

Outbound Email and Data Loss Prevention in Today's Enterprise, 2009



Results from Proofpoint's sixth annual survey on outbound messaging and content security issues, fielded by Osterman Research, July, 2009 ➤

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 220 responses from companies with 1,000 or more employees in June 2009. 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

- The Bottom Line: Key Findings, US 2009i**
- Overview.....1**
 - About the Study1
- Concerns about Outbound Email Compliance and Content Security.....2**
 - Top Outbound Email Concerns2
- How Risky is Outbound Email Content?3**
 - Most Common Forms of Inappropriate Content in Outbound Email4
 - As Many as 1 in 5 Outbound Emails May Pose a Risk4
- How Do Companies Reduce Outbound Email Risks Today?5**
 - They’re (Still) Reading Employee Email—More than Ever?5
 - Adoption of Technology Solutions for Mitigating Outbound Messaging Risks.....7
- Other Conduits for Exposure of Confidential Information.....7**
- The Messaging Policy Environment in Today’s Enterprise.....11**
- Investigations of Data Loss Incidents, Employee Training and Policy Enforcement Actions.....14**
 - Formal Email Policy Training14
 - Investigation of Data Leaks and Compliance Violations in the Last 12 Months15
 - Disciplinary Actions Taken Against Employees for Policy Violations in the Past 12 Months.....18
- Exposure and Theft of Sensitive Information20**
- Importance of Reducing the Risks Associated with Outbound Email21**
- Importance of Reducing Outbound HTTP Content Risks22**
- Economic Considerations: Budget, Layoffs and Data Security23**
- SaaS and Cloud Computing as Sources of Cost Savings and Data Loss Risk24**
- Importance of Investment in Various Email Security and Compliance Areas25**
- Appendix: Respondent Demographics.....26**
 - Respondent Titles26
 - Respondent Company Industries.....27
- About this Report28**
- For Further Reading28**
- About Proofpoint, Inc.29**

The Bottom Line: Key Findings, US 2009

Selected “Fast Facts” from Proofpoint’s forthcoming *Outbound Email and Data Loss Prevention in Today’s Enterprise* report, based on a June 2009 study of 220 email decision makers at US enterprises with more than 1000 employees:

Who’s Reading Your Corporate Email?

- **48% of US companies with 20,000 or more employees surveyed employ staff to read or otherwise analyze outbound email.** Overall, more than one third (38%) of US companies surveyed say they employ such staff. Additionally, **46% of US 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.
- **Nearly a quarter (24%) of companies surveyed said that employee email was subpoenaed in the past 12 months.**

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

- **More than one third (34%) of US companies surveyed say their business was impacted by the exposure of sensitive or embarrassing information in the last 12 months.** One third (33%) said they had been impacted by improper exposure or theft of customer information. 28% said they had been impacted by the improper exposure or theft of intellectual property.
- **43% of US companies investigated a suspected email leak of confidential or proprietary information in the past 12 months.** 34% 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.** 51% of respondents are highly concerned about the risk of information leakage via email sent from mobile devices.

How Often are Employees Fired for Email Misuse?

- **Nearly a third of US companies surveyed (31%) terminated an employee for violating email policies in the past 12 months.** More than half (51%) of US companies surveyed disciplined an employee for violating email policies in the past 12 months.

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

- **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).** 15% have disciplined an employee for violating media sharing/posting policies in the past 12 months. 8% reported terminating an employee for such a violation. 42% are highly concerned about the risk of information leakage via media sharing sites.
- **17% of US companies investigated the exposure of confidential, sensitive or private information via a posting to a social networking site (e.g., Facebook, LinkedIn).** 10% have disciplined an employee for violating social networking policies in the past 12 months. 8% reported terminating an employee for such a violation. 45% are highly concerned about the risk of information leakage via posts to social networking sites.
- **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).** 41% are highly concerned about the risk of information leakage via Web-based short messaging (e.g., Twitter).
- **18% of US companies surveyed investigated the exposure of confidential, sensitive or private information via a blog or message board posting.** 17% disciplined an employee for violating blog or message board policies in the past 12 months. 9% reported terminating an employee for such a violation. 46% are highly concerned about the risk of information leakage via blogs and message board postings.

Is the Recession Increasing the Risk of Data Loss?

- **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.**
- **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.**
- **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.**

The latest version of this report is always available at <http://www.proofpoint.com/outbound>

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 regulations. In addition, organizations remain very concerned about ensuring that email (and other electronic message streams) cannot be used to disseminate confidential or proprietary information.

This report summarizes the findings of Proofpoint's sixth 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 monitoring, data protection and information leaks.

As in previous years, data protection continues to be a hot topic—in the mainstream and IT press, legislative arenas and IT professional circles—as large-scale breaches of personal information continue to come to light and as the regulatory environment becomes more sophisticated.

At the same time, data protection, monitoring, filtering and encryption technologies continue to advance. The continuing proliferation and growing popularity of electronic communication channels (such as webmail, blogs, social networking sites, media sharing sites and instant messaging) pose new sources of risk for IT security professionals and the organizations they serve.

This year's (2009) survey also looked at two topical areas of concern:

Has the global economic recession affected data security? As the economic environment continues to be turbulent in the US and around the world, we were curious to know if IT decision makers felt that declining budgets were negatively impacting their organizations' ability to protect confidential data and whether increasing numbers of layoffs have, themselves, posed a serious risk of data leakage.

Does the increasing popularity of Software-as-a-Service (SaaS) and cloud-computing technologies pose an increased risk of data leakage? And are the cost benefits perceived as outweighing security concerns? 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 an on-demand (SaaS) model. As a result, more confidential, private and proprietary data is stored outside the enterprise, posing new security concerns for IT professionals.

About the Study

This report summarizes findings from Proofpoint's sixth annual study of outbound email security 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. For 2009, Proofpoint added questions related to security concerns around SaaS/cloud computing, declining budgets and employee layoffs.

For the 2009 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 the content of email leaving their organizations. During June 2009, Osterman gathered responses from enterprises with 1,000 or more employees. In total, 220 valid responses were received, comprised of 75 companies with 1000-5000 employees, 85 with 5001-20,000 employees and 60 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.

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 50% of all respondents reported being

“concerned” or “very concerned.” In general, the larger the organization, the more concern was expressed about each issue.

Protecting personal identity/financial privacy information was the area of greatest concern, with 66.3% of US respondents reporting that they are “concerned” or “very concerned.” Ensuring that email cannot be used to disseminate confidential internal memos was the second most important issue, with 63.3% expressing a high level of concern. Ensuring that email cannot be used to disseminate company trade secrets or valuable intellectual property was the third most important issue, with 62.1% of respondents expressing a high level of concern.

See Figure 1, below, for the relative rankings of each area of concern, including a comparison by company size.

Outbound Email Concerns: Overall and by Company Size, 2009

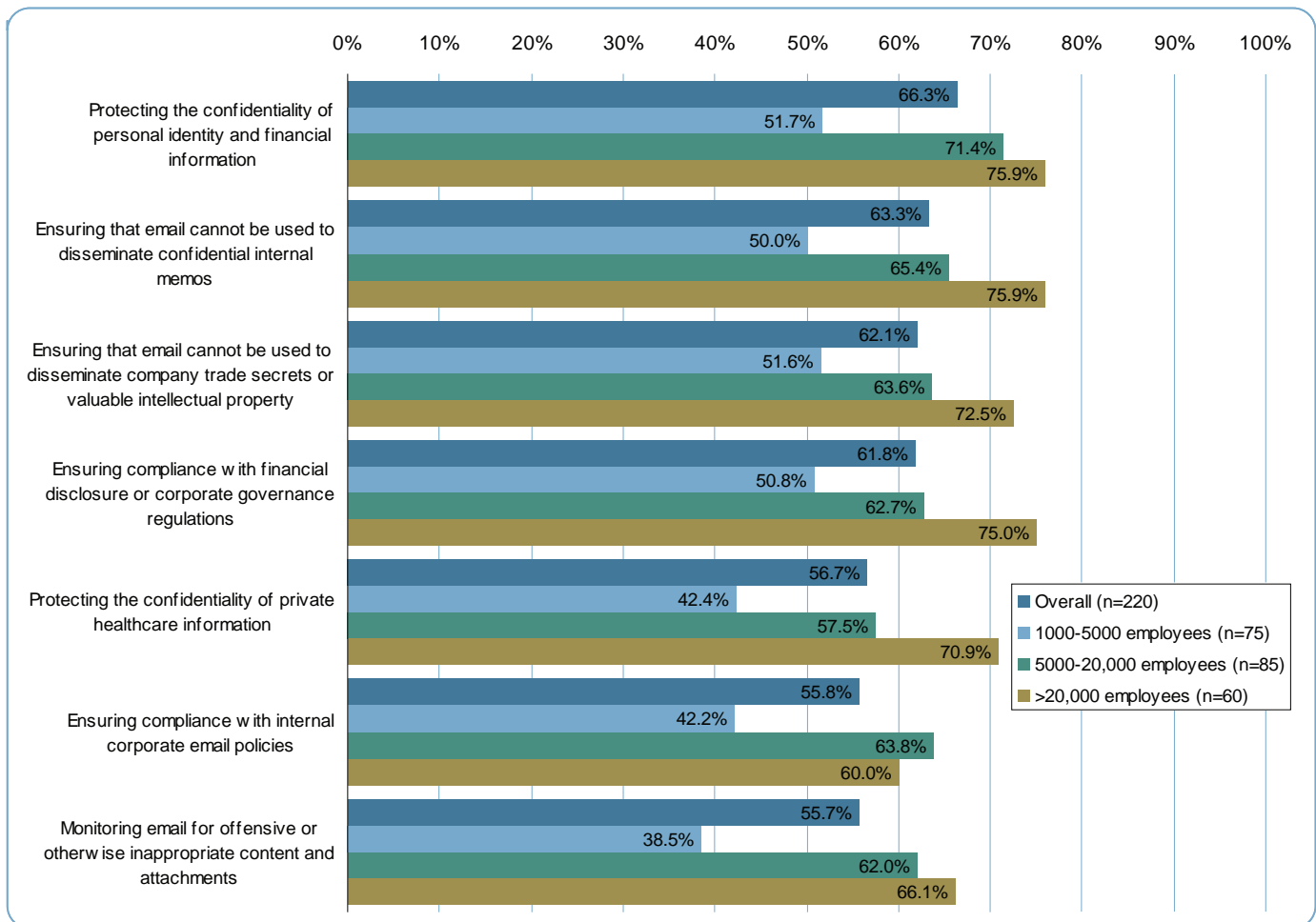


Figure 1: Percentage of respondents who reported being “very concerned” or “concerned” about various outbound email security issues.

How Risky is Outbound Email Content?

As a way of estimating the magnitude of the problem posed by non-compliant email messages in today’s enterprise, respondents were asked two questions. First, they were asked how common it is for various forms of inappropriate content to be found in outbound email. Second, they were 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?’” This is slightly different from previous years’ surveys where respondents were asked to pick one category as the “most common” form of inappropriate content leaving their organizations.

Figure 2, below, charts the distribution of answers for four different types of inappropriate content in outbound email:

- **Valuable intellectual property or trade secrets** which should not leave the organization. 27.4% of respondents say this type of content is “common” or “very common.”
- **Adult, obscene or potentially offensive content.** 23.3% of respondents say this type of content is “common” or “very common.”
- **Confidential or proprietary business information** about your organization. 24.7% of respondents say this type of content is “common” or “very common.”
- **Personal healthcare, financial or identity data** which may violate privacy and data protection regulations. 26.5% of respondents say this type of content is “common” or “very common.”

Most Common Forms of Inappropriate Outbound Email Content, 2009

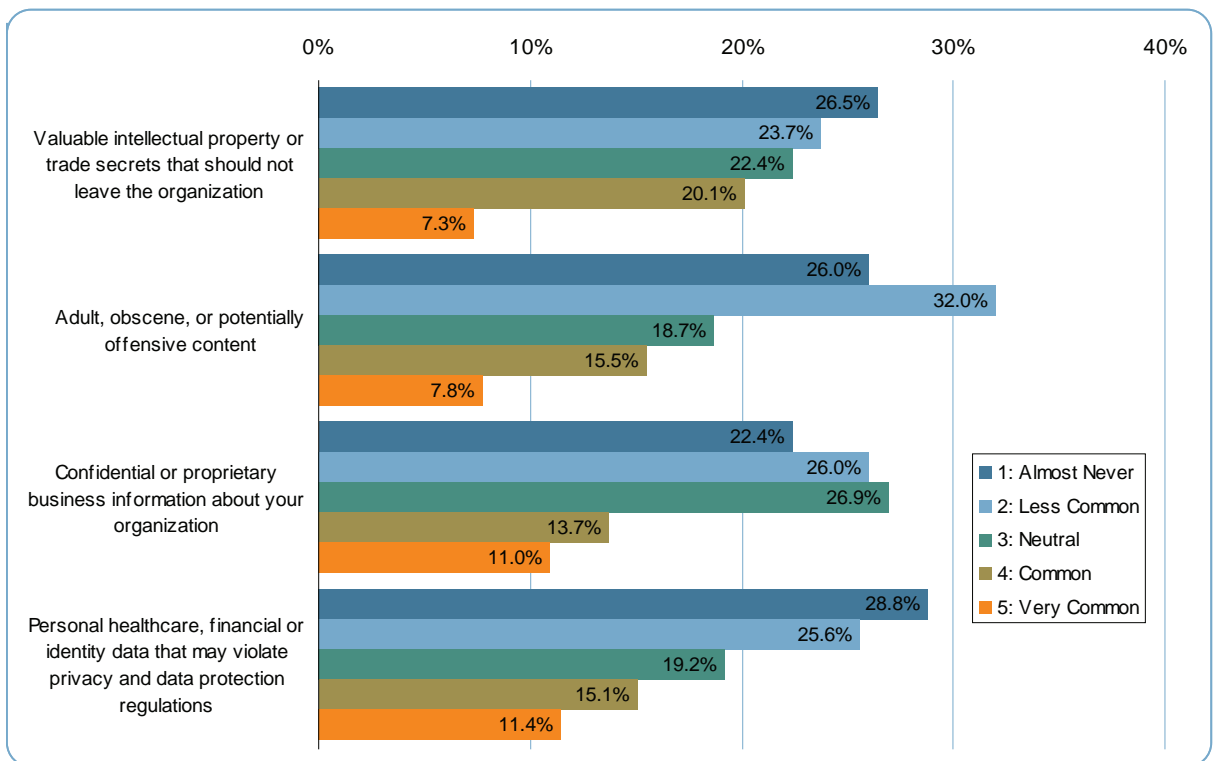


Figure 2: Four different categories of inappropriate content. Respondents rated how common it is to find each type of content in email leaving their own organizations.

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 (182 respondents) was that nearly 1 in 5 (19.6%) of outbound email poses a risk.

Not all survey respondents provided an estimate in answer to this question, with 17.6% 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%).

How Do Companies Reduce Outbound Email Risks Today?

The survey also asked respondents about their company's deployment of a variety of techniques and technologies to mitigate risks related to outbound email content and security. Companies are clearly concerned about these risks but even though technology adoption is increasing, the 2009 results still show a relatively low rate of adoption for technology solutions related to better securing outbound email. Looking at the overall results from this year's sample, only one of the technology solutions—email archiving—showed more than 50% penetration.

At the same time, manual processes—such as conducting regular audits of outbound email content and employing staff to read outbound email—continue to be relatively common and, in this year's sample, reached their highest levels ever.

Figure 3 on the next page 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).

They're (Still) Reading Employee Email—More than Ever?

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 3).

In this year's survey, more than a third of all US respondents—38.4%—reported that they employ staff to monitor (read or otherwise analyze) outbound email content. An additional 23% of companies surveyed said that they intend to deploy such staff in the future. This technique is even more common in the largest organizations—48.3% of US companies surveyed with more than 20,000 employees employ staff to monitor the content of outbound email (and 21.6% say they intend to deploy such staff in the future).

These findings are the highest in the six year history of this survey. While the use of such staff may actually be increasing, it is important to note that this year's US survey sample is unique (the exact makeup and size of the panel varies from year to year) and was provided by Osterman Research, a research and analysis firm that specializes in the field of electronic messaging issues. For example, in this year's survey panel, directors or managers of email/messaging systems are well represented (15.5% of respondents hold this title) as opposed to the 2008 panel where just 1% of respondents shared that title.

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., in 2008, 29% of US companies surveyed said they employed staff to read outbound email; in 2007 the finding was 32% in 2006, the finding was 38%; in 2005, the finding was 36%; in 2004, the finding was 31%).

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." Again, the 2009 findings are the highest ever: 32.9% of US companies surveyed employ such staff (2008 finding: 15%) with an additional 16.9% saying that they intend to employ such staff in the future (2008 finding: 17%).

Of the largest US companies surveyed (those with 20,000 or more employees), 38.3% employ staff whose primary or exclusive job function is to read or otherwise analyze outbound email content (2008 finding: 22%) and 21.7% of them intend to do so in the future.

The survey also asked respondents if they perform regular audits of outbound email content. Overall, 45.9% of US companies surveyed perform such audits (2008 finding: 38%). Among the largest companies, more than half (58.3%) perform regular audits of outbound email content.

Adoption of Techniques and Technologies for Mitigating Outbound Messaging Risks, Overall and by Company Size, 2009

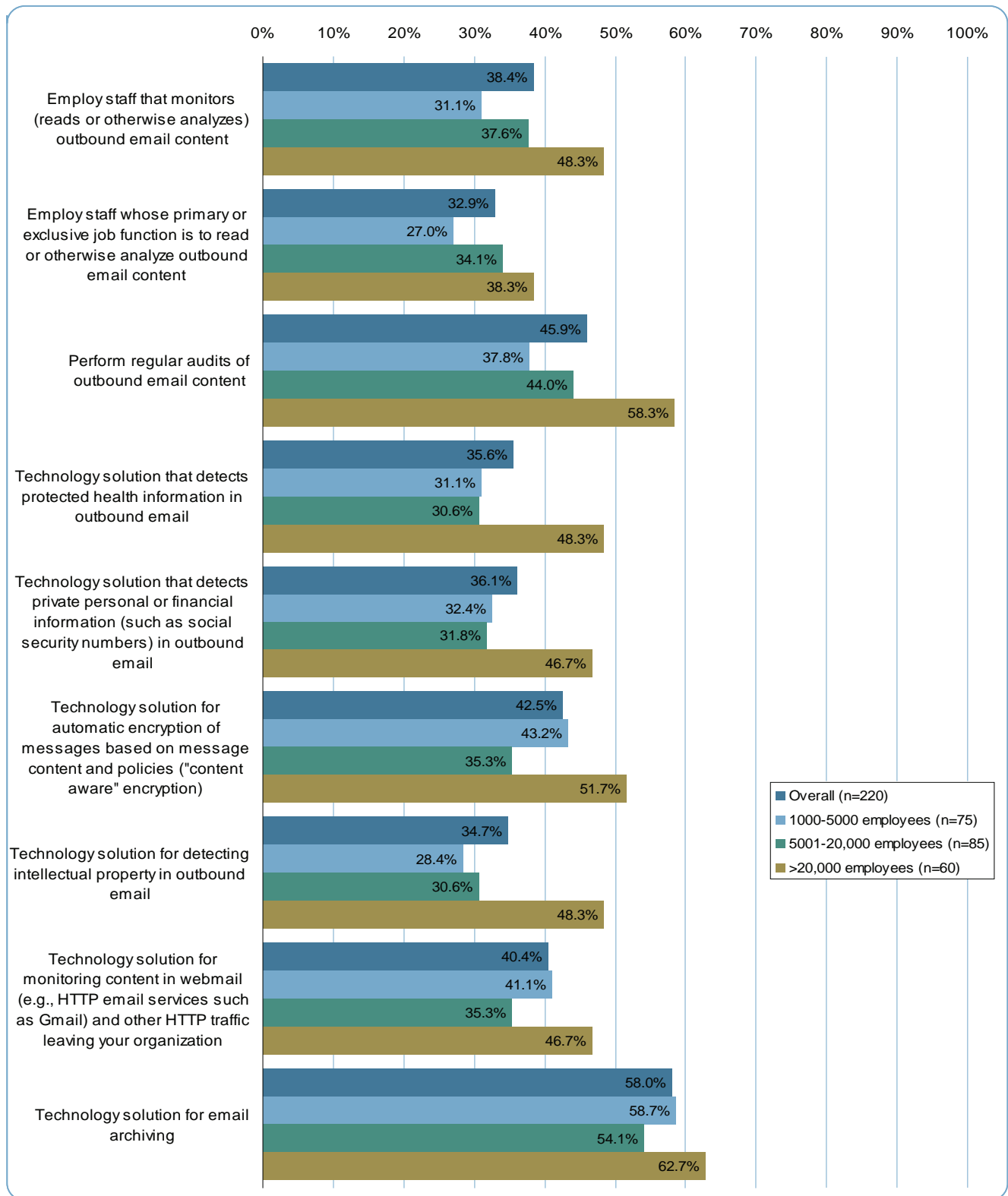


Figure 3: Percentage of respondents, overall and by company size, who report having deployed or used various techniques and technologies for mitigating outbound messaging-related risks.

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 3. As is the case with manual processes, in general, larger companies are more likely to have deployed a given technology.

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. 35.6% 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. 36.1% 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). 42.5% of US companies surveyed 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. 34.7% 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. 34.7% of US respondents said they have deployed such a solution.

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, 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 additional outbound data streams as conduits for the exposure of confidential or proprietary information. The key findings, overall and broken out by company size, are summarized in Figure 4 which shows the percentage of respondents who reported being "concerned" or "very concerned" about each outbound data stream.

In previous years' surveys (2006 through 2008), most conduits were rated as a concern by 40% or more of US respondents. That held true again this year (2009), as each area was rated as a concern by more than 40% of US respondents, with the exception of FTP (about which 38.9% of US respondents expressed a high degree of concern). It's worth noting that respondents from companies with 1000 to 5000 employees express a lower level of concern about all of these conduits than their counterparts at larger organizations (as can be easily seen in Figure 4).

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

In previous years, we concluded that outbound SMTP email was the number one risk area for data loss, based on the high levels of concern expressed around the various "areas of outbound email concern" (charted in Figure 1). Overall, this finding was explicitly confirmed in 2009, as

51.2% of respondents overall reported that they were “concerned” or “very concerned” about exposure of confidential or proprietary information via “email sent from your organization’s SMTP email system.”

Looking at the results broken out by company size, however, it is interesting to note that the largest enterprises (those with more than 20,000 employees) expressed a higher level of concern about “Email sent from mobile devices” and organizations with between 5000 and 20,000 employees expressed a higher level of concern about “Web-based email services” and “Postings to social networking sites” as potential conduits for data loss.

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

For the second year, respondents were asked about their level of concern about email sent from mobile devices (such as smartphones or other wireless, Internet-connected devices). Overall, just over half (50.5%) of US respondents said they are “concerned” or “very concerned” about the potential for data loss via mobile email.

Organizations with more than 20,000 employees reported a notably higher level of concern about mobile email, with 63.8% reporting that they are “concerned” or “very concerned.”

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 one third (33%) of employees have such access (broken out by company size, mean estimates were 41.3% for organizations with 1000 to 5000 employees, 27.5% for those with 5000 to 20,000 employees and 30.1% for those with more than 20,000 employees).

For statistics on the number of data loss incidents associated with *lost or stolen* mobile devices and storage media, please see “Policy Enforcement and Investigations of Suspected Violations” later in this document.

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

This year, just under half of US respondents (49.8%) surveyed said they were “concerned” or “very concerned” about Web-based email (e.g., services such as Google Gmail, Yahoo! Mail, Hotmail, etc.) as a conduit for the exposure of confidential information.

For organizations with 5000 to 20,000 employees, this was the number one area of concern (57.5% of such respondents).

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 risk. 46.2% of US respondents surveyed expressed a high degree of concern about blog and message board postings as a potential source for confidential or proprietary information exposure.

For statistics on the number of data loss incidents, employee discipline and terminations associated with postings to blogs and message boards, please see “Policy Enforcement and Investigations of Suspected Violations” later in this document.

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

For the second 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. The now explosive growth of social networking sites and their increasing popularity as a business networking and recruitment tool has created a new source of data leakage risk.

45.1% of US companies surveyed were “concerned” or “very concerned” about posts to social networking sites as a potential conduit for data loss (2008 finding: 44%).

For statistics on the number of data loss incidents, employee discipline and terminations associated with postings to social networking sites, please see “Policy Enforcement and Investigations of Suspected Violations” later in this document.

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

Instant Messaging (IM) is increasingly common in today's enterprise and continues to be a significant source of risk. Concern about Instant Messaging (IM) as a conduit for confidential or proprietary information exposure was high for 44.6% of US respondents.

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

New for 2009, 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. 44.1% of respondents said they were "concerned" or "very concerned."

As with mobile email, organizations with more than 20,000 employees expressed a significantly higher level of concern than other organizations. More than half (55.9%) of such respondents reported being "concerned" or "very concerned" about this conduit.

For statistics on the number of data loss incidents, employee discipline and terminations associated with mobile and Web short message services, please see "Policy Enforcement and Investigations of Suspected Violations" later in this document.

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, Revver, Vimeo, etc.) and the proliferation of digital media creation in the workplace continues to be a source of risk for large organizations. This year, 42.1% of US companies expressed a high level of concern about postings to media sharing sites

For statistics on the number of data loss incidents, employee discipline and terminations associated with postings to media sharing sites, please see "Policy Enforcement and Investigations of Suspected Violations" later in this document.

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

New for 2009, the survey asked respondents to rate their level of concern about short messages sent from Web-based short messaging services (e.g., Twitter, Friendfeed, etc.). The apparent "overnight success" of Twitter is the most obvious example of such services. But regardless of the success of any individual Web-based short message service, the popularity of the concept would seem to guarantee that such services will play a part in the messaging threat landscape for the foreseeable future.

Can data loss happen 140 characters at a time? 41.5% of US respondents report that they are "concerned" or "very concerned" about this possibility.

For statistics on the number of data loss incidents associated with mobile and Web short message services, please see "Policy Enforcement and Investigations of Suspected Violations" later in this document.

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

Though they may not be in the news as much as in previous years, peer-to-peer networks (commonly used for both legitimate distribution and rights-infringing sharing of digital files) continue to represent a significant source of risk for large enterprises. 40% of US companies surveyed said they were "concerned" or "very concerned" about P2P networks as potential conduits for data loss.

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

As in previous years, respondents expressed the lowest level of concern about the venerable FTP (File Transfer Protocol). 38.9% of US respondents said they were "concerned" or "very concerned" about FTP protocol transmissions as a potential source of information leakage.

Level of Concern about Potential Conduits for Exposure of Confidential Information, Overall and by Company Size, 2009

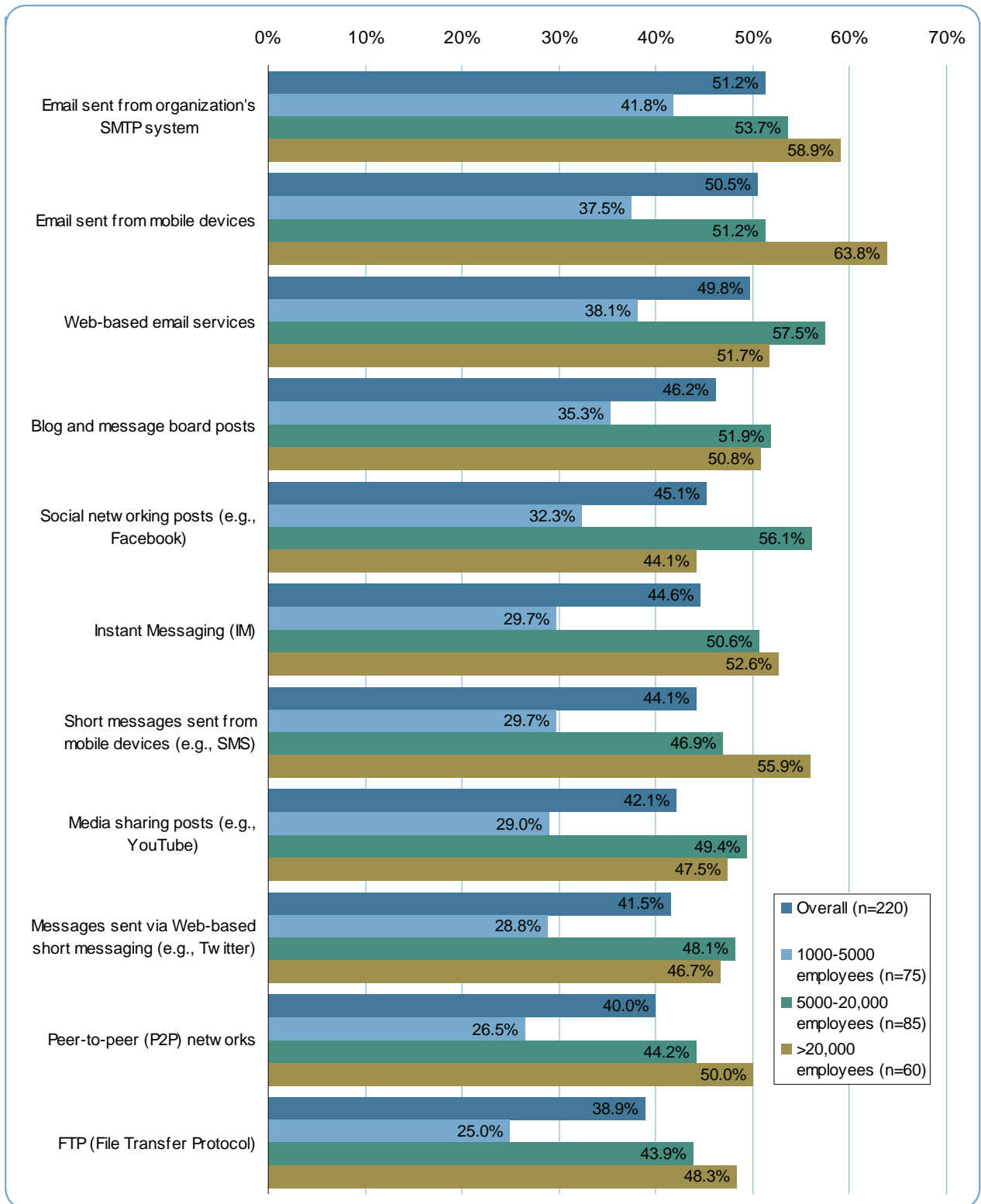


Figure 4: Percentage of respondents who reported being “concerned” or “very concerned” about various protocols that may serve as conduits for exposure of confidential info.

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. As a way of measuring the sophistication of the policy environment in large companies around the world, respondents were asked, "at what stage is your organization in defining, implementing and enforcing" twelve different types of email- or content security-related policies.

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 5 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, 93.6% of US companies reported having formalized an acceptable use policy for email. As shown in Figure 5, acceptable use policies for email have a nearly universal level of adoption in the largest companies (98.3%), but 8.1% of companies with 1000 to 5000 employees and 4.7% of companies with 5000 to 20,000 employees report that they have "no formal policy" for acceptable use of email (the remainder, 3.5% of respondents in the 5000 to 20,000 employee range, said they "don't know").

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, 90.3% of US companies reported having a formal ethics policy.

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, 84.5% of US companies reported having a formal email retention policy.

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, 83.1% of US companies reported having formalized such a 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, 82.2% of US companies reported having formalized such a remote access policy for mobile computing and storage devices.

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, 77.7% 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, 76.8% of US companies reported having a formal risk assessment policy.

Media sharing/posting policy

An acceptable use policy that specifically addresses the use of video or audio content sharing sites and P2P (peer-to-peer) networks (e.g., YouTube, Revver, BitTorrent, Google Video, etc.).

Overall, 72.1% of US companies reported having a formal media sharing/posting policy.

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, 71.8% 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, 71.4% of US companies reported having a formal audit vulnerability scanning policy.

Automatically forwarded email policy

A policy that governs the automatic forwarding of email to external destinations.

Overall, 69.1% of US companies reported having a formal policy for automatically forwarded email.

Social networking policy

An acceptable use policy that specifically addresses the use of social networking sites (e.g., MySpace, Facebook, etc.).

Overall, 66.8% of US companies reported having a formal acceptable use policy for social networking sites.

Adoption of Outbound Messaging-related Security Policies, Overall and by Company Size, 2009

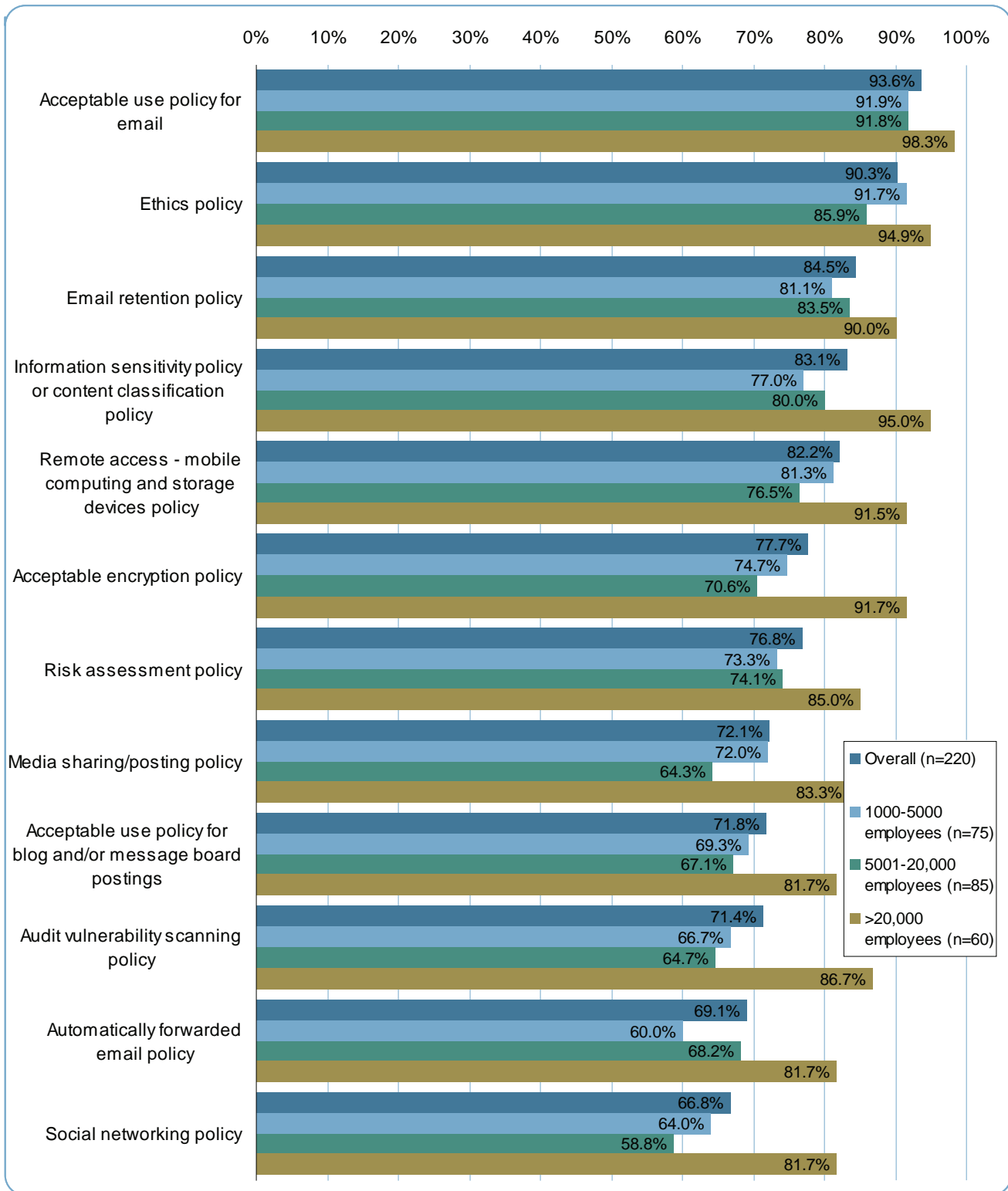


Figure 5: Percentage of companies reporting that they have formalized various security-related policies, by company size.

Investigations of Data Loss Incidents, Employee Training and Policy Enforcement Actions

More interesting than the adoption of various policies are the actions that companies have taken to educate employees about messaging and content security policies, as well as actions taken to enforce policy violations.

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 6 through 8 on the following pages.

Formal Email Policy Training

Respondents were asked if their company had conducted formal training for employees about its email security policies or about external regulations that apply to the organization's use of email in the past 12 months. The results, overall and broken out by company size category, are summarized in Figure 6, below.

- **Email security policy training:** Overall, more than half (56.5%) of US 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, 72.9% had conducted such a training.
- **Email regulation training:** Overall, 39.7% of US respondents said their organization 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 more likely to have conducted such training, with more than half (54.2%) of the organizations with more than 20,000 employees reporting that they had provided such training.

Formal Email Policy Training, Overall and by Company Size, 2009

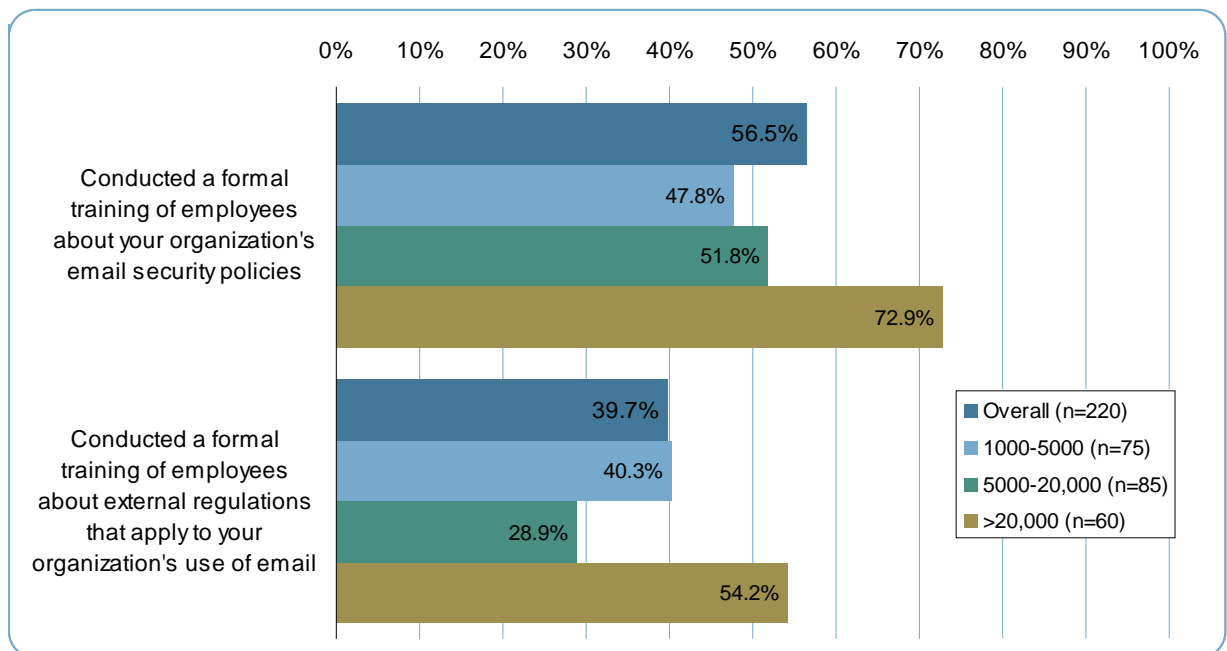


Figure 6: Percentage of companies that reported conducting formal training for employees about that organization's email policies in the past 12 months.

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 7, 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 most cases, 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

Leaks of confidential information via email occurred at nearly the same rate as in 2008, when we saw investigations of such leaks hit their highest levels since Proofpoint started tracking this statistic in 2005.

This year, 43.1% of respondents said that they had investigated a suspected leak of confidential or proprietary information via email (2008 finding: 44%). Looking at the largest US companies (those with 20,000 or more employees), these investigations were even more common—nearly half (49.2%) of the largest US companies had done so.

As can be seen from Figure 7, of the various types of leaks the survey asks about, investigations of email-based leaks of confidential or proprietary information remain the most common.

Potential Violations of Privacy and Data Protection Regulations via Email

Overall, more than a third (34%) of 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 lower than our 2008 finding of 40%, when we saw investigations of such data privacy violations reach their highest levels since we started tracking this statistic in 2005).

Leaks of Confidential Information Via Blog or Message Board Postings

Blogs and message board postings continued to be a significant source of risk. Overall, 18.2% of respondents 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.

More than a quarter (25.4%) of surveyed companies with more than 20,000 employees reported investigating such a leak.

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

The increasing ease of producing video and audio media, combined with the continued popularity of media sharing sites such as YouTube, has made such sites a real source of risk.

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, 17.7% of US respondents to this year's survey reported such an investigation (up from 12% in 2008). More than 1 in 5 companies (22%) with more than 20,000 employees reported that they investigated the exposure of confidential information via video or audio media posted to a media sharing site in the past 12 months.

Leaks of Confidential Info Via Social Networking Site Postings

For the second year, 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. In the past year, services such as Facebook have exploded in popularity, both with individuals and with enterprises seeking to leverage social media in their marketing efforts.

It's no surprise then, that investigations of data loss events related to social networking sites increased over our 2008 findings. Overall, 17.2% of US 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 (2008 finding: 12%).

More than a quarter (25.4%) of surveyed companies with more than 20,000 employees reported investigating this type of leak.

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

New for 2009, 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.

While such investigations are not (yet) particularly common, they are far from insignificant. Overall, more than 1 in 10 (13.4%) organizations reported such an investigation. Looking at the largest organizations (those with more than 20,000 employees), 1 in 5 (20.3%) reported that they investigated the exposure of confidential, sensitive or private information via short message services in the past 12 months.

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). 15.3% of US public companies surveyed (there were 120 of them in this year’s sample, or 54.8% of the total respondents) said that they investigated the exposure of material financial information via a blog or message board posting. Among non-public companies, 9.9% reported such an investigation. Note that, in Figure 7, the aggregate results for all companies (both public and non-public) are shown.

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

For the second year, respondents were asked if they had investigated “the exposure of confidential, sensitive or private information via lost or stolen mobile devices (e.g., laptop, smart-phone, 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 it’s interesting to compare the risk of this type of “physical” data loss to the risks presented by electronic channels such as email.

This year’s survey found that more than 1 in 5 (21.5%) US organizations reported investigating the exposure of confidential information via lost or stolen mobile devices or media (2008 finding: 27%). Nearly one third (32.2%) of the largest companies reported such an investigation.

So, while data loss events related to email are more common, lost/stolen devices and storage media are a significant source of data loss risk (roughly on par with the risk presented by blog/message board postings).

Employee Terminations as a Source of Data Loss Risk

In keeping with this year’s special focus on the intersection of data loss and the global economic recession, 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, 17.7% of US companies surveyed said they investigated such a leak or theft. As can be seen in Figure 7, the frequency of such investigations varied substantially by company size. Organizations with more than 20,000 employees were more than twice as likely to report such an investigation as companies with 5001 to 20,000 employees (32.2% versus 14.5%) and more than 3 times as likely to report such an investigation as companies with 1000 to 5000 employees (32.2% versus 9.0%).

Litigation Concerns: Subpoenas of Employee Email

Exposure of confidential information can also occur when, in the course of civil or criminal investigations, a company’s email messages 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?).”

Overall, nearly one quarter (23.9%) of US companies surveyed reported having to produce employee email in the past year. This is one area where responses did *not* vary much by company size, as can be seen in Figure 7.

Investigations of Potential Data Leaks and Compliance Violations, Overall and by Company Size, 2009

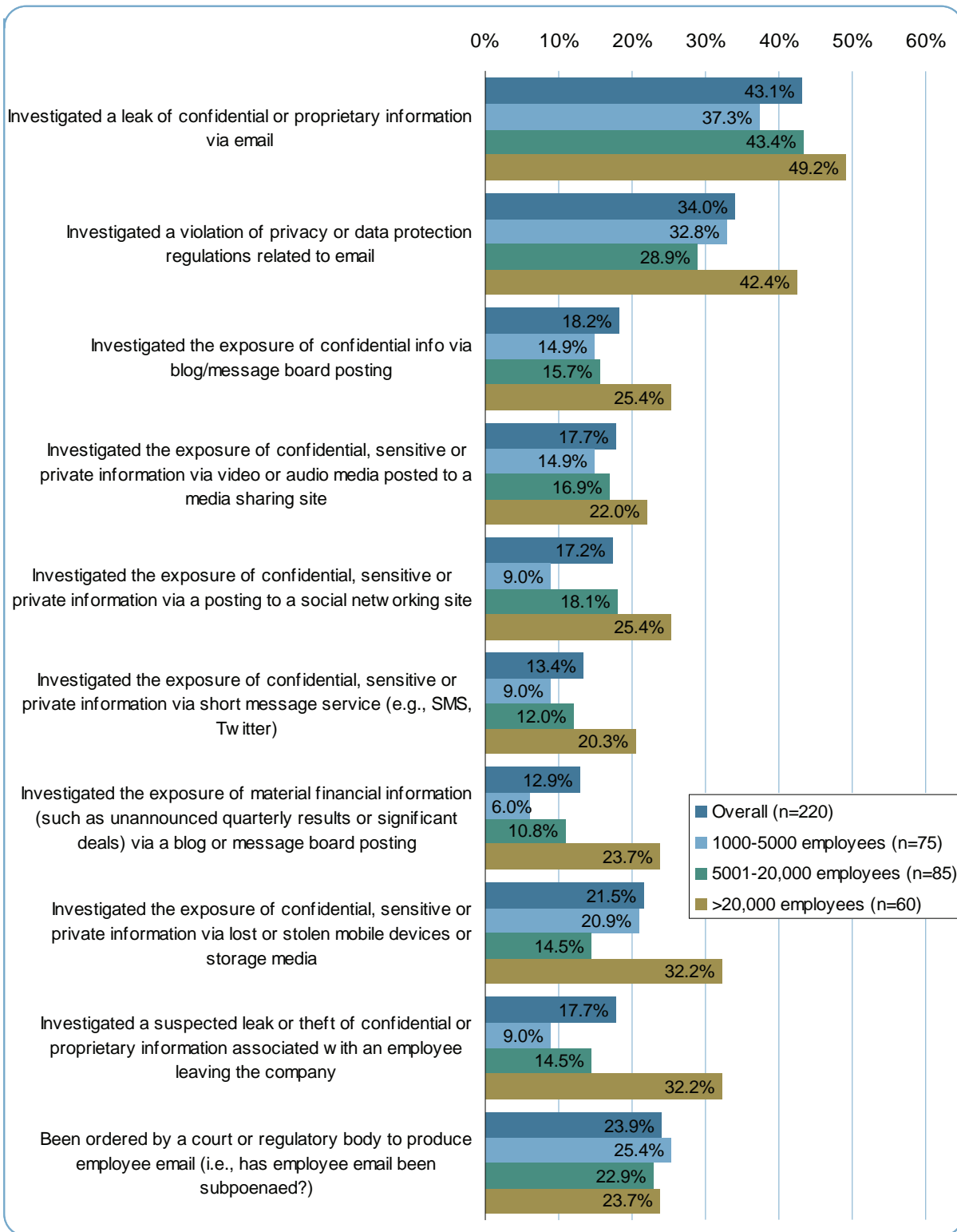


Figure 7: Percentage of US respondents who reported investigating various types of data loss events in the past 12 months.

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

As in past years, the 2009 survey asked respondents about various disciplinary actions, including termination, that they took against employees for violations of various messaging-related policies. The key findings are summarized in Figure 8. In general, the larger the organization, the more likely they are to report taking some form of disciplinary action.

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 more than half (51.7%) of US companies surveyed had disciplined an employee for violating email policies in the past 12 months. These results are consistent with previous years' findings (e.g., in 2008, 51% US companies reported this type of disciplinary action; in 2007 the finding was 52%).

Terminations were slightly more frequent this year. Overall, 31.6% of US companies reported that they terminated an employee for violating email policies in the past 12 months (2008 finding: 26%).

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, 17.2% of US companies surveyed said they had disciplined an employee for blog or message board policy violations in the past year. Terminations were less frequent, with 9.1% of US companies reporting that they had terminated an employee for violating blog or message board policies.

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, 15.3% of US companies surveyed reported disciplining an employee for violating media sharing/posting policies. As expected, terminations were less frequent with 7.7% of US companies reporting 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, 1 in 10 (10%) US companies reported that an employee had been disciplined for this reason. Terminations of employees for violations of social networking policies were slightly less frequent as 7.7% of US companies reported taking such actions.

Discipline and Termination Actions Taken by Companies, Overall and by Company Size, 2009

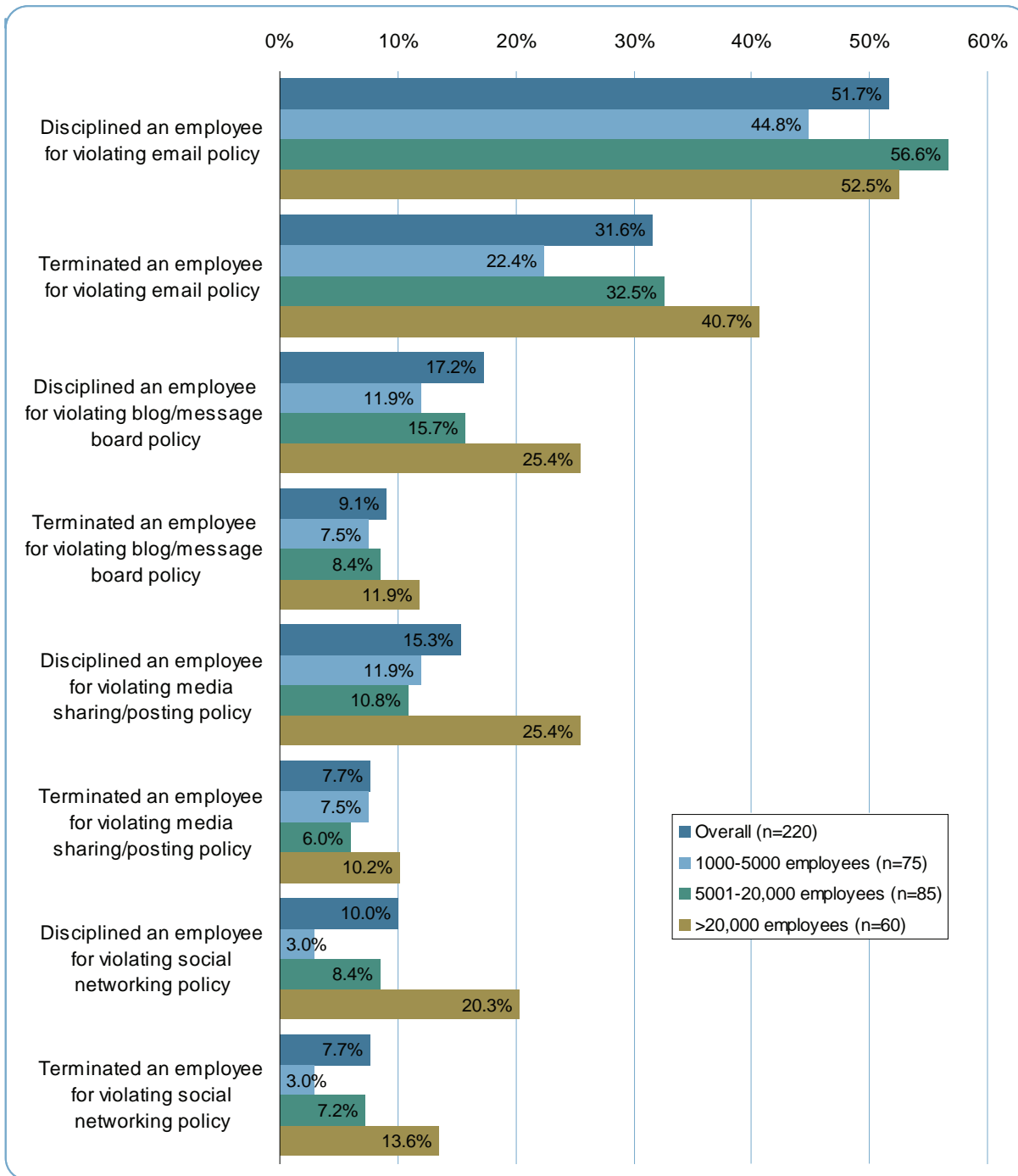


Figure 8: Percentage of respondents who reported various types of disciplinary actions against employees for messaging-related policy violations in the past 12 months.

Exposure and Theft 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.

Figure 9, below, summarizes the 2009 responses to these questions, showing overall findings as well as breakouts by company size.

Improper Exposure or Theft of Customer Information

Overall, nearly 1 in 3 US companies surveyed (32.8%) reported that they had been impacted by improper exposure or theft of customer information in the past 12 months. Companies with more than 20,000 employees were even more likely to report being impacted by customer information theft (42.4% said they experienced such exposure).

Improper Exposure or Theft of Intellectual Property

Overall, more than 1 in 4 US companies surveyed (27.4%) reported that they had been impacted by improper exposure or theft of intellectual property in the past 12 months. More than a third of companies with more than 20,000 employees (33.9%) said they experienced improper exposure or theft of intellectual property.

Exposure of Sensitive or Embarrassing Information

Overall, more than 1 in 3 US companies surveyed (33.8%) reported that their business had been impacted by the exposure of sensitive or embarrassing information in the past 12 months. In this instance, it was companies in the 5001 to 20,000 employee range that reported the most frequent exposure of “sensitive or embarrassing information” (42% say they were impacted).

Exposure or Theft of Sensitive Information, Overall and by Company Size, 2009

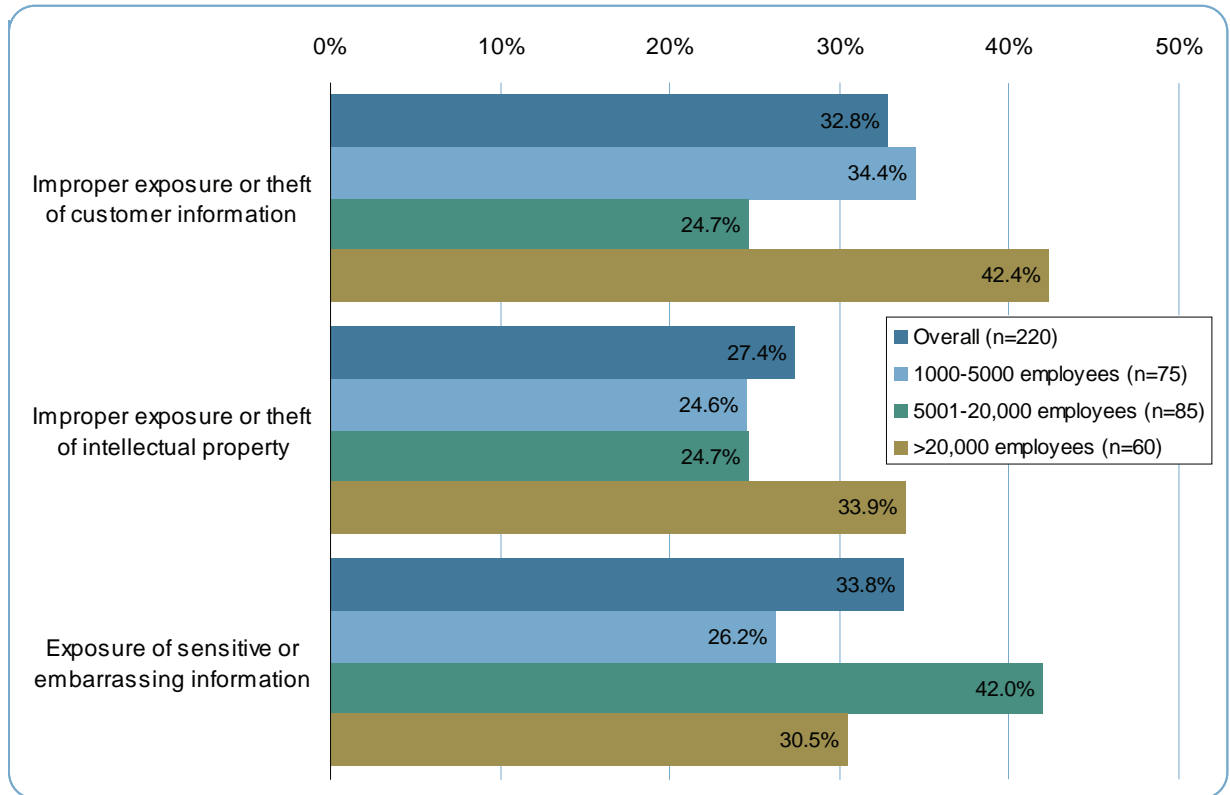


Figure 9: Percent of respondents who reported that their organization had been impacted by exposure or theft of various types of sensitive information in the past 12 months.

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, more than half of US respondents surveyed (62%) 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.

The responses, also broken out by company size, are summarized in Figure 10 below.

Importance of Reducing Risks Associated with Outbound Email, Overall and by Company Size, 2009

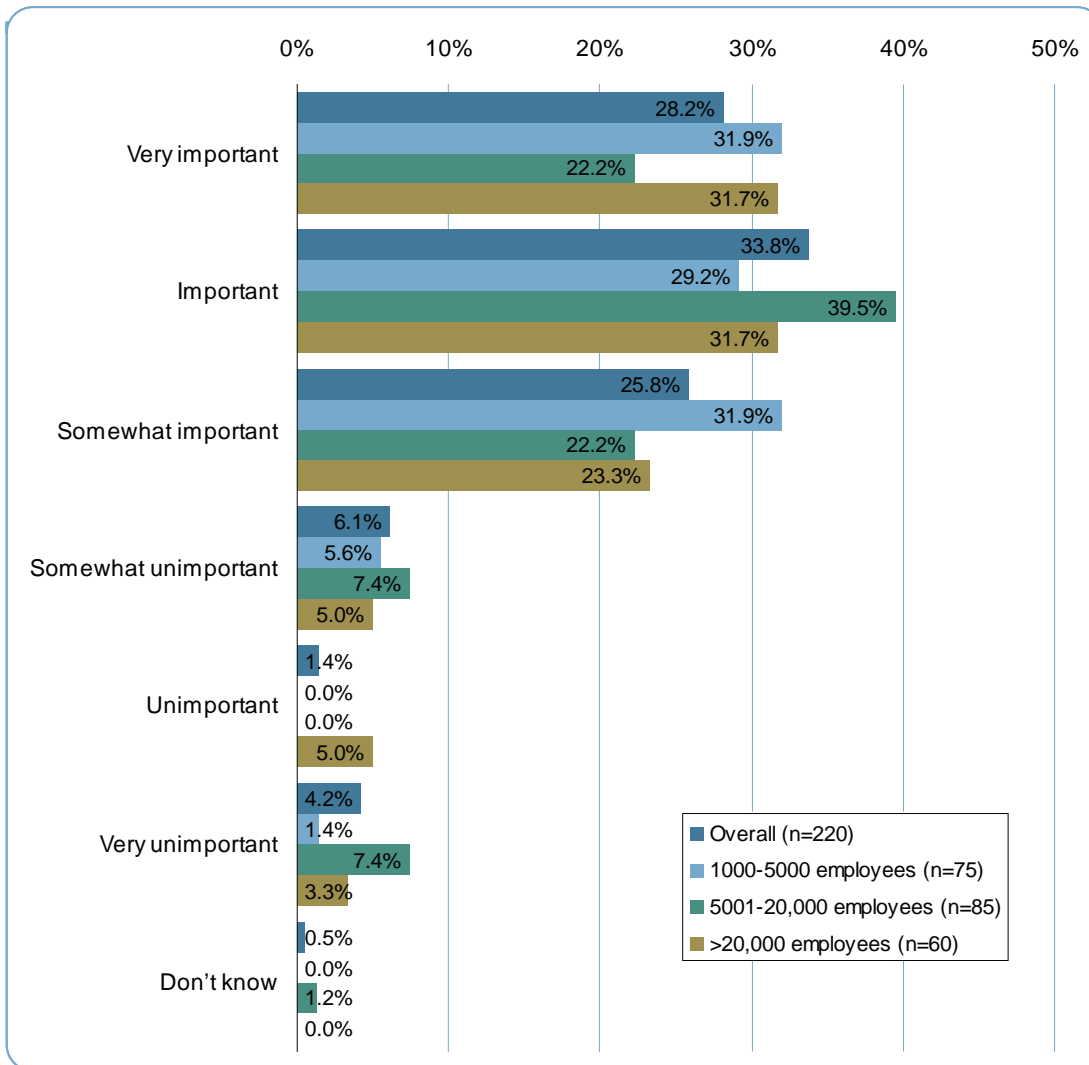


Figure 10: Importance of reducing the legal and financial risks associated with outbound email in the next 12 months.

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, more than half of US respondents surveyed (56.4%) 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.

The responses, also broken out by company size, are summarized in Figure 11 below.

Importance of Reducing Risks Associated with Outbound HTTP Content, Overall and by Company Size, 2009

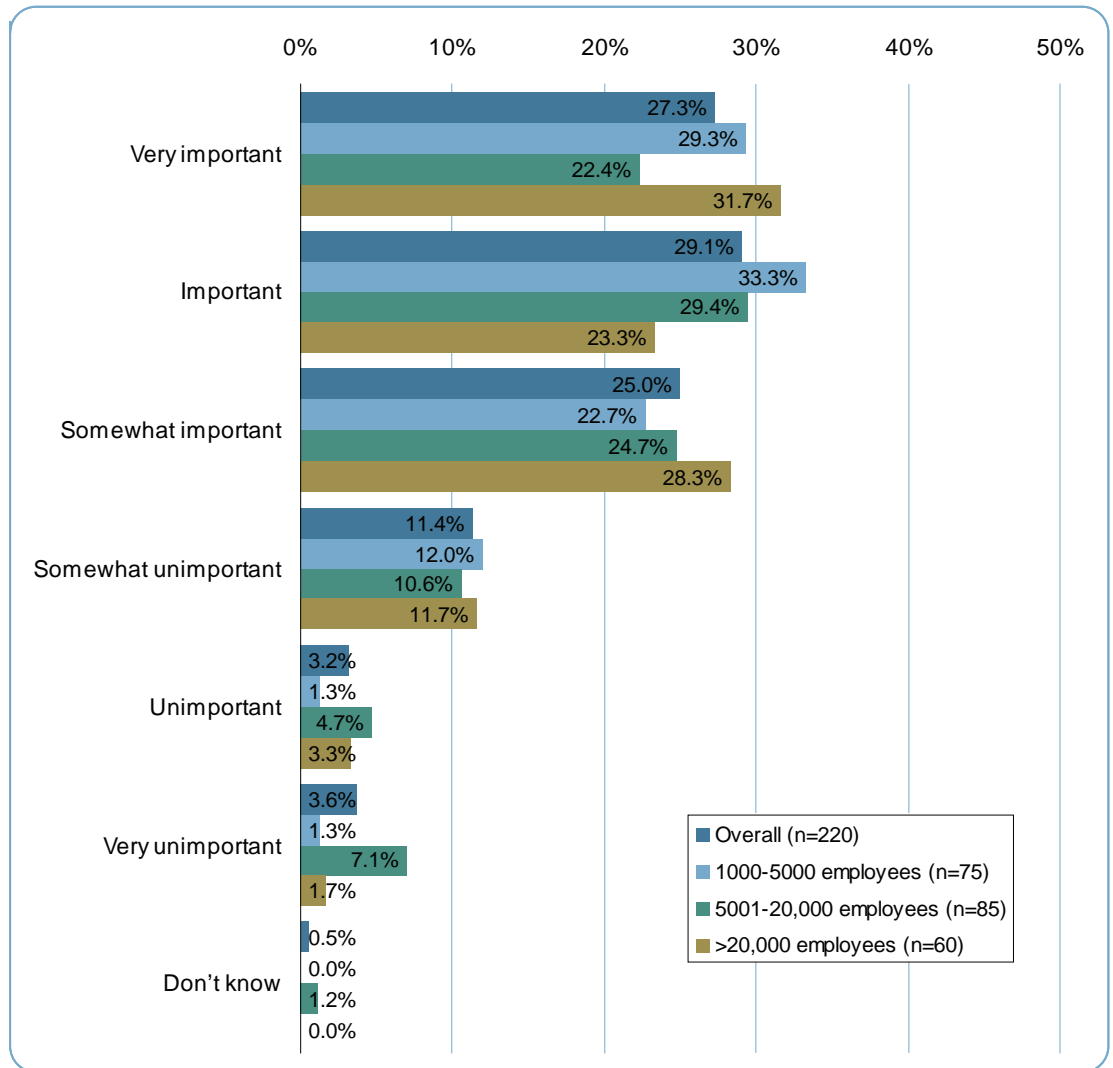


Figure 11: Importance of reducing the legal and financial risks associated with outbound HTTP content (e.g., webmail, blog and message board postings, etc.) in the next 12 months.

Economic Considerations: Budget, Layoffs and Data Security

New for the 2009 survey, we 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. 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, half of respondents (50.5%) agreed or strongly agreed with this statement. Smaller organizations (those with 1000 to 5000 employees) seem to be impacted more by budget constraints with 61.3% of respondents from those companies agreeing with this statement.
- “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, 47.3% 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, 42.2% of respondents agreed or strongly agreed with this statement.

Responses to this question are summarized in Figure 12, below.

Budget and Economic Trends Issues, Overall and by Company Size, 2009

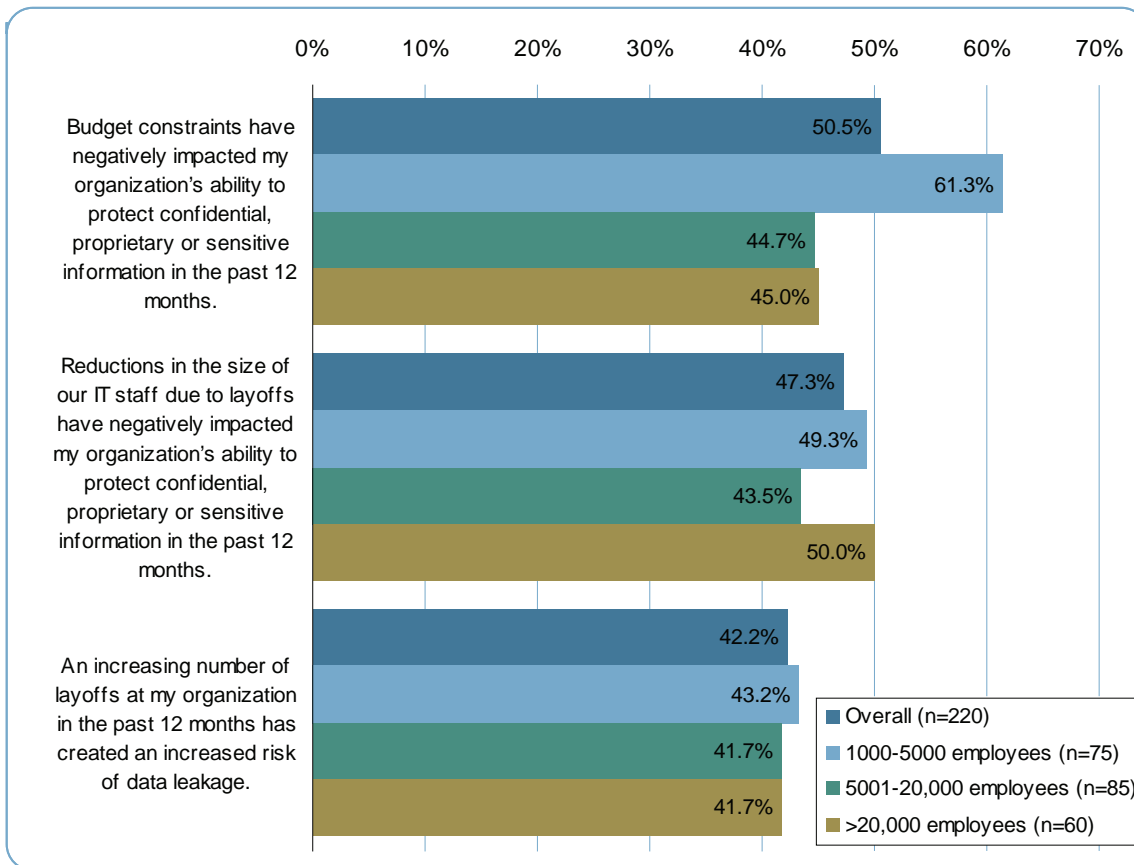


Figure 12: Percentage of respondents that “agree” or “strongly agree” with various statements about the data security impact of budget constraints and employee layoffs in their organizations.

SaaS and Cloud Computing as Sources of Cost Savings and Data Loss Risk

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 an on-demand (SaaS) model. As a result, more confidential, private and proprietary data is stored outside the enterprise, potentially posing new security concerns for IT professionals. New for 2009, we asked questions to identify (1) whether large organizations have adopted, or will adopt, SaaS technology for securing outbound email or HTTP transmissions and (2) whether the increasing use of SaaS and cloud computing technologies is perceived as a source of data loss risks.

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:

- “My organization has deployed or will deployed SaaS-based (Software-as-a-Service) solutions for outbound email or HTTP security in order to reduce costs.” Overall, more than one third of respondents (37.4%) indicated that they have or are likely to deploy such technology. Smaller organizations (those with 1000 to 5000 employees) are more likely to agree with this approach as almost half (49.3%) of respondents from those companies agreed or strongly agreed with this statement.
- “The trend toward using SaaS and cloud computing solutions in the enterprise seriously increases the risk of data leakage.” Overall, 40.5% of respondents agreed or strongly agreed with this statement.

Affirmative responses to these statements are summarized in Figure 13, below.

SaaS Issues, Overall and by Company Size, 2009

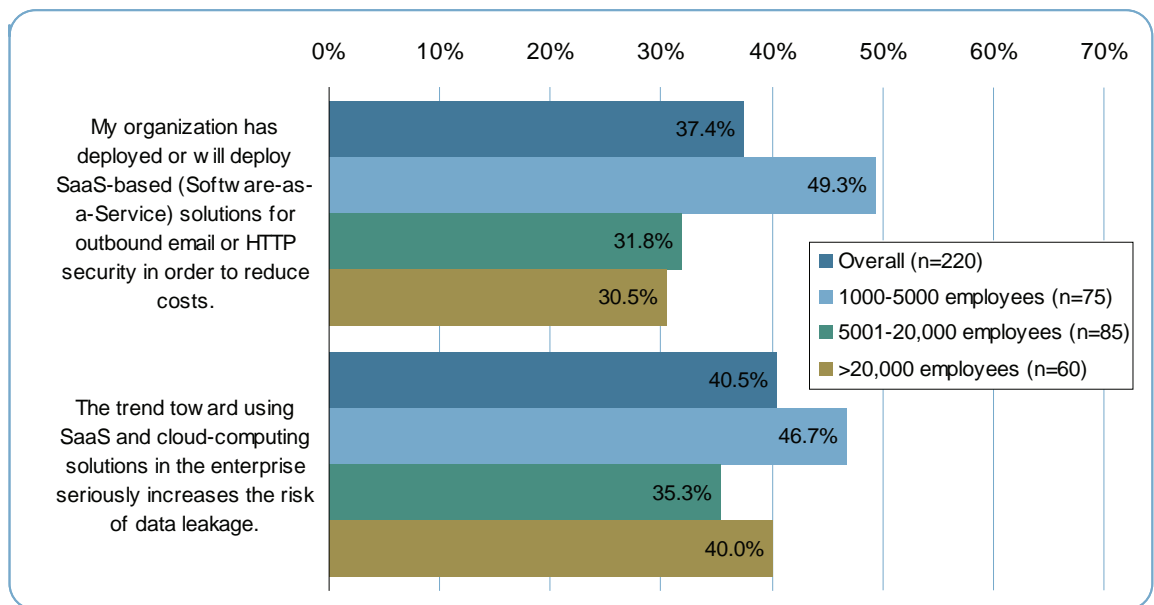


Figure 13: Percentage of companies that “agree” or “strongly agree” with statements related to SaaS and cloud computing issues.

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. As a way of measuring the relative importance of inbound email filtering, outbound email filtering/email data loss prevention and email archiving, 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 14, below, shows the percentage of companies who rated each area as “important/priority” or “very important/high priority.” Overall, respondents rated “improving malware detection and prevention” as a slightly higher priority than “improving the ability to prevent sensitive content from leaving the organization through email.” However, investing in such outbound email protection was rated as slightly more important than “improving spam filtering.” Email archiving related investment areas were rated as a lower priority, followed by improving e-discovery for non-email electronic content.

Relative Priority of Investment in Various Messaging Security Areas, Overall and by Company Size, 2009

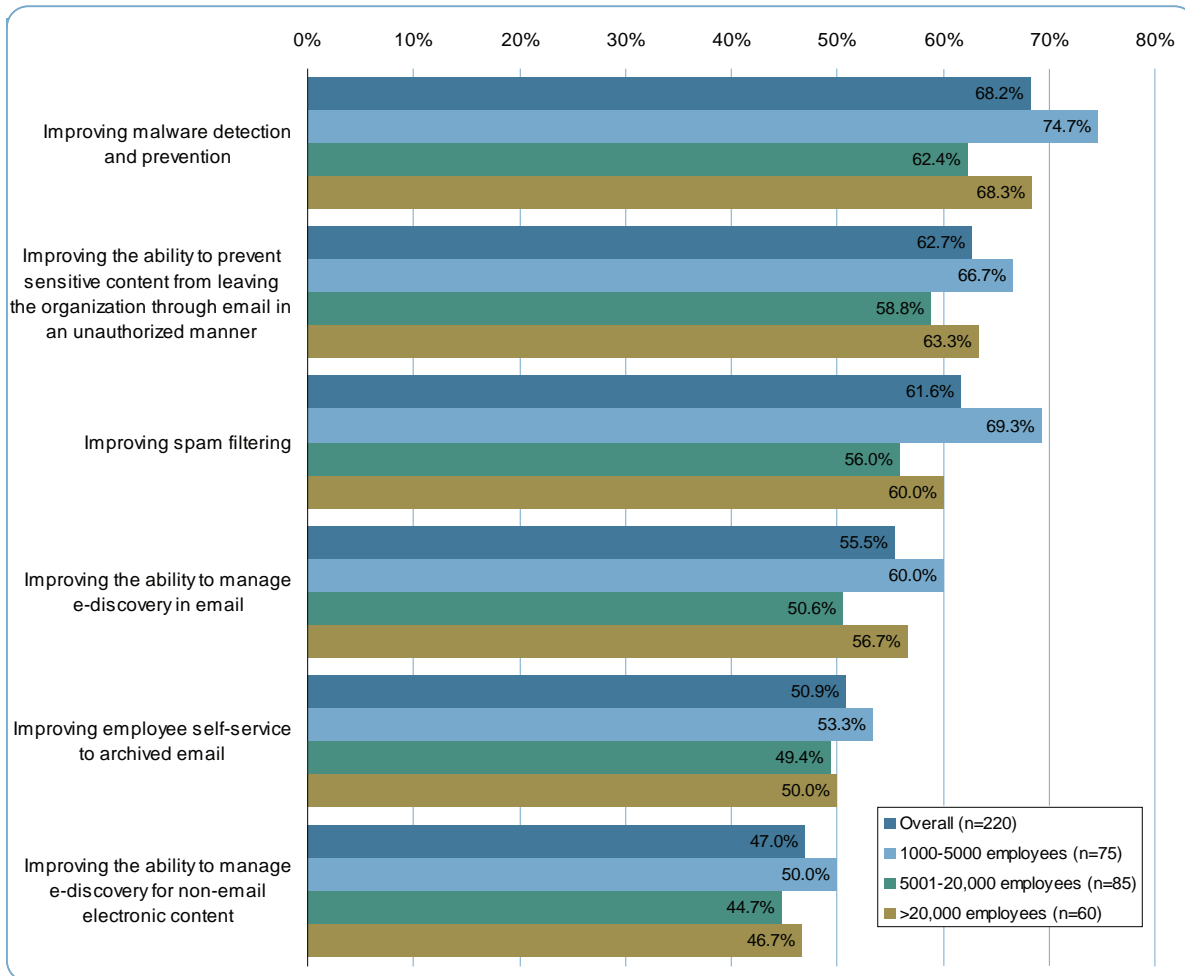


Figure 14: Percentage of respondents who rated investment in various messaging security areas as a “priority” or “high priority” over the next 12 months.

Appendix: Respondent Demographics

Respondent Titles

The 220 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	12.7%
CSO, CISO, or senior-most IT security executive	1.4%
VP or executive of IT	7.3%
VP or executive of security	1.8%
Director or manager of IT	44.5%
Director or manager of security	3.2%
CFO, CEO, COO	3.2%
Compliance or legal officer, or counsel	0.5%
Senior finance executive	5.5%
Senior human resource executive	4.5%
Director or manager of messaging/email systems	15.5%

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	34.1%
5,001 to 20,000 employees	38.6%
More than 20,000 employees	27.3%

Ownership	Percent of Respondents
Publicly traded	54.8%
Privately held	26.5%
Other (e.g., non-profit, public sector, etc.)	18.7%

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	4.5%
Consumer products manufacturing	4.5%
Chemical and petroleum manufacturing	3.2%
Pharmaceutical/biotech manufacturing	3.2%
High-tech products manufacturing (software, computer components, etc.)	7.3%
Industrial products manufacturing	3.6%
RETAIL/WHOLESALE	
Retail	9.5%
Wholesale	1.8%
BUSINESS SERVICES	
Transportation and logistics	3.2%
Professional services (consulting, legal, etc.)	10.0%
Construction and engineering	2.7%
Media, entertainment, and leisure	3.2%
UTILITIES/TELECOM	
Utilities	2.3%
Telecom carriers	2.7%
FINANCE/INSURANCE	
Financial services	10.0%
Insurance	4.5%
PUBLIC SECTOR	
Government	7.7%
Higher education	6.4%
Healthcare	7.3%
Non-profit/other public services	2.3%

About this Report

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

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

The summaries of Proofpoint's prior annual surveys (previously titled *Outbound Email and Content Security in Today's Enterprise*) can be downloaded from the following URLs:

<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>

The Critical Need for Encrypted Email and Secure File Transfer Solutions

This whitepaper from Proofpoint and Osterman Research discusses key issues around the encryption of both email and file transfer systems, some of the leading statutes that require sensitive content to be encrypted, and suggestions for moving forward with encryption:

<http://www.proofpoint.com/id/osterman-encryption-wp/index.php>

Global Best Practices in Email Security, Privacy and Compliance

This whitepaper discusses the impact of the latest global regulations that impact the email security policies and strategies of today's enterprises, universities and government organizations.

<http://www.proofpoint.com/id/email-security-best-practices-wp/index.php>

Regulations Shift Focus on Outbound Email Security

Discusses the impact of relatively new data protection regulations and standards such as the Payment Card Industry (PCI) Data Security Standard (DSS) and the Office of Management and Budget (OMB) Personally Identifiable Information Guidelines (PIIG), which place new constraints on how data is stored, processed, and transmitted over email:

<http://www.proofpoint.com/regulationswp>

Email Archiving: A Proactive Approach to eDiscovery

This whitepaper addresses the key e-discovery 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:

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

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:

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>

About Proofpoint, Inc.

Proofpoint secures and improves enterprise email infrastructure with solutions for email security, archiving, encryption and data loss prevention. Proofpoint solutions defend against spam and viruses, prevent leaks of confidential and private information, encrypt sensitive emails and archive messages for retention, e-discovery and easier mailbox management. Proofpoint solutions can be deployed on-demand (SaaS), on-premises (appliance), or in a hybrid architecture for maximum flexibility and scalability.

Proofpoint Solutions for Outbound Email Content Security, Data Loss Prevention and Regulatory Compliance

Proofpoint's SaaS, appliance, virtual appliance and software solutions for email security and data loss prevention defend against all types of inbound and outbound message-borne threats. Proofpoint provides a variety of modular defenses for protecting enterprises against the threats described in this report.

Enforcing Email Acceptable Use Policies

Proofpoint makes it easy to define and enforce corporate acceptable use policies for message content and attachments. A convenient point-and-click interface simplifies the process of defining complex logical rules related to file types, message size, and message content. Proofpoint's content compliance features can be used to identify and prevent a wide variety of inbound and outbound policy violations—including offensive language, harassment, file sharing, and violations of external regulations. Non-compliant messages can be acted on with a wide variety of options, including quarantine, reroute, reject, annotate, and other actions.

Preventing Leaks of Confidential and Proprietary Information

As email has become the most important communication channel in today's enterprise, email systems have become the main repository for sensitive, confidential, and mission-critical information. The Proofpoint Digital Asset Security™ module keeps valuable corporate assets and confidential information from leaking outside your organization via email. Powerful Proofpoint MLX™ machine learning technology analyzes and classifies your confidential documents and then continuously monitors for that information in the outbound message stream—stopping content security breaches before they happen.

Ensuring Compliance with Data Protection and Privacy Regulations

The Proofpoint Regulatory Compliance™ module protects your organization from liabilities associated with data protection and privacy regulations such as HIPAA, GLBA and PCI. Pre-defined rules automatically scan for non-public information, including protected health information and personal financial information, and act on non-compliant communications, rejecting or encrypting messages as appropriate.

Enabling Content-aware Encryption

Proofpoint's SaaS, appliance and software solutions for email security can all optionally be equipped with robust, policy-based encryption features that automatically encrypt individual messages based on an organization's policies, without requiring end-users to take any special actions. Proofpoint's flexible rules, managed dictionaries and "smart identifiers" are used to accurately detect non-public information—such as protected health information and personal financial information—and reject or encrypt messages as appropriate.

<http://www.proofpoint.com/encryption>

Protecting HTTP and FTP Streams: Multi-protocol Content Security

The Proofpoint Network Content Sentry™ extends Proofpoint's email protection to additional messaging streams, including HTTP and FTP. This module inspects all outbound network traffic in real-time, monitoring for confidential information, private customer or employee data (including private healthcare, financial or identity information) and other sensitive content that may leak outside the enterprise.

Archiving Email for eDiscovery Readiness, Compliance and Easier Mailbox Management

Proofpoint ARCHIVE™, a SaaS email and IM archiving solution, incorporates Proofpoint's patented DoubleBlind Encryption™ technology, which encrypts messages before transmission to

Proofpoint's datacenters where they are stored in encrypted form. At the same time, Double-Blind Encryption ensures that data remains fully searchable via the secure Proofpoint ARCHIVE appliance. Proofpoint ARCHIVE helps organizations be prepared for eDiscovery events, improves end-user access to historical email and ensures compliance with your organization's email retention policies.

<http://www.proofpoint.com/emailarchiving>

Eliminating Risks Associated with FTP and Email Transmission of Large or Confidential Files: Secure File Transfer

Proofpoint Secure File Transfer™ lets end users send large files (or files that require enhanced security) easily and securely—while minimizing the impact of large attachments on your email infrastructure.

<http://www.proofpoint.com/sft>

For More Information

**Proofpoint, Inc. US
Worldwide Headquarters**
892 Ross Drive
Sunnyvale, CA 94089
USA
P 408 517 4710
F 408 517 4711
E info@proofpoint.com
www.proofpoint.com

Proofpoint, Inc. EMEA
Proofpoint, Ltd.
The Oxford Science Park
Magdalen Centre
Robert Robinson Avenue
Oxford, UK
OX4 4GA
Tel +44 (0) 870 803 0704
Fax +44 (0) 870 803 0705
E info@proofpoint.com
www.proofpoint.com

Proofpoint, Inc. Asia Pacific
5th Floor, Q.House Convent Bldg.
38 Convent Road, Silom, Bangrak
Bangkok 10500, Thailand
Tel +66 2 632 2997
E info@proofpoint.com
www.proofpoint.com

Proofpoint Japan K.K.
906 BUREX Kojimachi
Kojimachi 3-5-2, Chiyoda-ku
Tokyo, 102-0083
Japan
P +81 3 5210 3611
F +81 3 5210 3615
E sales-japan@proofpoint.com
www.proofpoint.co.jp

Proofpoint, Inc. Canada
60 Adelaide Street East, 9th Floor
Toronto, Ontario M5C 3E4
Tel +1 416 366 6666
Fax +1 416 366 6667
E info@proofpoint.com
www.proofpoint.com

Proofpoint, Inc. Mexico
Uxmal 165 int 7
Col. Narvarte
CP 03020
México D.F.
Tel: +52 55 5330 3382
E info@proofpoint.com
www.proofpoint.com

©2009 Proofpoint, Inc. All rights reserved.
Proofpoint, Proofpoint Protection Server, Proofpoint Messaging Security Gateway, Proofpoint on Demand, Proofpoint MLX, Proofpoint Content Compliance, Proofpoint Regulatory Compliance, Proofpoint Network Content Sentry, Proofpoint ARCHIVE, Proofpoint Secure Messaging and Proofpoint Digital Asset Security are trademarks or registered trademarks of Proofpoint, Inc. in the US and other countries.
Version 08/09 - Rev B