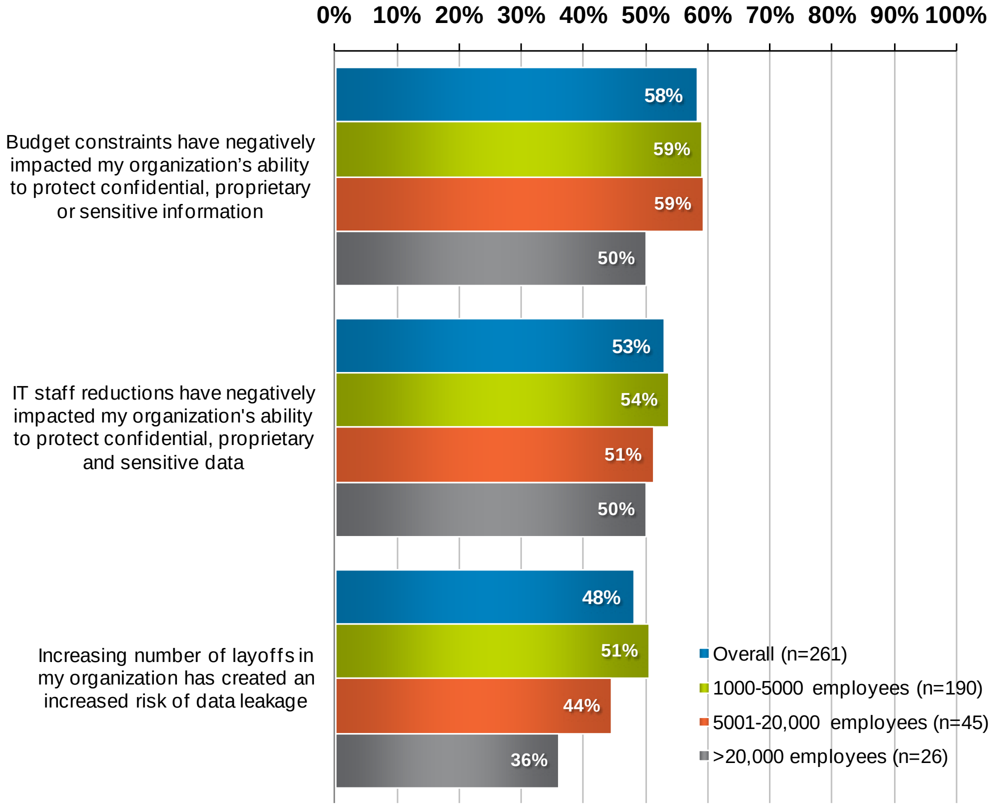

Figure 15: Percentage of respondents that "agree" or "strongly agree" with various statements about the data security impact of budget constraints and employee layoffs in their organizations.

PERCEIVED DATA LOSS RISKS ABOUT SAAS AND CLOUD COMPUTING

One way that enterprises are dealing with contracting IT budgets is to move more functions—including security functions such as email security and data loss prevention—to a SaaS (Software-as-a-Service) or cloud computing model. As a result, more confidential, private and proprietary data is stored outside the enterprise, potentially posing new security concerns for IT professionals.

As we first did in 2009, our 2010 survey asked respondents if they felt that the increasing use of SaaS and cloud computing technologies is perceived as a source of data loss risks.

As part of the trend questions described in the previous section (see Figure 15), respondents were also asked to assess the statement:

- "The trend toward using SaaS and cloud computing solutions in the enterprise seriously increases the risk of data leakage." As Proofpoint has seen in other research, IT decision makers are still fairly evenly split on whether SaaS and cloud computing increase data loss risks. Overall, 49% (up from 41% in 2009) of respondents agreed or strongly agreed with this statement.

Affirmative responses to this statement, overall and by company size, are shown in Figure 16, below.

Despite these concerns, respondents continue to embrace SaaS technology and significant numbers of them intend to use SaaS solutions for various email security and compliance functions. The 2010 survey asked about adoption and deployment plans for SaaS-based security and compliance solutions. A few of the findings included:

- While the vast majority of responding organizations (98%) have an on-premises messaging system (e.g., mail server such as Microsoft Exchange, Lotus Notes/Domino or Novell GroupWise), 31% of responding companies have a SaaS/hosted email system (typically in addition to the on-premises system). 20% of respondents say they "will definitely" deploy SaaS mailbox hosting in the future and an additional 18% indicate that they "might" do so.
- More than half of respondents (52%) say that they have already deployed a SaaS solution for inbound email scanning for spam and viruses. An additional 17% say they "will definitely" deploy such technology in the future and another 14% say they "might."
- 31% of respondents say they have already deployed a SaaS solution for outbound scanning of content for data loss prevention or compliance. An 19% say they "will definitely" deploy such technology in the future and another 17% say they "might."

Perception of Data Loss Risks Associated with SaaS and Cloud Computing, Overall and by Company Size, 2010

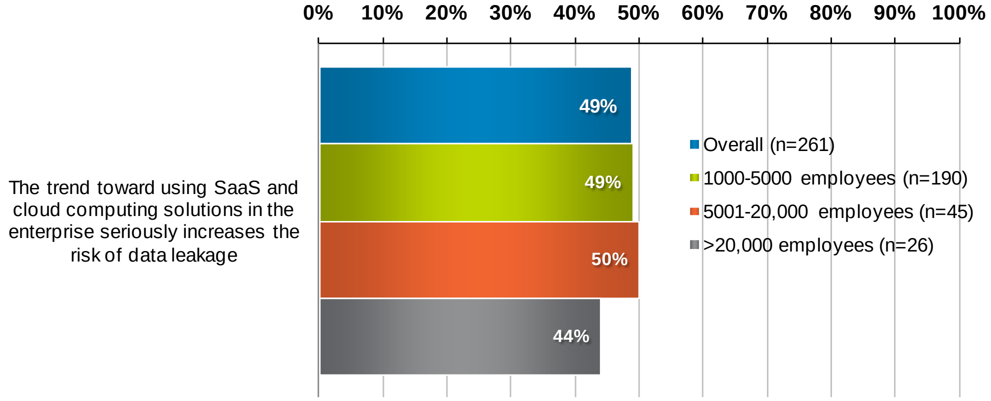

Figure 16: Percentage of companies that "agree" or "strongly agree" with the statement that SaaS and cloud computing solutions in the enterprise increase the risk of data leakage.

IMPORTANCE OF INVESTMENT IN VARIOUS EMAIL SECURITY AND COMPLIANCE AREAS

Because enterprise IT budgets are finite, IT professionals must always prioritize their spending when addressing the multitude of security risks they face. To assess the relative importance of investing in inbound email filtering, outbound email filtering/email data loss prevention and email archiving/eDiscovery, respondents were asked, "On a scale of 1 to 5, how important will the following areas of investment be for your company over the next 12 months, where 1 is 'not important/low priority' and 5 is 'very important/ high priority'?"

Figure 18, below, shows the relative importance that respondents gave to six different email security and compliance investment areas. While inbound threat protection (e.g., improving malware detection and improving spam filtering) were most likely to be rated as "Very High" priorities, looking at both "Very High" and "High" priority categories shows that improving eDiscovery for email and improving the ability to prevent sensitive content form leaving via email are seen as equally important investment areas.

Relative Priority of Investment in Various Messaging Security Areas, 2010

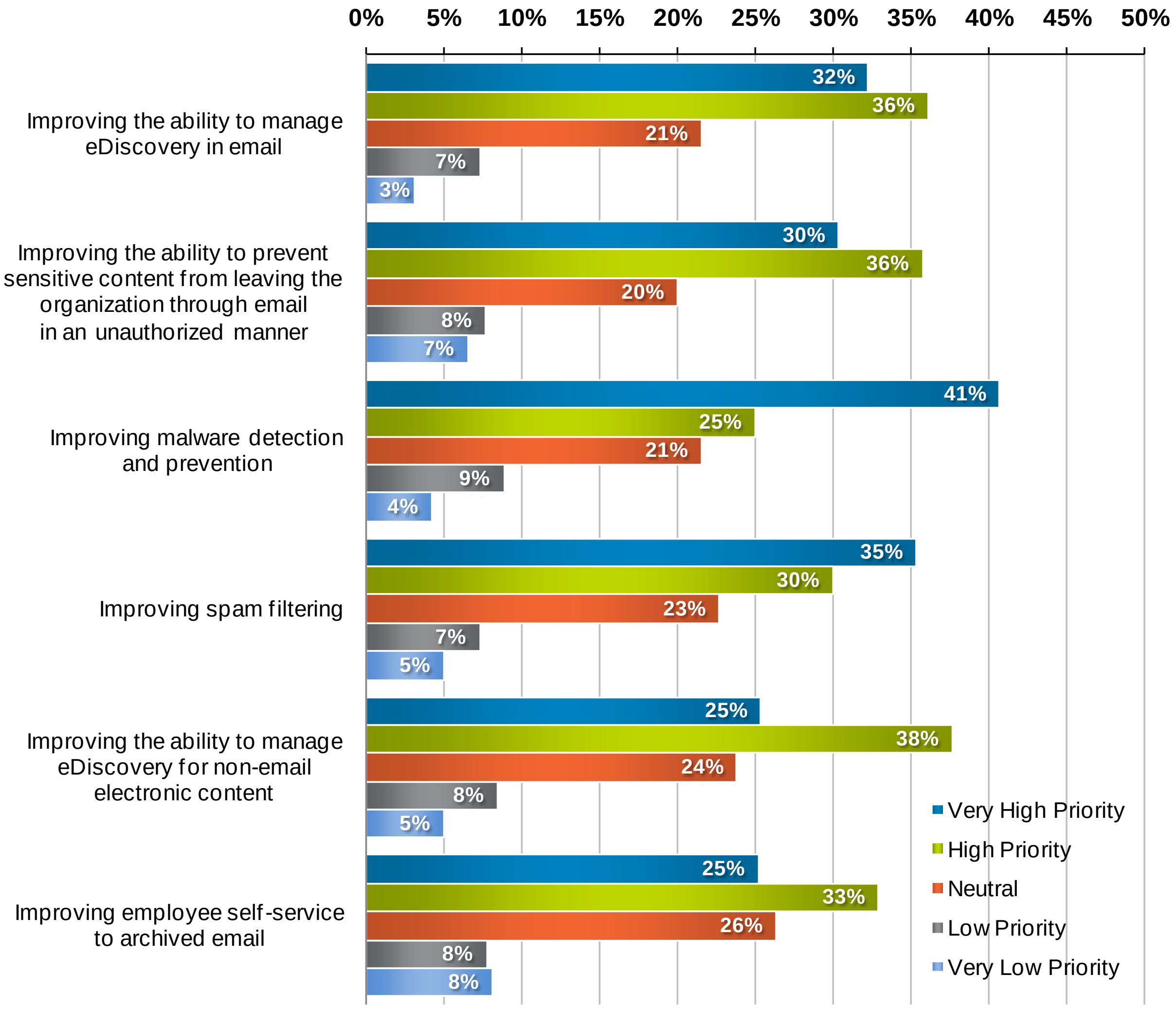

Figure 18: Percentage of respondents who rated investment in various messaging security areas as a "priority" or "high priority" over the next 12 months.

APPENDIX: RESPONDENT DEMOGRAPHICS

Respondent Titles

The 261 US respondents to this survey represented a wide variety of IT decision makers including respondents with the following titles:

Title	Percent of Respondents
CIO, CTO, or senior-most IT executive	20.7%
CSO, CISO, or senior-most IT security executive	2.3%
VP or executive of IT	5.7%
VP or executive of security	1.5
Director or manager of IT	46.4%
Director or manager of security	2.7%
CFO, CEO, COO	3.1%
Compliance or legal officer, or counsel	0.4%
Senior finance executive	2.7%
Senior human resource executive	2.7%
Director or manager of messaging/email systems	11.9%

Respondent Company Sizes and Ownership

The size of the surveyed organizations (based on number of employees) and ownership type was reported as follows:

Size Category	Percent of Respondents
1,000 to 5,000 employees	72.8%
5,001 to 20,000 employees	17.2%
More than 20,000 employees	10.0%

Ownership	Percent of Respondents
Publicly traded	46.7%
Privately held	53.7%

Respondent Company Industries

Responding companies, represented a wide variety of industries, reported as follows:

Industry Group / Specialty	Percent of Respondents
MANUFACTURING	
Primary production and raw materials manufacturing	8.8%
Consumer products manufacturing	6.6%
Chemical and petroleum manufacturing	3.5%
Pharmaceutical/biotech manufacturing	4.8%
High-tech products manufacturing (software, computer components, etc.)	8.3%
Industrial products manufacturing	7.0%
RETAIL/WHOLESALE	
Retail	8.8%
Wholesale	6.1%
BUSINESS SERVICES	
Transportation and logistics	9.6%
Professional services (consulting, legal, etc.)	10.1%
Construction and engineering	5.7%
Media, entertainment, and leisure	1.3%
UTILITIES/TELECOM	
Utilities	0.0%
Telecom carriers	0.9%
FINANCE/INSURANCE	
Financial services	5.7%
Insurance	2.2%
PUBLIC SECTOR	
Government	3.9%
Higher education	4.4%
Healthcare	2.2%
Non-profit/other public services	0.0%

ABOUT THIS REPORT AND PROOFPOINT, INC.

This report has been created and developed solely by Proofpoint, Inc.

Proofpoint focuses exclusively on the art and science of cloud-based email security, eDiscovery and compliance solutions. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against spam and viruses, safeguard privacy, encrypt sensitive information, and archive messages for easier management and discovery. Proofpoint's enterprise email solutions mitigate the challenges and amplify the benefits of enterprise messaging.

FOR FURTHER READING

Proofpoint offers a variety of free educational whitepapers that further describe the risks associated with outbound email and the policies, processes and technologies that can be used to reduce those risks.

Previous Outbound Email and Data Loss Prevention Research Reports

Previous editions of this report can be downloaded by visiting the following URLs:

http://www.proofpoint.com/outbound2009

http://www.proofpoint.com/outbound2008

http://www.proofpoint.com/outbound2007

http://www.proofpoint.com/outbound2006

http://www.proofpoint.com/outbound2005

http://www.proofpoint.com/outbound2004

Email Encryption Whitepapers

Download two whitepapers, Proofpoint's *Protecting Enterprise Data with Proofpoint Encryption* and Osterman Research's *The Critical Need for Encrypted Email and Secure File Transfer Solutions* to learn more about the issues around encryption of both email and file transfer systems, some of the regulatory statutes that require sensitive content to be encrypted and suggestions for how to move forward with the deployment of policy-based encryption systems. Please visit:

http://www.proofpoint.com/id/email-encryption-wp/index.php

Email Archiving: A Proactive Approach to eDiscovery

This whitepaper addresses the key eDiscovery challenges facing legal and IT departments today, including the impact of regulations such as the Federal Rules of Civil Procedure (FRCP) and how email archiving technology can help your organization be better prepared. Please visit:

http://www.proofpoint.com/id/email-archiving/index.php

Gartner Magic Quadrant for Secure Email Gateways, 2010

Gartner, Inc. positions Proofpoint in the Leaders quadrant in its *2010 Magic Quadrant for Secure Email Gateways*. In this report, Gartner analysts note that, "The e-mail security market is very mature. Targeted phishing detection, outbound e-mail inspection, encryption and delivery form factor are the major differentiators." To read a copy of the full report, compliments of Proofpoint, Inc., please visit:

http://www.proofpoint.com/magicquadrant

Leveraging SaaS Technology to Reduce Costs

These whitepapers from Proofpoint and Osterman Research discuss how Software-as-a-Service solutions for email security and email archiving can greatly reduce costs—without sacrificing the security of your organization's most valuable data. Please visit:

Using SaaS to Reduce the Costs of Email Security

http://www.proofpoint.com/id/saas-email-security-costs-whitepaper/index.php

Email Archiving: Realizing the Cost Savings and Other Benefits from SaaS

http://www.proofpoint.com/id/saas-email-archiving-costs-whitepaper/index.php

Connect with Us on Social Media

For more information on email security, compliance, archiving, eDiscovery and data loss prevention issues, connect with us on the following social media channels:

Proofpoint Email Security Blog

http://blog.proofpoint.com

Follow Us on Twitter

@Proofpoint_Inc

http://www.proofpoint.com/twitter

Facebook

http://www.proofpoint.com/facebook

Proofpoint Video Channel

http://www.proofpoint.com/youtube

US Worldwide Headquarters
Proofpoint, Inc.
892 Ross Drive
Sunnyvale, CA 94089
United States
Tel +1 408 517 4710

US Utah Satellite Office
Proofpoint, Inc.
13997 South
Minuteman Drive,
Suite 320
Draper, UT 84020
United States
Tel +1 801 748 4610

Asia Pacific
Proofpoint APAC
Suntec Tower 2,
9 Temasek Boulevard,
31F
Singapore 038989
Tel +65 6559 6128

EMEA
Proofpoint, Ltd.
200 Brook Drive
Green Park
Reading, UK
RG2 6UB
Tel +44 (0) 870 803 0704

Japan
Proofpoint Japan K.K.
BUREX Kojimachi
Kojimachi 3-5-2,
Chiyoda-ku
Tokyo, 102-0083
Japan
Tel +81 3 5210 3611

Canada
Proofpoint Canada
210 King Street East,
Suite 300
Toronto, Ontario,
M5A 1J7
Canada
Tel +1 647 436 1036

Mexico
Proofpoint Mexico
Salaverry 1199
Col. Zacatenco
CP 07360
México D.F.
Tel: +52 55 5905 5306

Proofpoint focuses exclusively on the art and science of cloud-based email security, eDiscovery and compliance solutions. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against spam and viruses, safeguard privacy, encrypt sensitive information, and archive messages for easier management and discovery. Proofpoint's enterprise email solutions mitigate the challenges and amplify the benefits of enterprise messaging.

proofpoint™

www.proofpoint.com