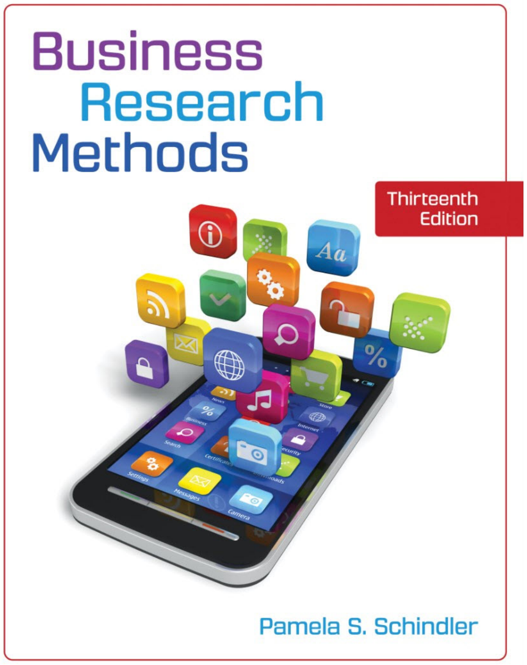

Outbound Email and Content Security in Today's Enterprise, 2006

proofpoint™

Outbound Email and Content Security in Today's Enterprise, 2006

Results from a survey by Proofpoint, Inc. fielded by Forrester Consulting on outbound messaging and content security issues

May 2006

On behalf of Proofpoint, Inc., Forrester Consulting fielded an online survey of email decision makers at US and UK businesses. Respondents were asked about their concerns, priorities and plans related to the content of email leaving their organizations. Forrester gathered 294 responses from US companies with 1,000 or more employees and 112 responses from UK companies with 1,000 or more employees. This report summarizes the findings of this study.

Contents

Outbound Email and Content Security in Today's Enterprise, 2006

The Bottom Line: Key US Findings

Fast facts from Proofpoint's May 2006 survey of 294 email decision makers at US enterprises with more than 1000 employees:

- In both the US and the UK, **more than a third of companies (38%) employ staff to read or otherwise analyze outbound email.** 44% of US companies with more than 20,000 employees do this. Additionally, 46.9% of US companies perform regular audits of outbound email content.
- US companies estimate that **more than 1 in 5 outgoing emails (22.8%) contains content that poses a legal, financial or regulatory risk.** The most common form of non-compliant content is email that contains confidential or proprietary business information.
- More than **1 in 3 US companies (34.0%) investigated a suspected email leak of confidential or proprietary information in the past 12 months.** More than 1 in 3 (36.4%) investigated a suspected violation of privacy or data protection regulations in the past 12 months.
- **More than a third (34.7%) of US companies say their business was impacted by the exposure of sensitive or embarrassing information in the last 12 months.** More than 1 in 5 (21.1%) said they had been impacted by the improper exposure of theft of customer information. 15.0% said they had been impacted by improper exposure or theft of intellectual property.
- **Nearly 1 in 3 US companies (31.6%) has terminated an employee for violating email policies in the past 12 months.** More than half (52.4%) of US companies have disciplined an employee for violating email policies in the past 12 months.
- **17.3% of US companies have disciplined an employee for violating blog or message board policies in the past 12 months.** 7.1% reported terminating an employee for such a violation.
- **10% of US publicly-traded companies investigated the exposure of material financial information (such as unannounced quarterly results) via a blog or message board posting in the past 12 months.**
- **More than 1 in 4 (25.2%) US companies were ordered by a court or regulatory body to produce employee email** in the past 12 months.
- In addition to concerns about the corporate mail system, **more than half (55.4%) of US companies are "very concerned" or "concerned" about web-based email as a conduit for exposure of confidential or proprietary information.**
- **A majority (65%) of US companies say that it is "important" or "very important" to reduce the legal and financial risks associated with outbound email in the next 12 months.**
- **A majority (60.5%) of US companies say that it is "important" or "very important" to reduce the legal and financial risks associated with outbound HTTP traffic (such as webmail and blog postings) in the next 12 months.**

The Bottom Line: Key UK Findings

Fast facts from Proofpoint's May 2006 survey of 112 email decision makers at UK enterprises with more than 1000 employees:

- In both the US and the UK, **more than a third of companies (38%) employ staff to read or otherwise analyze outbound email.** 40% of UK companies with more than 20,000 employees do this. Additionally, 61.6% of UK companies perform regular audits of outbound email content.
- UK companies estimate that **nearly 1 in 5 outgoing emails (18.1%) contains content that poses a legal, financial or regulatory risk.** The most common form of non-compliant email content is "adult, obscene or potentially offensive" content.
- More than **half of UK companies (50.9%) investigated a suspected email leak of confidential or proprietary information in the past 12 months.** Nearly 2 in 5 (39.3%) investigated a suspected violation of privacy or data protection regulations in the past 12 months.
- **More than a third (33.9%) of UK companies say their business was impacted by the exposure of sensitive or embarrassing information in the last 12 months.** 14.3% said they had been impacted by the improper exposure of theft of customer information. 15.2% said they had been impacted by improper exposure or theft of intellectual property.
- **More than 1 in 3 UK companies (33.9%) have terminated an employee for violating email policies in the past 12 months.** More than 70% of UK companies have disciplined an employee for violating email policies in the past 12 months.
- **20.5% of UK companies have disciplined an employee for violating blog or message board policies in the past 12 months.** 3.6% reported terminating an employee for such a violation.
- **13% of UK publicly-traded companies investigated the exposure of material financial information (such as unannounced quarterly results) via a blog or message board posting in the past 12 months.**
- Subpoenaing employee email in the UK is more rare: 6.3% of companies were ordered by a court or regulatory body to produce employee email in the past 12 months.
- In addition to concerns about the corporate mail system, **nearly half (49.1%) of UK companies are "very concerned" or "concerned" about web-based email as a conduit for exposure of confidential or proprietary information.**
- **A large majority (81.3%) of UK companies say that it is "important" or "very important" to reduce the legal and financial risks associated with outbound email in the next 12 months.**
- **A majority (67%) of UK companies say that it is "important" or "very important" to reduce the legal and financial risks associated with outbound HTTP traffic (such as webmail and blog postings) in the next 12 months.**

Overview

Email has emerged as 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 new 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 both internal rules, best practices for data protection and external regulations. In addition, organizations are concerned about ensuring that email (and other electronic message streams) cannot be used to disseminate confidential or proprietary information.

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 growing popularity of new electronic communication channels (such as webmail, blogs and instant messaging) pose new sources of risk for IT security professionals and the organizations they serve.

About the Study

This report summarizes findings from Proofpoint's third annual study of outbound email security and content compliance 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 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.

In previous years, this study looked at only large enterprises in the US. In the 2006 study, Proofpoint also surveyed large enterprises based in the UK. Additionally, some new questions were posed to explore concerns about increasingly popular communications mediums including web-based email (webmail) and blogs.

Proofpoint, Inc. commissioned Forrester Consulting to field an online survey of email decision makers at large US and UK enterprises. Respondents were asked about their concerns, priorities and plans related to the content of email leaving their organizations. Forrester gathered 294 responses from US companies with 1,000 or more employees and 112 responses from UK companies with 1,000 or more employees. Respondents were qualified based on their knowledge of their company's email and messaging technologies. The same survey questions were fielded to both US and UK respondents.

Concerns about Outbound Email Compliance and Security

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. As in previous years, the survey asked about level of concern around seven different outbound email topics. The phrasing of some questions was modified slightly this year to make the questions relevant to both US and UK survey respondents:

Complying with internal email policies

Respondents were asked to rate their level of concern around "ensuring that outbound email complies 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 (for example, in compliance with best practices or regulations such as HIPAA in the US and the Data Protection Act in the UK)."

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 (for example, in compliance with best practices or regulations such as Gramm-Leach-Bliley in the US and the Data Protection Act in the UK).”

Complying with financial disclosure and corporate governance regulations and guidelines

Respondents were asked to rate their level of concern around “ensuring compliance with financial disclosure or corporate governance regulations (such as Sarbanes-Oxley, SEC regulations, NASD regulations, UK Companies Act, etc.).”

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 outside the organization.”

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 in the US

Though the top concerns vary by geography, both US and UK respondents showed a high level of concern in all seven areas. Figure 1 shows the percentage of US respondents who reported being “very concerned” or “concerned” about each of the topic areas for this year’s survey (2006) last year’s survey (2005, which gathered 332 responses and 2004 (which gathered 140 responses). Respondents demonstrated a high level of concern across all categories—in each one, more than half of all respondents reported being “concerned” or “very concerned.”

This year, protecting personal identity/financial privacy information was the area of most concern, with 71.1% of respondents reporting that they are “concerned” or “very concerned.” Ensuring compliance with financial disclosure/corporate governance regulations was a close second with 68.0% of US respondents reporting that they are “concerned” or “very concerned” about this category. As shown in Figure 1, roughly two-thirds of respondents shared the same level of concern around preventing leaks of confidential internal memos, protecting the confidentiality of private healthcare information in email and ensuring that email cannot be used to disseminate company trade secrets or valuable intellectual property. Though it is hard to make a “scientific” comparison from year-to-year (because of differences in the size and makeup of the survey sample), concerns about protecting healthcare privacy seem to be steadily increasing. It’s also worth noting that, in this year’s responses, concerns about defending against trade secret and intellectual property leaks are somewhat lower than last year (when it was the number one concern).

Top Outbound Email Concerns in the UK

This is the first year in which Proofpoint surveyed UK companies. Overall, the level of concern expressed by UK respondents was lower than that expressed by their counterparts in the US. However, for all but one category (protecting the confidentiality of private healthcare information in email), more than half of all respondents reported being “concerned” or “very concerned.” Figure 2 compares results from UK and US respondents.

The top concerns in UK were protecting the confidentiality of personal identity/financial information in email (67.9% reporting “concerned” or “very concerned”), followed by ensuring that email cannot be used to disseminate company trade secrets or valuable intellectual property (64.3%). 60.7% of respondents reported a high level of concern about ensuring that email cannot be used to disseminate confidential internal memos. Roughly half of all UK respondents expressed a high level of concern about monitoring email for offensive or otherwise inappropriate content and attachments (50.9%), ensuring compliance with financial disclosure or corporate governance regulations (50.0%) and ensuring compliance with internal corporate email policies (50.0%).

Outbound Email Concerns, US 2006, 2005 and 2004

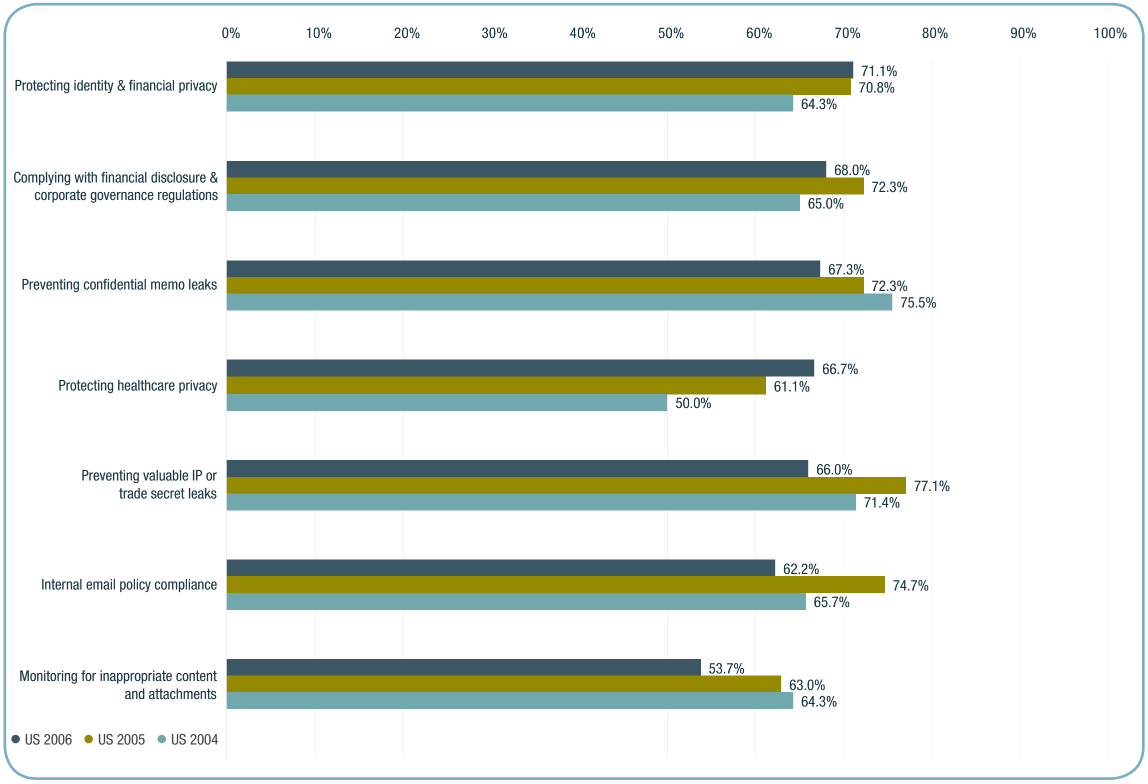

Figure 1: Percentage of US respondents who reported being "concerned" or "very concerned" about various outbound email compliance issues, 2004-2006 results compared.

Outbound Email Concerns, UK and US Compared, 2006

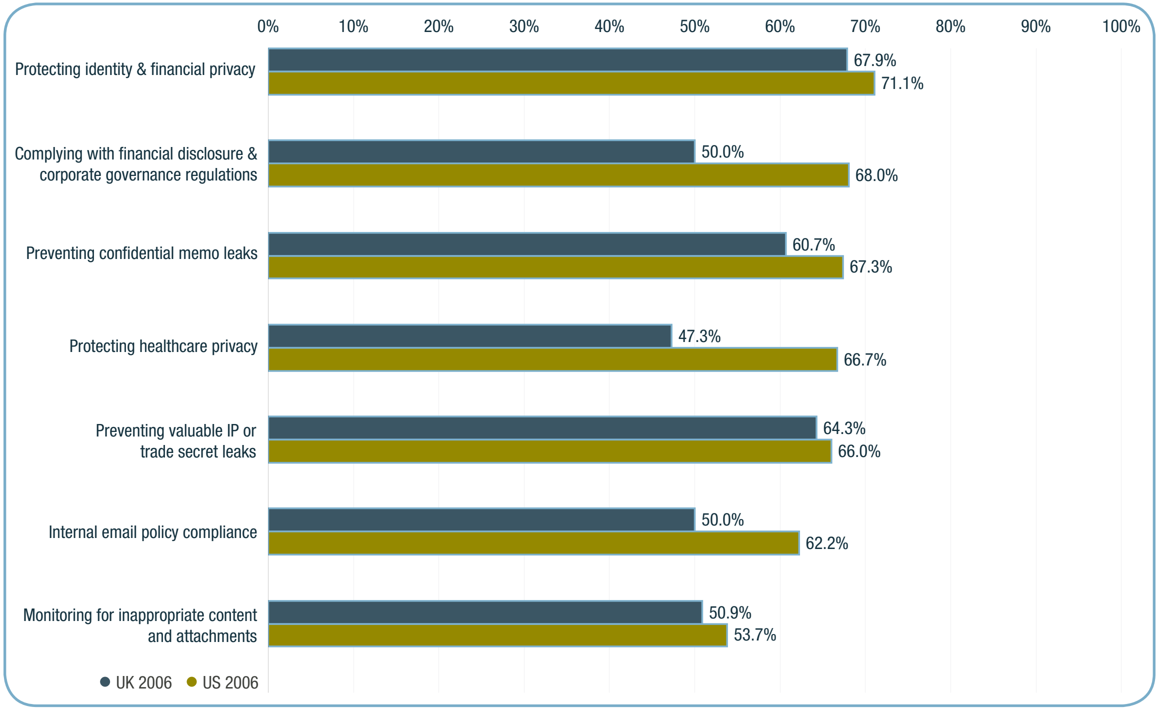

Figure 2: Percentage of UK and US respondents who reported being "concerned" or "very concerned" about various outbound email compliance issues.

The relatively large disparities between UK and US concerns around the "corporate governance" and "healthcare privacy" topics might be explained by the fact that there are specific regulations in the US (Sarbanes-Oxley and HIPAA, respectively) that apply to a large number of US companies while the UK regulatory environment is more focused on protecting personal identify information.

The lower level of *concern* expressed by UK respondents is also interesting in light of the fact that they expressed a higher level of *urgency* than their US counterparts when asked about the importance of reducing outbound email and outbound HTTP risks in the next 12 months. (See "Importance of Reducing Outbound Email Risks" and "Importance of Reducing Outbound HTTP Content Risks" at the end of this report.)

It should also be kept in mind when comparing UK versus US responses that, while the same questions were fielded to both UK and US respondents, the sample sizes (294 US companies versus 112 UK companies) and industry groupings (see appendix) were different.

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 what is the most common form of inappropriate content found in non-compliant email messages leaving their organization. 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 Form of Inappropriate Content in Non-compliant Email

Answers to the first question, "In non-compliant email messages leaving your organization, what is the most common form of inappropriate content?" were reported in the US as follows:

- **27.6%** Confidential or proprietary business information about your organization
- **26.2%** Adult, obscene or potentially offensive content
- **22.8%** Personal healthcare, financial or identity data which may violate privacy and data protection regulations
- **15.3%** Valuable intellectual property or trade secrets which should not leave the organization
- **8.2%** Don't know

Answers to this question were rather different in the UK, with a clear majority of respondents estimating that offensive content is the most common form of risky email. UK responses were as follows:

- **46.4%** Adult, obscene or potentially offensive content
- **25.0%** Confidential or proprietary business information about your organization
- **15.2%** Personal healthcare, financial or identity data which may violate privacy and data protection regulations
- **9.8%** Valuable intellectual property or trade secrets which should not leave the organization
- **3.6%** Don't know

More than 1 in 5 Outbound Emails 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 answer for all respondents was that 21.4% of outbound email poses a risk. US respondents estimated the percentage of risky outbound email slightly higher (22.8%) than UK respondents (18.1%).

Not all survey respondents provided an estimate in answer to this question. In the US, 30.6% of respondents said they didn't know. In the UK, 21.4% of respondents said they didn't know. This result is consistent with Proofpoint's experiences in working with large organizations to mitigate outbound email risks. Though most organizations are extremely concerned about outbound email risks, many have no quantifiable measures about the magnitude of the risks that they face.

Email Encryption Issues

Respondents were also asked to estimate “what percentage of outbound emails that *should* be encrypted are actually being *sent* in encrypted form?” The mean response from all respondents was 51.4%. In the US, respondents estimated that less than half (49.4%) of email that should be encrypted is actually sent in encrypted form. In the UK, respondents estimated that slightly more than half (56.5%) of email that should be encrypted is actually sent in encrypted form.

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. Though companies are clearly concerned about these risks, the results show a relatively low rate of adoption for technology solutions related to outbound email content screening and compliance (though adoption of most technologies is increasing in the US, compared to previous years). At the same time, manual processes—such as conducting regular audits of outbound email content and employing staff to read outbound email—are still surprisingly common.

Figure 3 shows the techniques and technologies the survey asked about and the percentage of companies that have already deployed each. Figure 4 shows the same information, but only for those companies with more than 20,000 employees.

Adoption of Techniques & Technologies to Mitigate Outbound Messaging Risks, All Companies, UK and US, 2006

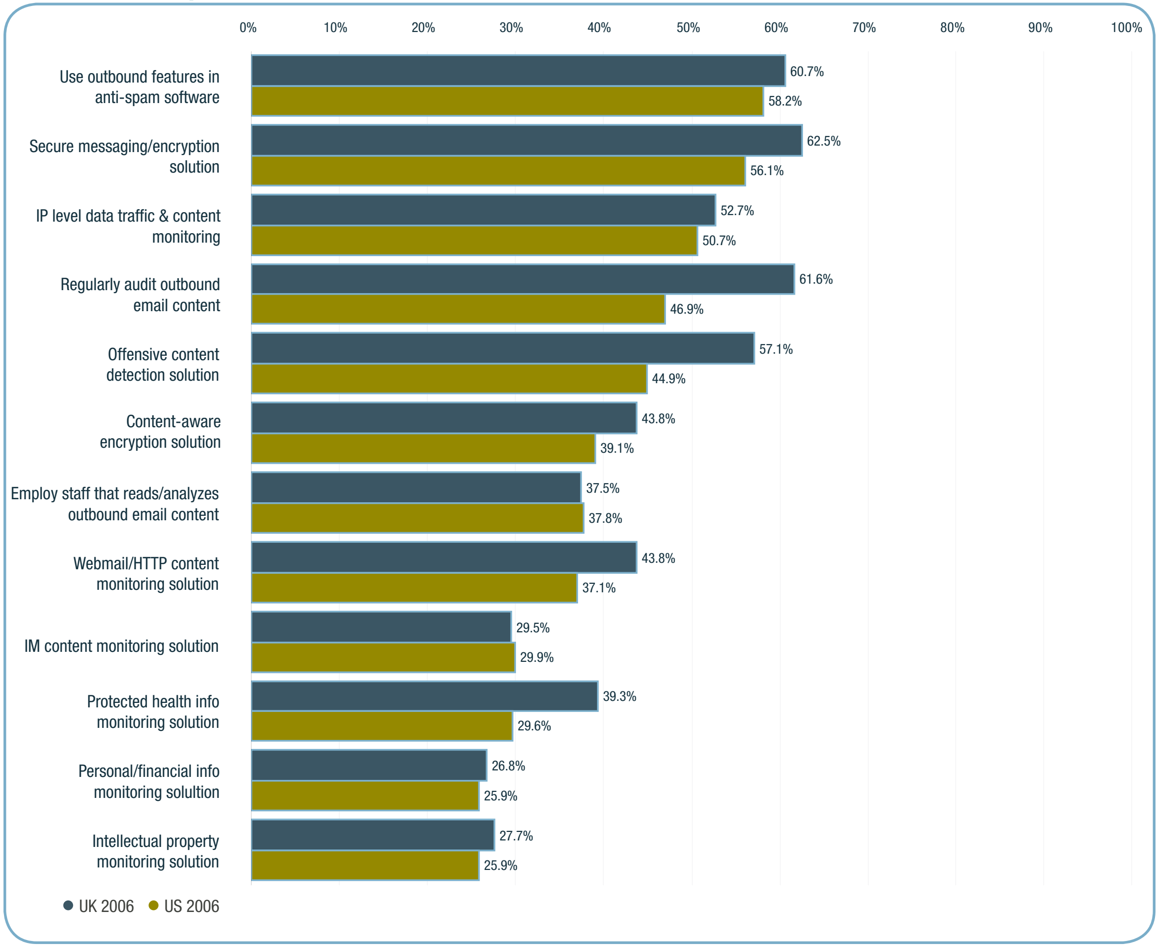

Figure 3: Percentage of UK and US respondents who report having deployed or used various techniques and technologies for mitigating messaging-related risks—data from all companies.

They're (Still) Reading Your Email

As in 2005 and 2004, one of the most surprising results of the survey was the high percentage of organizations that reported they employ staff to read or otherwise monitor outbound email content (see Figures 3 and 4). These numbers have remained remarkably consistent from year to year (e.g., in 2005, 36.1% of companies said they employed staff to read outbound email) and, in this year's survey, it can be seen that UK enterprises are just as likely to use them as US enterprises.

Out of all respondents (both US and UK), more than a third—37.7%—reported that they employ staff to monitor (read or otherwise analyze) outbound email. An additional 26.3% of companies said that they intend to deploy such staff in the future. Even more companies—51.0%—conduct regular audits of outbound email content.

Broken out by geography, 37.8% of US companies and 37.5% of UK companies employ staff to monitor the content of outbound email. An additional 23.8% of US companies and 33.0% of UK companies said that they intend to deploy such staff in the future.

In the US, 46.9% of companies say they regularly audit outbound email content. In the UK, this technique is even more prevalent, with 61.6% of companies saying they regularly audit outbound email content.

These techniques are even more prevalent in large organizations—44.2% of US companies and 40.6% of UK companies with more than 20,000 employees employ staff to monitor outbound email. Of these companies, another 18.8% (US) and 31.3% (UK) said they intend to deploy such staff in the future. Nearly half of the largest US companies (47.8%) reported and more than two-thirds of the largest UK companies (68.8%) said that they conduct regular audits of outbound email content.

Adoption of Technology Solutions for Mitigating Outbound Messaging Risks

In addition to the manual processes described above, the survey asked respondents about their deployment plans for a variety of outbound email compliance technologies. See again Figures 3 and 4. In general, large companies are more likely to have deployed these 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.

Use of outbound features in anti-spam solutions

More than half of surveyed US companies (58.2%) and UK companies (60.7%) said that they use the outbound email compliance or monitoring features included in anti-spam software. Depending upon the anti-spam software deployed, these features may be rudimentary (e.g., enforcing maximum attachment sizes) or more sophisticated (e.g., detecting certain keywords or information patterns, such as social security numbers).

Adoption of secure messaging and content-aware encryption

Secure messaging (encryption) systems are also a popular technology, with 56.1% of US and 62.5% of UK companies reporting that they have deployed a technology solution for secure or encrypted messaging. Such systems are commonly used to encrypt sensitive content (such as protected health information or financial data) for transmission via email.

The 2005 survey also asked respondents if they had deployed a "technology solution for automatic encryption of messages based on message contents." 39.1% of US and 43.8% of UK companies said they had deployed such a system. Content-aware encryption solutions are commonly used for compliance with data protection regulations such as HIPAA (which specifies that private healthcare information cannot be transmitted in an unencrypted form).

Internet Protocol monitoring

More than half of both US (50.7%) and UK (52.7%) companies said that they have deployed a technology solution for monitoring data traffic and content at the Internet Protocol (IP) level.

Adoption of Techniques & Technologies to Mitigate Outbound Email Risks, Companies with 20K+ Employees, US and UK, 2006

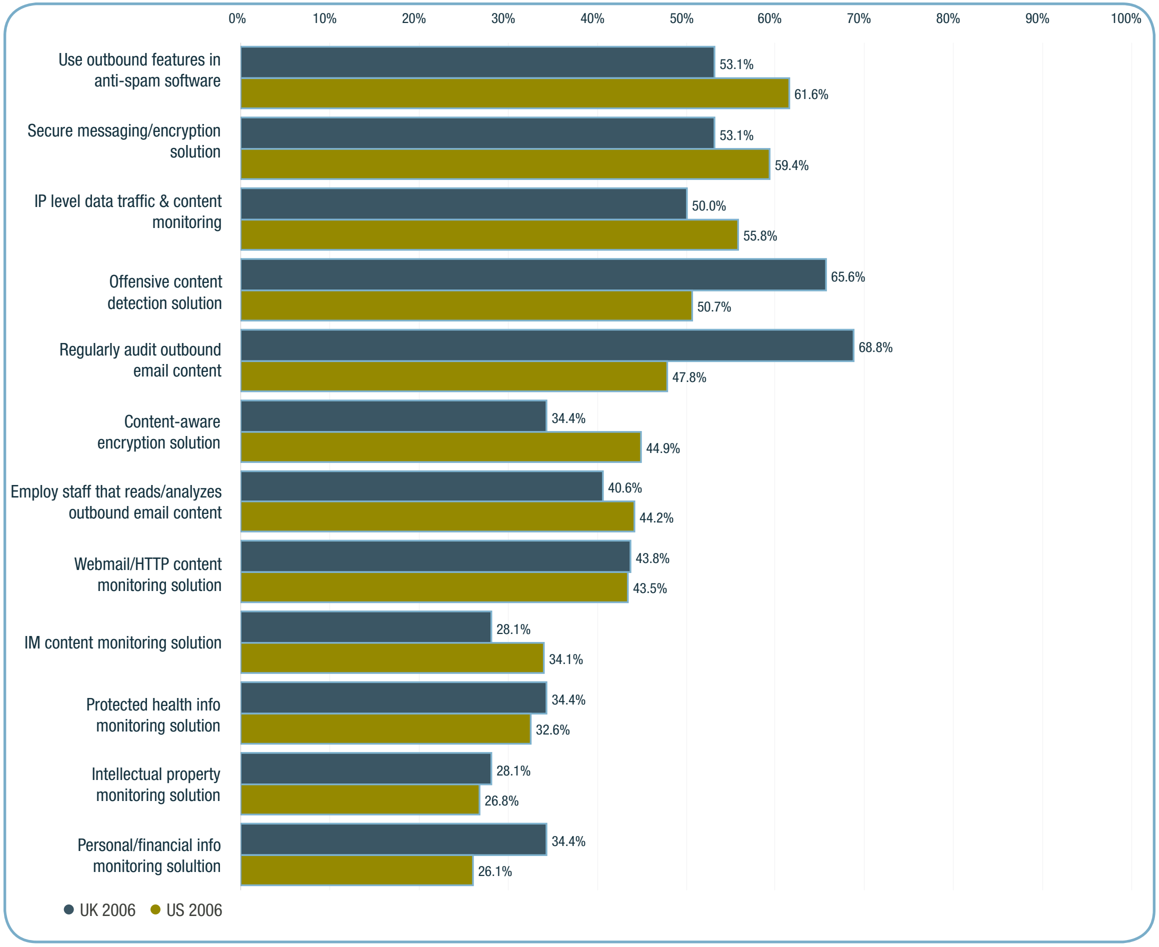

Figure 4: Percentage of UK and US respondents who report having deployed or used various techniques and technologies for mitigating messaging-related risks—data from companies with 20,000 or more employees.

Various compliance solutions

44.9% of US and 57.1% of UK respondents said they have deployed technology for detecting vulgar or offensive content in outbound email. 29.6% of US and 39.3% of UK companies said they had deployed a technology solution for detecting protected health information in outbound email. About a quarter of respondents (25.9% in the US, 26.8% in the UK) said they had deployed technology for detecting personal financial information in outbound email. About a quarter of respondents (25.9% in the US, 27.7% in the UK) said they have deployed technology for detecting intellectual property in outbound email.

Webmail monitoring

More than a third of companies (37.1% in the US, 43.8% in the UK) said they had deployed a technology solution for monitoring content in webmail (i.e., HTTP email services such as Hotmail, Gmail, etc.) or other forms of HTTP traffic. Another 23.8% of US and 25.0% of UK respondents said that they intend to deploy such technology in the next 12 months.

IM monitoring

More than a quarter (29.9% in the US, 29.5% in the UK) respondents said they had deployed a technology solution for monitoring content in Instant Messaging traffic. Another 21.4% of US and 30.4% of UK respondents said that they intend to deploy such technology in the next 12 months.

Other Conduits for Exposure of Confidential Information

Though this survey primarily explored concerns about the corporate email system, email is not the only technology that poses a potential risk to organizations. Other communication 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 and proprietary information. The findings are summarized in Figure 5.

In the 2006 survey results, US companies reported a lower (but still significant) level of concern about these protocols than they did in 2005. In 2005, more than 50% of US respondents reported being “concerned” or “very concerned” about each of the 5 different data streams (web-based email, IM, FTP, blog/message board postings and P2P networks). In 2006, each category was rated as a concern by more than 40% of US respondents.

This year, roughly half of companies in the US (55.4%) and UK (49.1%) said they were “concerned” or “very concerned” about web-based email as a conduit for the exposure of confidential information. Nearly half of US companies (48.0%) and more than a third of UK companies (34.8%) expressed a high level of concern about FTP. Concerns about Instant Messaging (IM) applications were high for 47.3% of US and 38.4% of UK companies. Peer-to-peer networks were a concern for 44.6% of US and 34.8% of UK companies.

See Figure 5 for a comparison of US and UK results.

Level of Concern Around Other Potential Conduits for Exposure of Confidential Info, US and UK, 2006

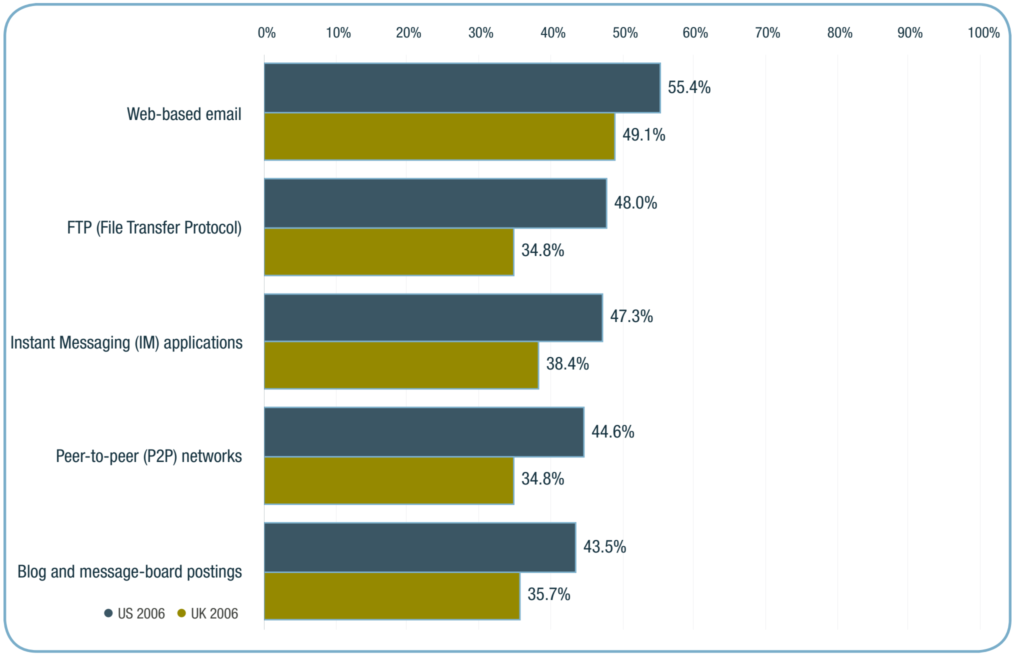

Figure 5: Percentage of US and UK respondents who reported being “concerned” or “very concerned” about other conduits (besides SMTP email) for the exposure of confidential info.

Implementation of Email-related Security Policies, US and UK, 2006

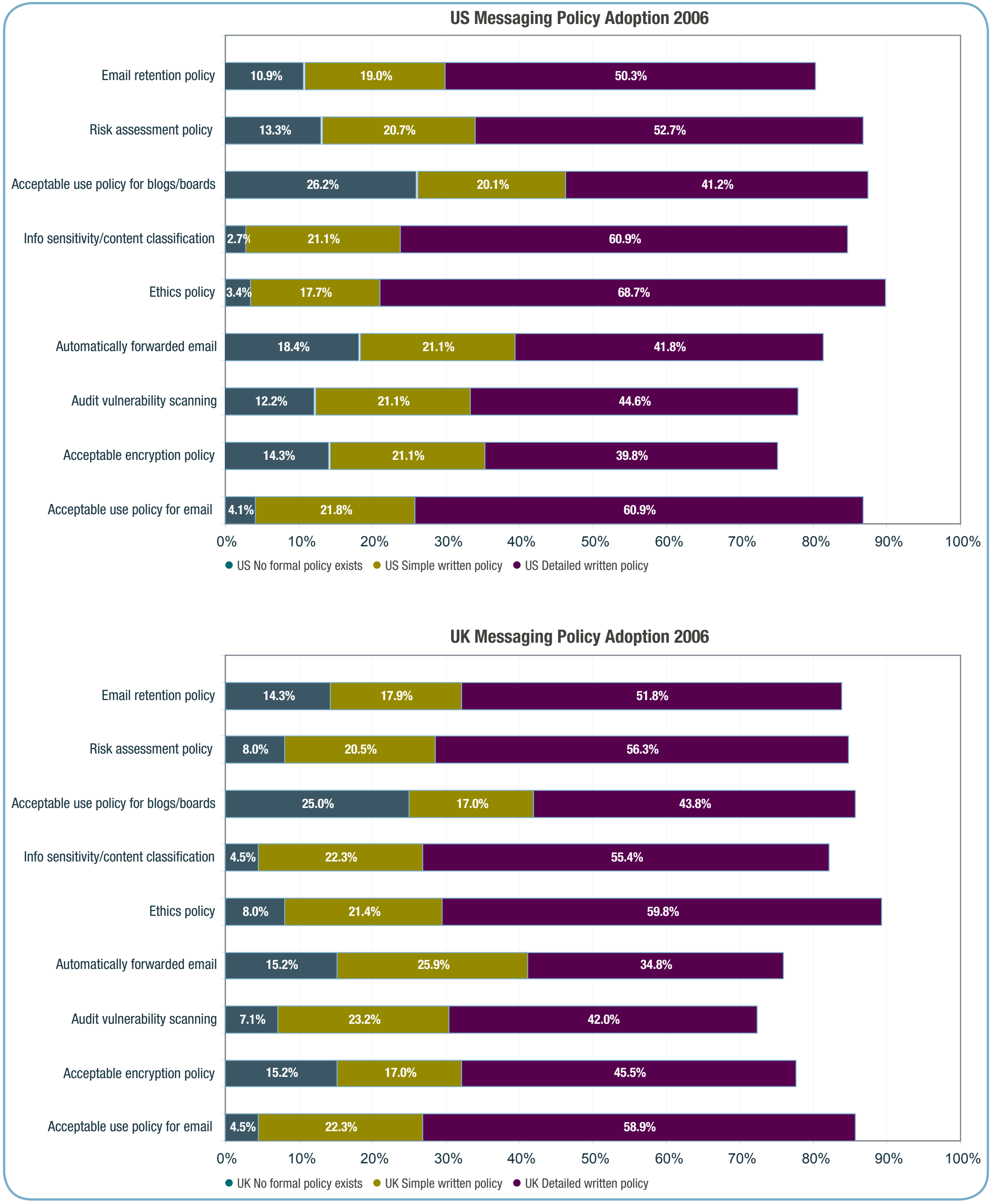

Figure 6: Implementation of various messaging-related policies—data from all US and UK companies.

The Messaging Policy Environment in Today's Enterprise

An important part of mitigating outbound email 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, respondents were asked, "at what stage is your organization in defining, implementing and enforcing" nine different email-related policies. The responses are summarized in Figure 6, on the previous page. 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) or a detailed written policy (e.g., a separate policy document):

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. 82.7% of US and 81.3% of UK companies reported having a simple or detailed written policy.

Acceptable use policy for blog and/or message board postings

A policy that defines appropriate uses of internal and external web log or message board systems and may include personal use policies, confidentiality rules, monitoring and privacy policies, etc. 61.2% of US and 60.7% of UK companies reported having a simple or detailed written policy.

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. 65.6% of US and 65.2% of UK companies reported having a simple or detailed written policy.

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 HIPAA, which include encryption requirements. 60.9% of US and 62.5% of UK companies reported having a simple or detailed written policy.

Automatically forwarded email policy

A policy that governs the automatic forwarding of email to external destinations. 62.9% of US and 60.7% of UK companies reported having a simple or detailed written policy.

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. 86.4% of US and 81.3% of UK companies reported having a simple or detailed written 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. 82.0% of US and 77.7% of UK companies reported having a simple or detailed written 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. 73.5% of US and 76.8% of UK companies reported having a simple or detailed written policy.

Email retention policy

A policy that defines what information sent or received by email should be retained and for how long. In certain highly-regulated industries, email retention is required by law. 69.4% of US and 69.6% of UK companies reported having a simple or detailed written policy.

Policy Enforcement and Investigations of Suspected Violations

More interesting than the implementation of various policies are the actions that companies have taken to educate employees about email-related policies as well as actions taken to enforce policy violations. Survey respondents were asked whether their organization had experienced twelve different policy enforcement-related events in the past 12 months.

Responses are summarized in Figure 7, on the page 13. Figure 7 shows the responses for both US and UK companies, broken out by company size (companies with 20,000 or more employees versus companies with 1000 to 20,000 employees). In the text below, aggregate responses from all US and UK companies are also reported.

Formal Policy Training

Companies were asked if they had conducted formal training for employees about the organizations email security policies or about external regulations that apply to the organization's use of email.

- **Email security policy training:** Just over half of US organizations (50.7%) and more than half of UK organizations (62.5%) had conducted a formal training on email security policies in the past 12 months. Large organizations (those with more than 20,000 employees) were more likely to have conducted such training sessions (see Figure 7).

- **Email regulation training:** 38.4% of US and 33.9% of UK organizations formally trained employees about external regulations that apply to that organization's use of email. In the US, large organizations were more likely to have conducted such training, though the opposite held true in the UK.

Discipline and Termination of Employees for Violating Email Policies

More than half of US respondents (52.4%) said their organization had disciplined an employee for violating email policies in the past 12 months. UK companies were even more likely to have disciplined an employee for violating email policies—70.5% reported doing so.

About one third of respondents (31.6% in the US and 33.9% in the UK) said their organization had terminated an employee for violating email policies in the past 12 months. As shown in Figure 7, companies of all sizes reported this at roughly the same frequency.

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

One of the new questions for 2006, companies were asked if they had disciplined or terminated an employee for violating the company's blog/message board policies in the past 12 months. In the US, 17.3% of organizations had disciplined an employee for violating such policies. In the UK, more than 1 in 5 (20.5%) companies had disciplined an employee for violating such policies.

Terminations were more rare. In the US, 7.1% of respondents said their company had terminated an employee for violating the blog/message board policies in the past 12 months. In the UK, just 3.6% had done so.

Investigation of Compliance Violations and Leaks of Confidential Information

Companies are justifiably concerned about outbound email content, based on the large number that say they have investigated regulatory compliance violations or leaks of confidential information via email in the past 12 months:

Leaks of Confidential Information

More than a third of companies in the US (34.0%) and more than half of companies in the UK (50.9%) report that they investigated a suspected leak of confidential or proprietary information via email in the past 12 months. In the US, the largest companies reported more such leaks—39.1% of companies with more than 20,000 employees versus 29.5% of companies with 1000 to 20,000 employees. In the UK, the largest companies reported a smaller number of leaks—46.9% of companies with more than 20,000 employees versus 52.5% of companies with 1000 to 20,000 employees.

Potential Violations of Privacy and Data Protection Regulations

More than a third of companies—36.4% of US companies and 39.3% of UK companies—report that they investigated a suspected violation of privacy or data protection regulations related to email in the past 12 months. In both countries, the largest companies reported more violations—39.1% of US and 40.6% of UK companies with more than 20,000 employees, versus 34.0% of US and 38.8% of UK companies with 1,000 to 20,000 employees.

Leaks of Confidential Information Via Blog or Message Board Postings

Blogs and message board postings were reported as a significant source of risk. More than one quarter (25.9%) of US companies had investigated the exposure of confidential, sensitive or private information via a blog or message board posting in the past 12 months. In the UK, 18.8% of companies reported such an investigation. In the US, the largest companies were more likely to investigate blog- or message board-related leaks (29.0% of companies with more than 20,000 employees versus 23.1% of smaller companies). In the UK, rates for large and small companies were the same (18.8% in both cases).

Exposure of Material Information 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." Overall, nearly 1 in 10 companies (9.2% in the US and 9.8% in the UK) reported such an investigation.

This question was primarily aimed at publicly-traded companies (who are most concerned with protecting "material" financial information). As expected, public companies were more likely to report these types of investigations. 9.9% of public companies in the US and 12.9% of public companies in the UK report that they investigated the exposure of material financial information via a blog or message board.

Leaks of Confidential Information Via Communications with Third-party Vendors or Outsourcing Providers

Respondents were asked if, in the past 12 months, they had investigated the exposure of confidential, sensitive or private information by a third-party vendor or outsourcing firm with whom they share such data. In the US, 17.7% of companies investigated such leaks. In the UK, more than 1 in 5 (23.2%) of companies reported conducting such an investigation.

Litigation Concerns

Respondents were asked if, in the past 12 months, their organization had been ordered to produce employee email by a court or other regulatory body (i.e., had employee email been subpoenaed in the past 12 months). In the US, more than one quarter (25.2%) of organizations reported having to produce employee email in the past year. This number was up substantially over 2005, where 10.5% of US organizations reported such an event.

Subpoenas of employee email are much less common in the UK, where just 6.3% of companies reported such an event in the past 12 months.

Which of the Following Did Your Organization Experience in the Last 12 Months? US and UK by Company Size, 2006

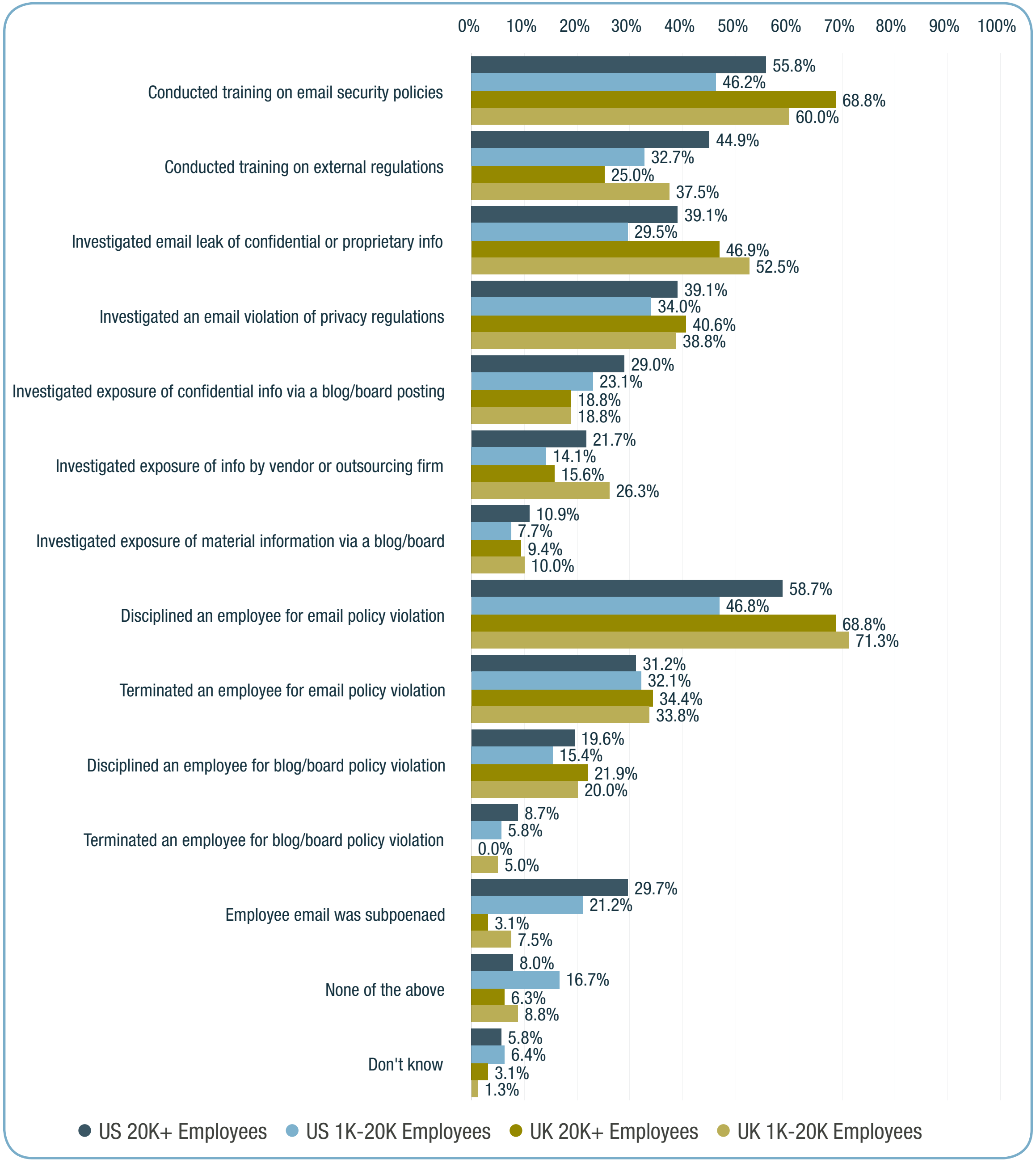

Figure 7: Percentage of US respondents who reported being “concerned” or “very concerned about various outbound email compliance issues, 2004-2006 results compared.

Exposure and Theft of Sensitive Information

In addition to the questions about *investigations* of various content security breaches, respondents were asked if their business had been impacted by the exposure or theft of different types of information.

Improper Exposure or Theft of Customer Information

More than 1 in 5 US companies (21.1%) and 14.3% of UK companies reported that their business had been impacted by the improper exposure or theft of customer information in the past 12 months.

Improper Exposure or Theft of Intellectual Property

About 15% of companies (15.0% US, 15.2% UK) reported that their business had been impacted by the improper exposure or theft of intellectual property in the past 12 months.

Exposure of Sensitive or Embarrassing Information

More than one third of companies (34.7% US, 33.9% UK) reported that their business had been impacted by the exposure of sensitive or embarrassing information in the past 12 months.

Importance of Reducing Outbound Email Content Risks

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?"

- **US:** 65.0% of US respondents 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. This number increased over 2005, where 57.8% of US companies said that such reductions were "important" or "very important."

- **UK:** Organizations in the UK feel an even greater sense of urgency. 81.3% of respondents 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. This finding is especially interesting in light of the lower level of concern that UK respondents expressed about the various outbound email topics (see "Top Outbound Email Concerns in the UK" on page 2).

Figure 8, below, shows the breakout of responses to this question.

Importance of Reducing Legal and Financial Risks Associated with Outbound Email in the Next 12 Months

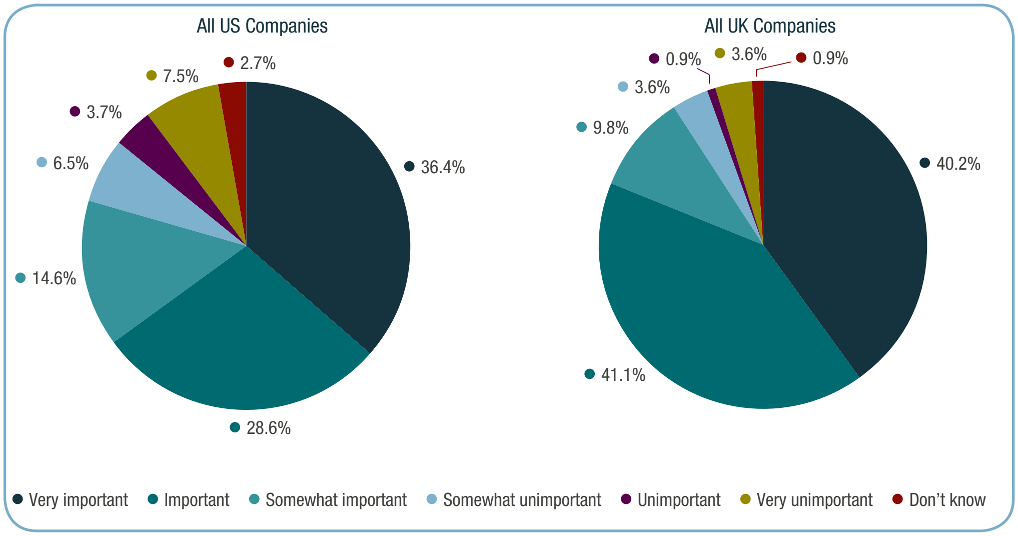

Figure 8: Importance of reducing the legal and financial risks associated with outbound email in the next 12 months, US and UK responses.

Importance of Reducing Outbound HTTP Content Risks

New for 2006, 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?”

- **US:** 60.5% of US respondents 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.

- **UK:** Organizations in the UK felt a slightly higher sense of urgency. 67.0% of respondents 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.

Figure 9, below, shows the breakout of responses to this question.

Importance of Reducing Legal and Financial Risks Associated with Outbound HTTP Content in the Next 12 Months, US and UK, 2006

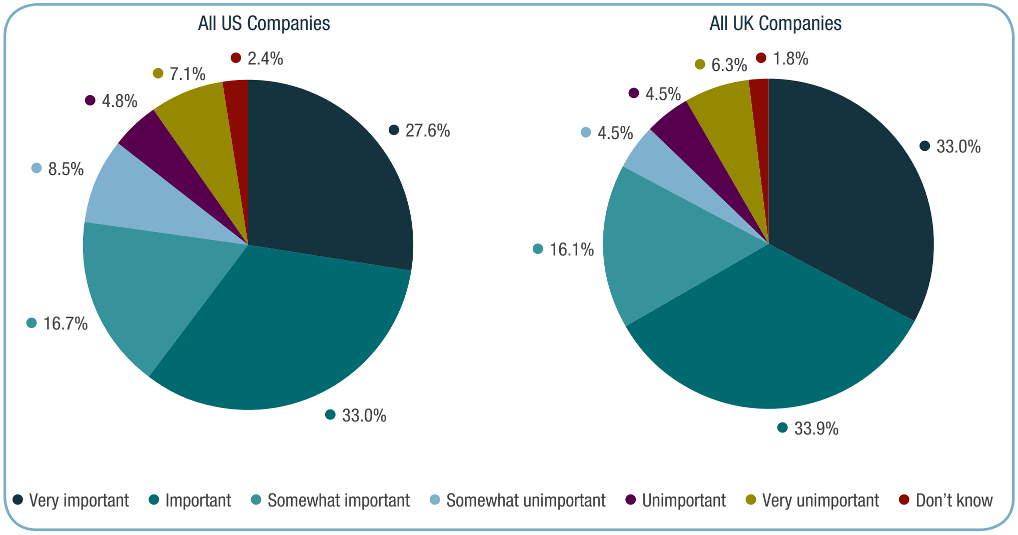

Figure 9: Importance of reducing the legal and financial risks associated with outbound HTTP traffic (such as webmail and blog postings) in the next 12 months, US and UK responses.

Appendix: Respondent Demographics

Respondent Titles

The 294 US and 112 UK respondents to this survey represented a wide variety of IT decision makers including respondents with the following titles:

Title	US	UK
CIO, CTO, or senior-most IT executive	9.9%	9.8%
CSO, CISO, or senior-most IT security executive	2.4%	2.7%
VP or executive of IT	10.9%	13.4%
VP or executive of security	1.4%	1.8%
Director or manager of IT	53.7%	55.4%
Director or manager of security	4.4%	2.7%
CFO, CEO, COO	4.4%	1.8%
Compliance or legal officer, or council	2.0%	0.9%
Senior finance executive	4.8%	1.8%
Senior human resource executive	2.0%	7.1%
Director or manager of messaging / email systems	4.1%	2.7%

Respondent Company Sizes

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

Size Category	US	UK
1,000 to less than 5,000	25.5%	34.8%
5,000 to less than 20,000	27.6%	36.6%
20,000 or more	46.9%	28.6%

Ownership Category	US	UK
Publicly traded	61.6%	55.4%
Privately held	38.4%	44.6%

Respondent Company Industries

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

Industry Group	US	UK
Primary production & raw materials manufacturing	2.4%	5.4%
Consumer products manufacturing	8.5%	5.4%
Chemical & petroleum manufacturing	1.0%	3.6%
Pharma/biotech manufacturing	6.5%	2.7%
High-tech products manufacturing	9.5%	5.4%
Industrial products manufacturing	4.1%	3.6%
Retail	5.1%	11.6%
Wholesale	2.4%	0.9%
Transportation and logistics	4.1%	4.5%
Professional services (consulting, legal, etc.)	9.2%	8.0%
Construction and engineering	0.7%	4.5%
Media, entertainment, and leisure	3.7%	1.8%
Utilities	1.0%	1.8%
Telecom carriers	4.4%	7.1%
Financial services	9.2%	8.0%
Insurance	1.7%	4.5%
Government	11.2%	4.5%
Higher education	6.5%	4.5%
Healthcare	7.5%	8.0%
Non-profit / other public services	1.4%	4.5%

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 Security and Content Compliance Research

The summaries of Proofpoint's prior annual surveys of Outbound Email Security and Content Compliance in Today's Enterprise, can be downloaded from the following URLs:

http://www.proofpoint.com/outbound2005

http://www.proofpoint.com/outbound2004

Email Confidential: Are Your Secrets Safe?

Discusses the financial and legal risks associated with leaks of confidential information and valuable intellectual property and outlines a process for implementing and enforcing policies that can keep valuable information secure:

http://www.proofpoint.com/confidential

Best Practices in Messaging Security

Discusses the increasing number of healthcare and financial privacy regulations and how they impact email systems:

http://www.proofpoint.com/regulatory

Encryption Made Easy

Discusses the development of encrypted messaging systems and the unique advantages of Proofpoint's secure messaging solution:

http://www.proofpoint.com/encryptionwp

About Proofpoint, Inc.

Proofpoint provides messaging security solutions for large enterprises to stop spam, protect against email viruses, ensure compliance with corporate policies and regulations and defend against leaks of confidential and proprietary information via email and other message streams. The company's flagship products, the Proofpoint Messaging Security Gateway™ and Proofpoint Protection Server® provide future-proof messaging security using Proofpoint MLX™ technology, an advanced machine learning system developed by Proofpoint scientists and engineers.

Proofpoint Solutions for Outbound Email Content Security and Regulatory Compliance

Proofpoint's software and appliance-based messaging security solutions 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 Content Compliance™ 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 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 and GLBA. 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. Proofpoint's Dynamic Update Service™ ensures that your compliance dictionaries and rules are always up to date.

Enabling Content-aware Encryption

The Proofpoint Secure Messaging™ module makes ad hoc, secure communication just as easy as traditional, non-encrypted messaging. Proofpoint's powerful, policy-driven encryption features mitigate the risks associated with regulatory violations, data loss and corporate policy violations, without adversely impacting business operations. Proofpoint Secure Messaging is ideal for organizations in the healthcare, financial services, government and other sectors that need to protect sensitive data, while still making it readily available to appropriate affiliates, business partners and end users.

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 easy-to-deploy appliance 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. When such breaches are detected, the Proofpoint Network Content Sentry—working in concert with Proofpoint Protection Server software or the Proofpoint Messaging Security Gateway appliance—actively alerts managers (such as compliance officers) so appropriate actions can be taken.

For More Information

Proofpoint, Inc. US
10201 Torre Avenue
Suite 100
Cupertino, CA 95014
USA
P 408 517 4710
F 408 517 4711
E info@proofpoint.com
www.proofpoint.com

Proofpoint, Inc. EMEA
Atlantic House
Imperial Way
Reading
RG2 0TD
United Kingdom
P +44 118 903 6046
F +44 118 903 6100
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. APAC
56 Berry Street
North Sydney
NSW 2060
Australia
P +61 02 9455 0289
F +61 02 9455 0001
E info@proofpoint.com
www.proofpoint.com