proofpoint™

Outbound Email and Data Loss Prevention in Today's Enterprise, 2008

Results from a survey by Proofpoint, Inc. fielded by Forrester Consulting on outbound messaging and content security issues May, 2008

On behalf of Proofpoint, Inc., Forrester Consulting fielded an online survey of email decision makers at large US, UK, German, French and Australian companies. 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, media sharing sites and other electronic communications technologies.

Forrester gathered a total of 424 responses from companies with 1,000 or more employees, including 301 US, 32 UK, 30 German, 31 French and 30 Australian companies. This report summarizes the findings of the 2008 study.

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

http://www.proofpoint.com/outbound

Contents

The Bottom Line: Key Findings, US 2008

Fast facts from Proofpoint's *Outbound Email and Data Loss Prevention in Today's Enterprise, 2008* report, based on a March 2008 study of 301 email decision makers at US enterprises with more than 1000 employees:

○ **41% of US companies with 20,000 or more employees surveyed employ staff to read or otherwise analyze outbound email.** Overall, more than one quarter (29%) of US companies surveyed employ such staff.

○ **22% 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, 15% of companies surveyed said they employ such staff.

○ **More than 1 in 3 (38.0%) US companies surveyed perform regular audits of outbound email content.**

○ **44% of US companies investigated a suspected email leak of confidential or proprietary information in the past 12 months.** 40% investigated a suspected violation of privacy or data protection regulations in the past 12 months.

○ **23% of US companies surveyed say their business was impacted by the exposure of sensitive or embarrassing information in the last 12 months.** 18% said they had been impacted by improper exposure or theft of customer information. 14% said they had been impacted by the improper exposure or theft of intellectual property.

○ **More than a quarter of US companies surveyed (26%) 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.

○ **More than a quarter of US companies surveyed (27%) investigated the exposure of confidential, sensitive or private information via lost or stolen mobile devices in the past 12 months.** 56% of respondents are concerned or very concerned about the risk of information leakage via email sent from mobile devices. Companies said that, on average, one quarter of their employees have mobile access to the corporate email system via smartphones or other wireless handheld devices.

○ **More than 1 in 5 US companies surveyed (21%) investigated the exposure of confidential, sensitive or private information via a blog or message board posting.** 11% disciplined an employee for violating blog or message board policies in the past 12 months. 6% reported terminating an employee for such a violation. 44% are concerned or very concerned about the risk of information leakage via blogs and message board postings.

○ **12% of US companies investigated the exposure of confidential, sensitive or private information via video or audio media posted to a media sharing site.** 14% have disciplined an employee for violating media sharing/posting policies in the past 12 months. 5% reported terminating an employee for such a violation. 44% are concerned or very concerned about the risk of information leakage via media sharing sites.

○ **12% of US companies investigated the exposure of confidential, sensitive or private information via a posting to a social networking site.** 13% have disciplined an employee for violating social networking policies in the past 12 months. 4% reported terminating an employee for such a violation. 44% are concerned or very concerned about the risk of information leakage via posts to social networking sites.

○ **14% of US publicly-traded companies surveyed 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 a third (34%) of companies surveyed with 20,000 employees reported that employee email was subpoenaed in the last 12 months.** Overall, nearly a quarter (24%) of companies surveyed 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 of US companies surveyed (56%) are "very concerned" or "concerned" about web-based email as a conduit for exposure of confidential or proprietary information.**

○ **Top concerns 2008:** 75% of US companies are "concerned" or "very concerned" about protecting the confidentiality of personal identity and financial information in outbound email. 70% are "concerned" or "very concerned" about ensuring compliance with financial disclosure or corporate governance regulations. 68% are "concerned" or "very concerned" about ensuring that email cannot be used to disseminate company trade secrets or valuable intellectual property.

○ **More than half of US companies surveyed (57%) say that it is "important" or "very important" to reduce the legal and financial risks associated with outbound email in the next 12 months.**

○ **More than half of US companies surveyed (51%) 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 Findings, Europe 2008

Fast facts from Proofpoint's *Outbound Email and Data Loss Prevention in Today's Enterprise, 2008* report, based on a March 2008 study of 93 email decision makers at European enterprises (32 UK, 30 Germany and 30 France) with more than 1000 employees:

- **35% of European companies with 20,000 or more employees surveyed employ staff to read or otherwise analyze outbound email.** Overall, one fifth (20%) of European companies surveyed (**38% UK,** 13% DE, 10% FR) employ such staff.
- 11% of European 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, 5% of European companies surveyed (**13% UK,** 3% DE, 0% FR) said they employ such staff.
- **30% of European companies surveyed (53% UK,** 17% DE, 19% FR**) perform regular audits of outbound email content.**
- **30% of European companies (47% UK,** 30% DE, 13% FR**) investigated a suspected email leak of confidential or proprietary information in the past 12 months.** 32% of companies surveyed (**56% UK,** 30% DE, 10% FR) investigated a suspected violation of privacy or data protection regulations in the past 12 months.
- **30% of European companies (**25% UK, 30% DE, **35% FR) surveyed say their business was impacted by the exposure of sensitive or embarrassing information in the last 12 months.** 10% (**13% UK,** 7% DE, 10% FR) said they had been impacted by improper exposure or theft of customer information. 17% (19% UK, **20% DE,** 13% FR) said they had been impacted by the improper exposure or theft of intellectual property.
- **More than a fifth (22%) of European companies surveyed (44% UK,** 7% DE, 13% FR**) terminated an employee for violating email policies in the past 12 months.** 46% of European companies surveyed (**78% UK,** 30% DE, 29% FR) disciplined an employee for violating email policies in the past 12 months.
- 18% of European companies surveyed (**28% UK,** 17% DE, 10% FR) investigated the exposure of confidential, sensitive or private information via **lost or stolen mobile devices** in the past 12 months. 40% (31% UK, **50% DE,** 39% FR) of respondents are concerned or very concerned about the risk of information leakage via email sent from mobile devices. On average, 17% of employees have mobile access to the corporate email system via wireless handheld devices.
- 12% of European companies (16% UK, **17% DE,** 3% FR) investigated the exposure of confidential, sensitive or private information via a blog or message board posting. 11% (**16% UK,** 13% DE, 3% FR) disciplined an employee for violating blog or message board policies in the past 12 months. 3% (**6% UK,** 3% DE, 0% FR) reported terminating an employee for such a violation. 24% (**28% UK,** 17% DE, 26% FR) are concerned or very concerned about the risk of information leakage via blogs and message board postings.
- 8% of European companies (9% UK, 3% DE, **10% FR**) investigated the exposure of confidential, sensitive or private information via video or audio media posted to a media sharing site. 8% (**9% UK,** 7% DE, 6% FR) have disciplined an employee for violating media sharing/posting policies in the past 12 months. 3% (3% UK, **7% DE,** 0% FR) reported terminating an employee for such a violation. 30% (31% UK, 23% DE, **35% FR**) are concerned or very concerned about the risk of information leakage via media sharing sites.
- 5% of European companies (**16% UK,** 0% DE, 0% FR) investigated the exposure of confidential, sensitive or private information via a posting to a social networking site. 6% (**16% UK,** 0% DE, 3% FR) have disciplined an employee for violating social networking policies in the past 12 months. 2% (**6% UK,** 0% DE, 0% FR) reported terminating an employee for such a violation. 28% (31% UK, 17% DE, **35% FR**) are concerned or very concerned about the risk of information leakage via posts to social networking sites.
- **11% of European publicly-traded companies surveyed investigated the exposure of material financial information (such as unannounced quarterly results) via a blog or message board posting in the past 12 months.**
- **11% of companies surveyed with 20,000 employees reported that employee email was subpoenaed in the last 12 months.** Overall, 9% of companies surveyed (6% UK, **10% DE, 10% FR**) 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 (48%) of European companies (**41% UK, **53% DE,** 52% FR**) are "very concerned" or "concerned" about web-based email** as a conduit for exposure of confidential or proprietary information.
- **Top European outbound email concerns 2008:** 63% of European companies (66% UK, 57% DE, **68% FR**) are "concerned" or "very concerned" about ensuring that email cannot be used to disseminate company trade secrets or valuable intellectual property. 62% (63% UK, 50% DE, **74% FR**) are "concerned" or "very concerned" protecting the confidentiality of personal identity and financial information in outbound email. 55% (**63% UK,** 47% DE, 55% FR) are "concerned" or "very concerned" about ensuring compliance with financial disclosure or corporate governance regulations.
- **Nearly half (49%) of European companies surveyed (**50% UK, **60% DE,** 39% FR**) say that it is "important" or "very important" to reduce the legal and financial risks associated with outbound email in the next 12 months.**
- **45% of European companies surveyed (**34% UK, **57% DE,** 45% FR**) 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 Findings, Australia 2008

Fast facts from Proofpoint's *Outbound Email and Data Loss Prevention in Today's Enterprise, 2008* report, based on a March 2008 study of 30 email decision makers at Australian enterprises with more than 1000 employees:

- **More than one quarter (27%) of Australian companies surveyed employ staff to read or otherwise analyze outbound email content.**
- **17% of Australian companies surveyed employ staff whose *primary or exclusive* job function is to read or otherwise monitor outbound email content.**
- **Nearly 1 in 3 (30%) Australian companies surveyed perform regular audits of outbound email content.**
- **Nearly one quarter (23%) of Australian companies investigated a suspected email leak of confidential or proprietary information in the past 12 months.** More than one quarter (27%) investigated a suspected violation of privacy or data protection regulations in the past 12 months.
- **Nearly one quarter (23%) of Australian companies surveyed say their business was impacted by the exposure of sensitive or embarrassing information in the last 12 months.** The same number (23%) said they had been impacted by the improper exposure or theft of intellectual property. 13% said they had been impacted by improper exposure or theft of customer information.
- **1 in 5 Australian companies surveyed (20%) terminated an employee for violating email policies in the past 12 months.** 43% of Australian companies surveyed disciplined an employee for violating email policies in the past 12 months.
- **13% of Australian companies surveyed investigated the exposure of confidential, sensitive or private information via lost or stolen mobile devices in the past 12 months.** 43% of Australian respondents are concerned or very concerned about the risk of information leakage via email sent from mobile devices. Companies said that, on average, about one quarter (26%) of their employees have mobile access to the corporate email system via smartphones or other wireless handheld devices.
- **1 in 5 Australian companies surveyed (20%) investigated the exposure of confidential, sensitive or private information via a blog or message board posting in the past 12 months.** 17% disciplined an employee for violating blog or message board policies in the past 12 months. 7% reported terminating an employee for such a violation. 40% are concerned or very concerned about the risk of information leakage via blogs and message board postings.
- **Of the 30 Australian companies surveyed, just 1 (3%) investigated the exposure of confidential, sensitive or private information via video or audio media posted to a media sharing site in the past 12 months.** However, 1 in 5 (20%) have disciplined an employee for violating media sharing/posting policies in the past 12 months. 13% reported terminating an employee for such a violation. 50% are concerned or very concerned about the risk of information leakage via media sharing sites.
- **More than one quarter (27%) of Australian companies investigated the exposure of confidential, sensitive or private information via a posting to a social networking site.** Nearly one quarter (23%) have disciplined an employee for violating social networking policies in the past 12 months. None of the surveyed Australian companies reported terminating an employee for such a violation. 40% are concerned or very concerned about the risk of information leakage via posts to social networking sites.
- **Of the 12 publicly-traded Australian companies surveyed, only 1 reported investigating the exposure of material financial information (such as unannounced quarterly results) via a blog or message board posting in the past 12 months.**
- **Of the 30 Australian companies surveyed, only 1 (3%) reported that employee email had been subpoenaed in the last 12 months.**
- In addition to concerns about the corporate mail system, **more than one third of Australian companies surveyed (37%) are "very concerned" or "concerned" about web-based email as a conduit for exposure of confidential or proprietary information.** Nearly half (47%) are "very concerned" or "concerned" about FTP as a conduit for the exposure of confidential or proprietary information.
- **Top Australian outbound email concerns 2008:** 60% of Australian companies are "concerned" or "very concerned" about protecting the confidentiality of personal identity and financial information in outbound email. 53% are "concerned" or "very concerned" about ensuring that email cannot be used to disseminate company trade secrets or valuable intellectual property. 47% are "concerned" or "very concerned" about protecting the confidentiality of private healthcare information in outbound email.
- **More than half of Australian companies surveyed (57%) say that it is "important" or "very important" to reduce the legal and financial risks associated with outbound email in the next 12 months.**
- **More than two thirds of Australian companies surveyed (70%) 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 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 both 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.

Now in its fifth year, Proofpoint's survey of enterprise attitudes about outbound email, content security and data protection has annually "taken the pulse" of IT decision-makers in the US and has helped raise awareness of the policy, technology and cultural issues surrounding email monitoring, data protection and information leaks. This year, for the first time, the survey takes a broader look at global attitudes as well—with British, German, French and Australian enterprises surveyed in addition to the US. The results show that data protection concerns are not confined to the US and that globally, email, webmail, FTP, blogs message boards, media sharing sites and social networking sites are a source of concern as well as real-world risk for IT professionals working in large enterprises.

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.

About the Study

This report summarizes findings from Proofpoint's fifth 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, blogs and message board postings, media sharing sites and social networking sites. For 2008, Proofpoint added questions related to security concerns around Internet connected mobile devices and storage media. In addition, the 2008 survey was fielded in the US, UK, France, Germany and Australia to explore global concerns.

As in previous years Proofpoint, Inc. commissioned Forrester Consulting to field an online survey of email decision makers at large enterprises in the US as well as in the UK, France, Germany and Australia. Respondents were asked about their concerns, priorities and plans related to the content of email leaving their organizations. During March 2008, Forrester gathered responses from enterprises with 1,000 or more employees. In total, 424 valid responses were received, comprised of 301 US, 32 UK, 30 German, 31 French and 30 Australian companies. Respondents were qualified based on their knowledge of their organization's email and messaging technologies. In all cases, respondents were either decision-makers or 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

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 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, by country.

In the US, 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.” Protecting personal identity/financial privacy information was the area of greatest concern, with 75% of US respondents reporting that they are “concerned” or “very concerned.” Ensuring compliance with financial disclosure or corporate governance regulations was the second most important area, with 70% of US respondents expressing a high level of concern. Ensuring that email cannot be used to disseminate trade secrets or other valuable intellectual property was a close third for US respondents with 68% expressing a high level of concern.

Though it is hard to make a “scientific” comparison between the US and other countries (because of the large differences in the size of the survey samples—there were 301 US respondents compared to roughly 30 each for the UK, Germany, France and Australia), answers from organizations based in France were most similar to US responses and these respondents demonstrated the highest levels of concern after the US.

See Figure 1 for a graphical view of how different outbound email concerns vary by country.

Outbound Email Concerns by Country, 2008

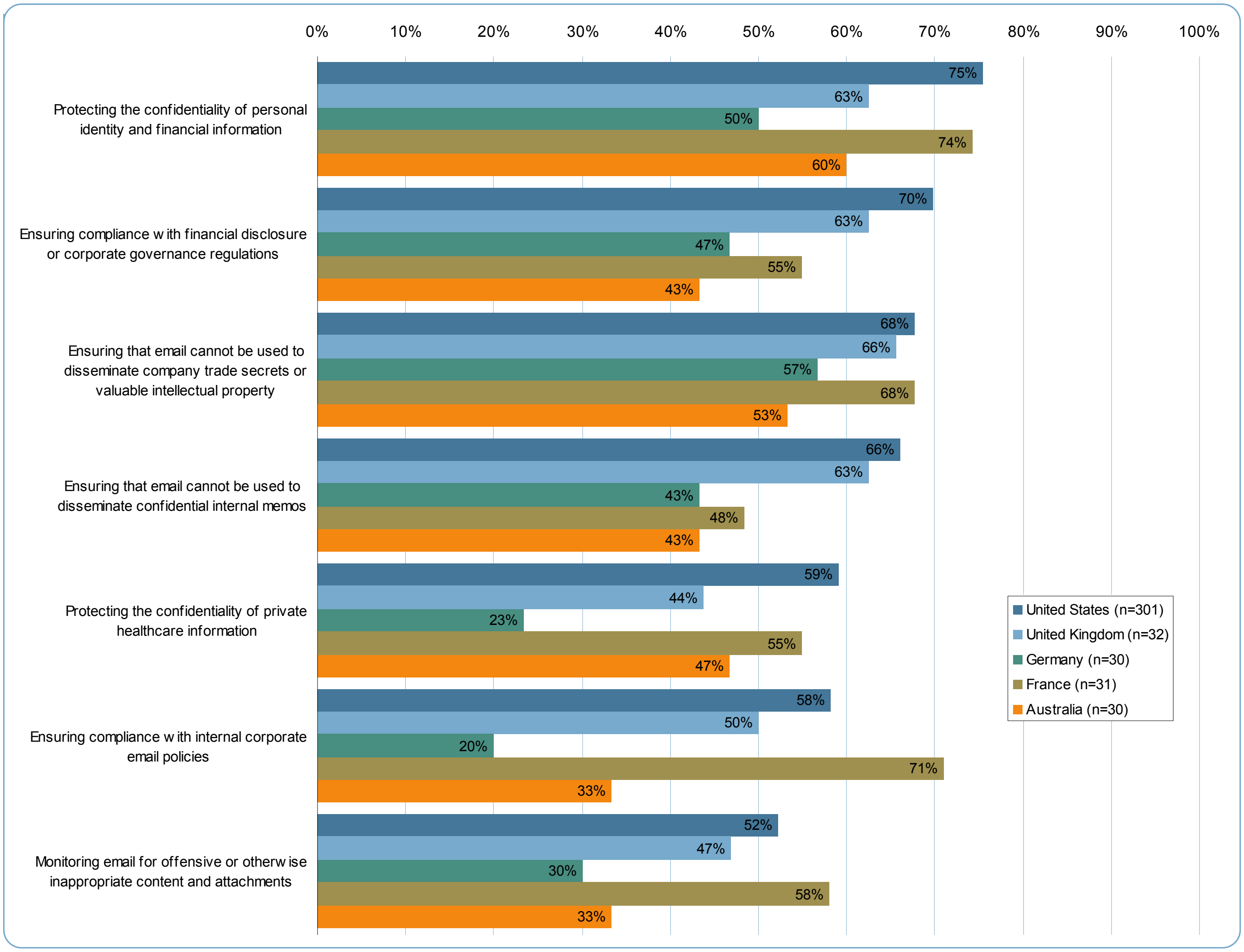

Figure 1: Percentage of respondents who reported being “very concerned” or “concerned” about various outbound email security issues, by country, 2008.

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 globally (424 respondents) as follows:

- **30%** Adult, obscene or potentially offensive content
- **26%** Confidential or proprietary business information about your organization
- **17%** Personal healthcare, financial or identity data which may violate privacy and data protection regulations

- **13%** Valuable intellectual property or trade secrets which should not leave the organization
- **14%** Don’t know

Broken out on a country-by-country basis, responses were as follows:

	US	UK	Germany	France	Australia
Adult, obscene, or potentially offensive content	28%	38%	20%	35%	40%
Confidential or proprietary business information about your organization	27%	31%	23%	23%	23%
Valuable intellectual property or trade secrets	12%	3%	17%	19%	23%
Personal healthcare, financial, or identity data	20%	9%	13%	3%	10%
Don’t know	13%	19%	27%	19%	3%

More than 1 in 10 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 (292 global responses) was that 12% of outbound email poses a risk.

Not all survey respondents provided an estimate in answer to this question, with 31% of respondents answering that they “don’t know.”

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?” Respondents estimated that less than less than half (43%, mean response from 297 global responses) of email that should be encrypted is actually sent in encrypted form, indicating that there is still a great need for more advanced email encryption solutions in today’s enterprise.

As with the previous question, not all survey respondents provided an estimate in answer to this question, with 30% of respondents answering that they “don’t know.”

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. In this year's sample—in all but one case—none of the technology solutions 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—appear to be quite common in the US, UK and Australia.

Figure 2 on page 7 shows the techniques and technologies the survey asked about and the percentage of companies that have already deployed each (reported on a country-by-country basis).

They're (Still) Reading Your Email—in the US and other Countries

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 2).

"Is Someone Reading My Email?"—US Results

In this year's survey, just under a third of all US respondents—29%—reported that they employ staff to monitor (read or otherwise analyze) outbound email content. An additional 15% of companies surveyed said that they intend to deploy such staff in the future. This technique is even more common in the largest organizations—41% of US companies surveyed with more than 20,000 employees employ staff to monitor the content of outbound email (and 10% say they intend to deploy such staff in the future).

The number of US companies that say they employ staff to monitor the contents of outbound email has remained reasonably consistent from year to year (e.g., in 2007, 32% of US companies surveyed said they employed staff to read outbound email; 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." The 2008 findings were similar to 2007: Out of all US companies surveyed, 15% employ such staff (2007 finding: 17%) and 17% say they intend to do so in the future. Of the largest US companies surveyed (those with 20,000 or more employees), 22% employ staff whose primary or exclusive job function is to read or otherwise analyze outbound email content (2007 finding: 19%) and 15% intend to do so in the future.

The survey also asked respondents if they perform regular audits of outbound email content. Overall, 38% of US companies of surveyed perform such audits (2007 finding: 37%).

"Is Someone Reading My Email?"—European Results

In this year's survey (the first time Proofpoint has collected data from multiple European countries), one fifth (20%) of European respondents reported that they employ staff to monitor (read or otherwise analyze) outbound email content. An additional 4% of European companies surveyed said that they intend to deploy such staff in the future. As in the US, this technique is more common in the largest organizations—35% of European companies surveyed with more than 20,000 employees employ staff to monitor the content of outbound email (and 8% say they intend to deploy such staff in the future).

As might be expected, the prevalence of manual email monitoring varies across the different European countries. Companies in the UK were much more likely to employ staff that reads or otherwise monitors outbound email content—38% said that they employ such staff. This result is consistent with Proofpoint's 2006 edition of the survey, which collected responses from 112 large UK companies and found that 38% of them employed "email reading" staff.

Among German respondents, 13% said they employ email reading staff. 10% of French companies employ such staff.

When European companies were asked if they "employ staff whose *primary* or *exclusive* job function is to read or otherwise analyze outbound email content," we found that only UK companies employ such staff with any regularity. 13% of UK companies say they employ such staff. Only one German company (3%) reported employing staff whose primary or exclusive job function is to read outbound email content. None (0%) of the French respondents reported employing such staff.

The survey also asked European respondents if they perform regular audits of outbound email content. Overall, 30% of European companies surveyed perform such audits, and again this type of monitoring is much more likely in the UK. 53% of UK companies surveyed—compared to 17% of German and 19% of French companies—perform regular audits of outbound email content.

"Is Someone Reading My Email?"—Australian Results

In this year's survey (the first time Proofpoint has collected data from Australian companies), more than one quarter (27%) of Australian respondents reported that they employ staff to monitor (read or otherwise analyze) outbound email content. An additional 40% of Australian companies surveyed said that they intend to deploy such staff in the future.

When Australian companies were asked if they "employ staff whose *primary* or *exclusive* job function is to read or otherwise analyze outbound email content," we found that 17% employ such staff. An additional 50% Australian companies said that they intend to deploy such staff in the future.

When asked if they perform regular audits of outbound email content, 30% of Australian companies say they perform such audits (an additional 57% say they intend to start performing such audits in the future).

Adoption of Techniques and Technologies for Mitigating Outbound Messaging Risks, by Country, 2008

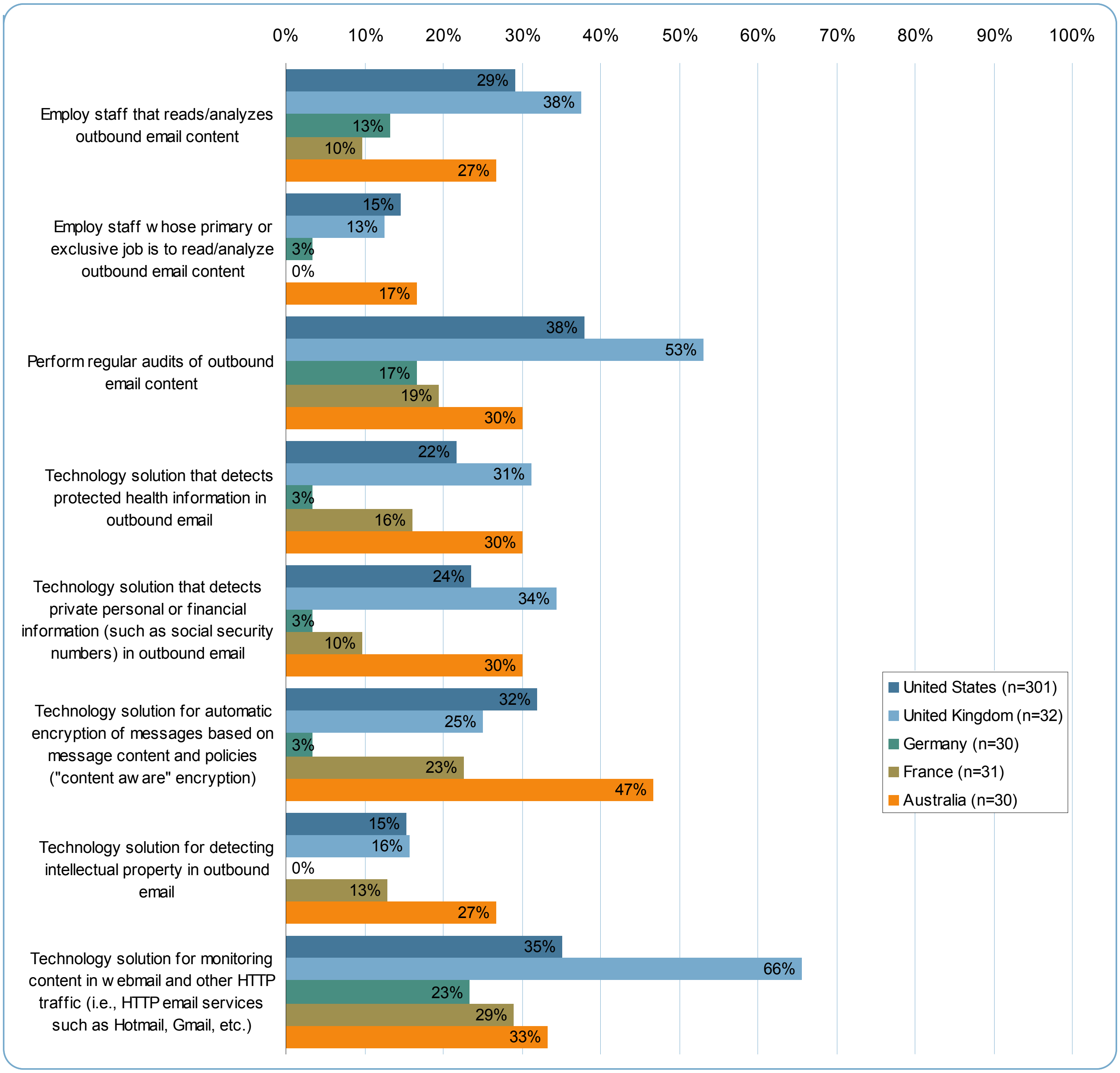

Figure 2: Percentage of respondents, by country, who report having deployed or used various techniques and technologies for mitigating outbound messaging-related risks.

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 2, which shows that deployment of technology solutions varies widely by country.

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. 22% of US, 31% of UK, 3% of German, 16% of French and 30% of Australian 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. 24% of US, 34% of UK, 3% of German, 10% of French and 30% of Australian 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). 32% of US, 25% of UK, 3% of German, 23% of French and 47% of Australian 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. 15% of US, 16% of UK, 0% of German, 13% of French and 27% of Australian 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 and other HTTP traffic (i.e., HTTP email services such as Hotmail, Gmail, etc.). 35% of US, 66% of UK, 23% of German, 29% of French and 33% of Australian 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, 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, by country, are summarized in Figure 3 (page 10) which shows the percentage of respondents who reported being "concerned" or "very concerned" about each outbound data stream.

In previous years' surveys (2006 and 2007), each category was rated as a concern by more than 40% of US respondents. This year (2008) each area was rated as a concern by more than 40% of US respondents, except for P2P networks (about which 39% of US respondents expressed a high degree of concern).

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

New in the 2008 survey, respondents were asked about their level of concern about email sent from mobile devices (such as smartphones or other wireless, Internet-connected devices). US respondents indicated the highest level of concern, with more than half (56%) reporting that they are "concerned" or "very concerned" about email sent from mobile devices as a potential conduit for exposure of confidential or proprietary information. Half of German respondents (50%) expressed a high level of concern about mobile email. 43% of Australian respondents and 39% of French respondents expressed a high level of concern.

Companies were also asked what percentage of their employees have mobile access to the corporate email system via smartphones or other wireless handheld devices. Mean estimates for each country were: US: 25%, UK: 19%, Germany: 18%, France: 12%, Australia: 26%.

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, more than half of US companies surveyed (56%) said they were "concerned" or "very concerned" about web-based email (i.e., services such as Google GMail, Yahoo! Mail, Hotmail, etc.) as a conduit for the exposure of confidential information. More than half of German (53%) and French (52%) companies also expressed a high level of concern. 41% of UK and 37% of Australian companies expressed a high level of concern about web-based email.

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

Concern about Instant Messaging (IM) as a conduit for confidential or proprietary information exposure was high for 47% of US companies, 43% of Australian companies, 35% of French companies, 28% of UK companies and 27% of German companies.

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. 44% of US companies surveyed expressed a high degree of concern about blog and message board postings as a potential source for confidential or proprietary information exposure. 40% of Australian companies, 28% of UK companies, 26% of French companies and 17% of German companies expressed a high level of concern.

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

New for 2008, survey respondents were asked to rate their level of concern about postings to social networking sites (e.g., Facebook, MySpace, Orkut, Highfive, BeBo, LinkedIn, etc.) as potential conduits for the exposure of confidential or proprietary information. Growing use of social networking sites and their increasing popularity as a business networking and recruitment tool has created a new source of data leakage risk.

44% of US companies surveyed were "concerned" or "very concerned" about posts to social networking sites. 40% of Australian companies, 35% of French companies, 31% of UK companies and 17% of German companies expressed a high level of concern.

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 Media Sharing Sites as a Conduit for Data Loss

The continuing popularity of video and audio media sharing sites (such as YouTube), and the proliferation of digital media creation in the workplace is a continuing source of risk for large enterprises.

Half (50%) of Australian companies surveyed said they were "concerned" or "very concerned" about video or audio media postings to media sharing sites as a conduit for exposure of confidential or proprietary information. 44% of US companies, 35% of French companies, 31% of UK companies and 23% of German 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 Other Potential Conduits for Exposure of Confidential Information, by Country, 2008

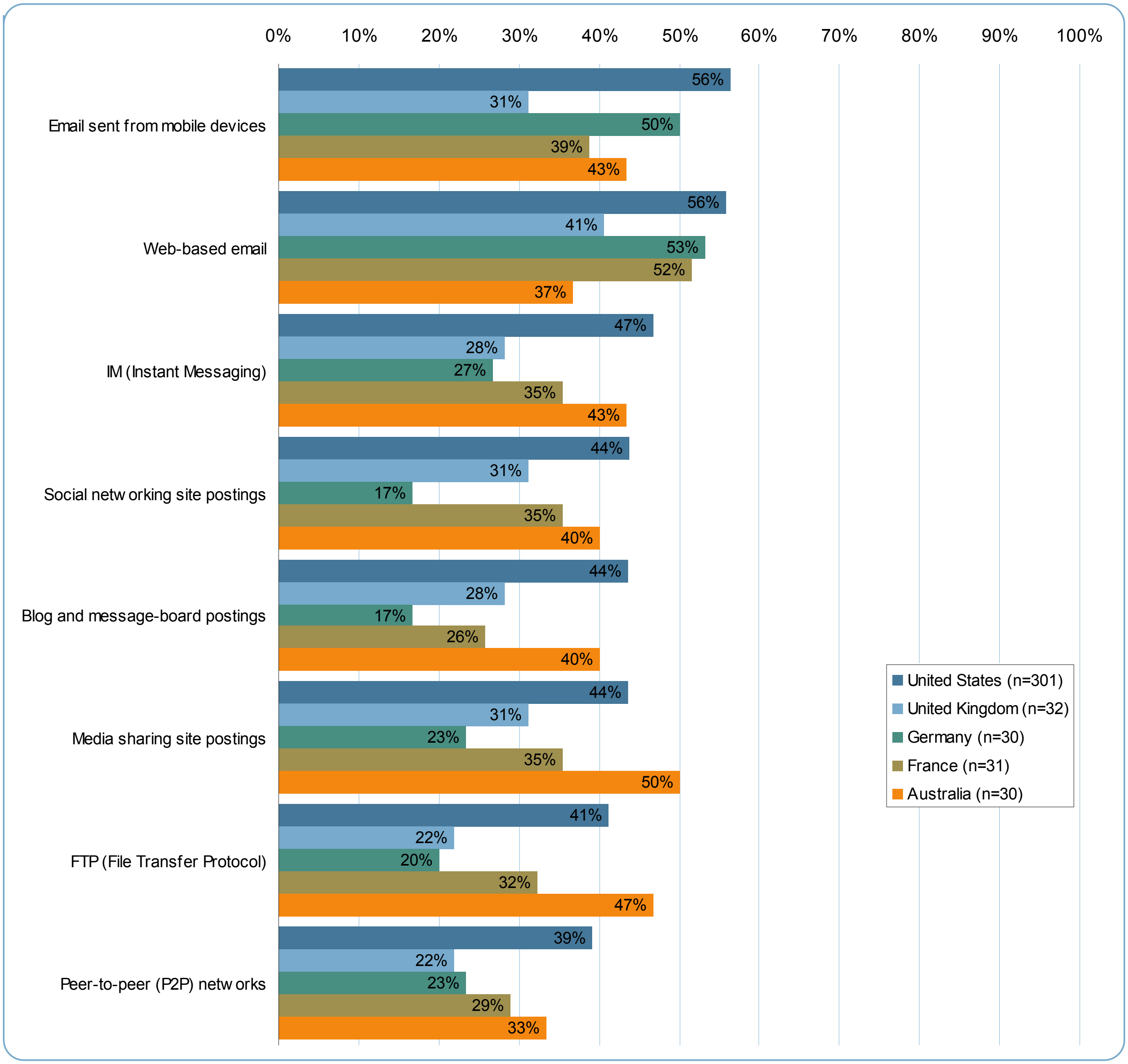

Figure 3: Percentage of respondents, by country, who reported being "concerned" or "very concerned" about other conduits (besides SMTP email) for the exposure of confidential info.

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

47% of Australian companies surveyed, 41% of US companies, 32% of French companies, 22% of UK companies and 20% of German companies expressed a high level of concern about FTP protocol transmissions as a potential source of information leakage.

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

Peer-to-peer networks (commonly used for both legitimate distribution and rights-infringing sharing of digital files) were one of the areas of lowest concern, but still represented a significant source of risk for large enterprises. 39% of US companies surveyed, 33% of Australian companies, 29% of French companies, 23% of German companies and 22% of UK companies said they were "concerned" or "very concerned" about P2P networks as potential conduits for data loss.

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 by country are summarized in Figure 4 on page 13 which shows the percentage of companies that reported having some sort of formal policy (whether "simple" or "detailed"). The policies themselves are described below:

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. As shown in Figure 4, acceptable use policies for email have nearly universal adoption among the companies in this year's survey, though 2% of US, 10% of German and 10% of French companies reported that they have "no formal policy" for acceptable use of email.

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, which include encryption requirements.

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.

Automatically forwarded email policy

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

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.

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.

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.

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.).

Social networking policy

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

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.

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.

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.

Adoption of Outbound Messaging-related Security Policies, by Country, 2008

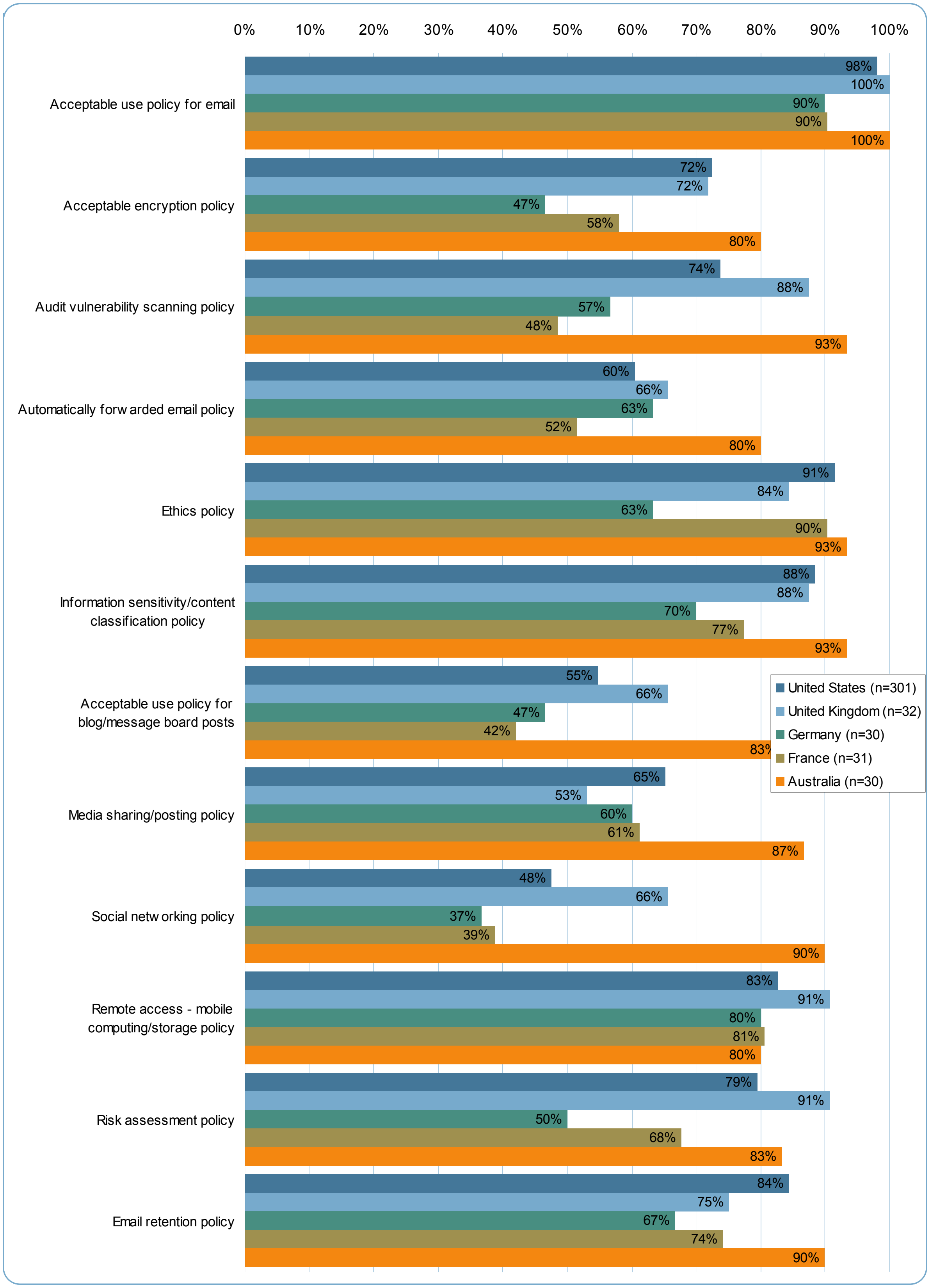

Figure 4: Percentage of companies reporting that they have formalized various security-related policies.

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 18 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, by country, in Figures 5 through 7 on the following pages.

Formal Email 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 in the past 12 months. The results, by country, are summarized in Figure 5, below.

- **Email security policy training:** Half (50%) of companies surveyed in the US and UK, and nearly half in Australia (47%), had conducted a formal training for employees about their email security policies in the past 12 months. Such training was less common in France (35%) and Germany (30%).

- **Email regulation training:** 40% of Australian companies say they formally trained employees about external regulations that apply to that organization's use of email in the past 12 months. Roughly a third of companies in the US, UK and Germany (34%, 31% and 33%, respectively) reported conducting such training. Just 13% of French companies reported conducting such training for employees.

Formal Email Policy Training, by Country, 2008

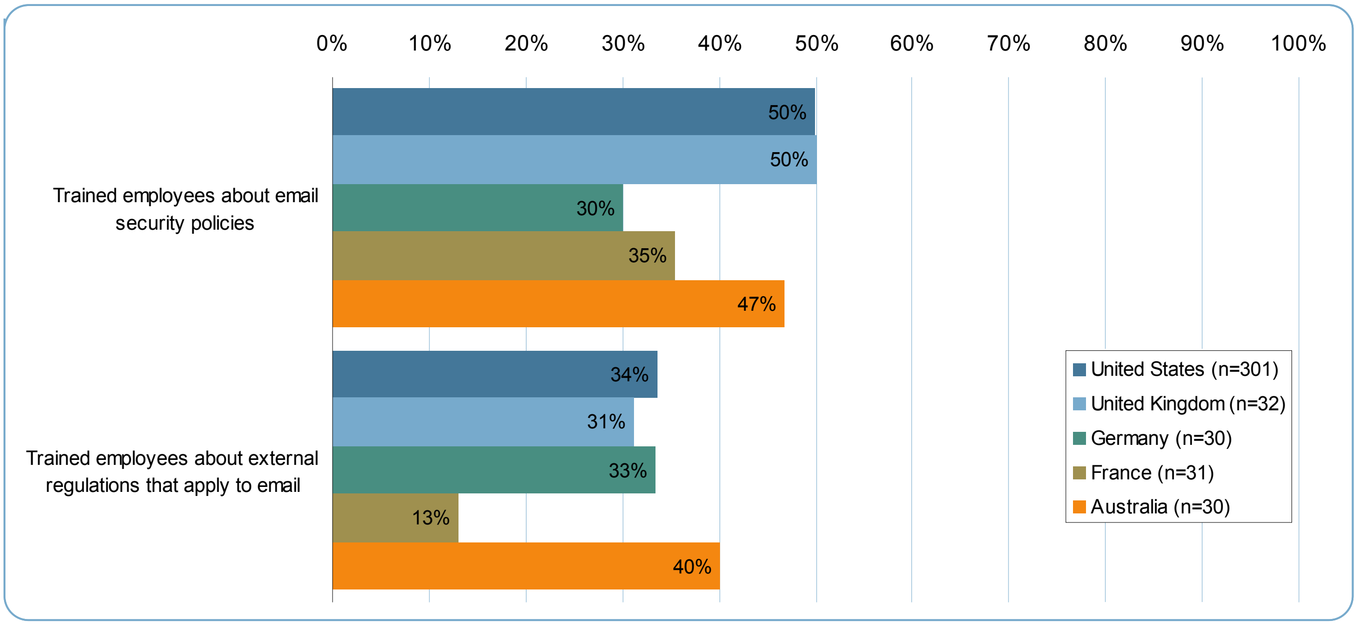

Figure 5: Percentage of companies that reported conducting formal training for employees about that organization's email policies in the past 12 months.

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

Companies 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 leaks of confidential information and regulatory compliance violations in the past 12 months. Key findings are summarized in Figure 6 on page 17, which shows the percentage of companies (by country) that investigated various types of data leaks in the past 12 months.

Leaks of Confidential Information via Email

Leaks of confidential information via email continued to be startlingly common in 2008, especially in the US and UK. 44% of US companies and 47% of UK companies surveyed report that they investigated a suspected leak of confidential or proprietary information via email in the past 12 months. Looking at the largest US companies (those with 20,000 or more employees), these investigations were even more common—more than half (54%) of the largest US companies had done so.

The 2008 finding about US companies (44%) is at its highest level since Proofpoint started tracking this statistic in 2005. For comparison, in 2007 and 2006, 34% of US companies surveyed said they had investigated an email-based leak of confidential information. In 2005, 35% of US companies conducted such an investigation.

Globally, email leaks of confidential information are far from rare: 30% of German companies, 13% of French companies and 27% of Australian companies report that they investigated an email leak of confidential information in the past 12 months.

Potential Violations of Privacy and Data Protection Regulations via Email

More than half of UK companies surveyed (56%) and 40% 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.

Again, the 2008 finding for US companies (40%) is at its highest level since Proofpoint started tracking this statistic in 2005. For comparison, in 2007, 32% of US companies surveyed said they had investigated an email-related violation of privacy or data protection regulations. In 2006, the US finding was 36%. In 2005, it was 32%.

Looking at the other countries in this year's survey, 30% of German, 10% of French and 23% of Australian companies surveyed report that they investigated an email-related violation of privacy or data protection regulations.

Leaks of Confidential Information Via Blog or Message Board Postings

Blogs and message board postings were reported as a significant source of risk. As in 2007, 21% of US companies surveyed had investigated the exposure of confidential, sensitive or private information via a blog or message board posting in the past 12 months.

With the exception of France, where just 1 company (3%) reported this type of investigation, global responses to this question were similar to the US. 16% of UK, 17% of German and 20% of Australian companies surveyed report that they investigated a blog- or message board-based leak of confidential information in the past 12 months.

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."

This question is aimed at publicly-traded companies (who are most concerned with protecting "material" financial information). 14% of US public companies surveyed said that they investigated the exposure of material financial information via a blog or message board posting. 11% of European public companies (primarily UK) reported such an investigation. In Figure 6, the results by country (for all respondents, not just publicly-traded companies) are shown.

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

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. After exploding onto the Internet scene in 2006, sites such as YouTube have remained extremely popular and they continue to pose a real risk as conduits for data leakage.

12% of US companies surveyed report that they investigated the exposure of confidential information via video or audio media posted to a media sharing site. 10% of French, 9% of UK and 3% of German and 3% of Australian companies reported likewise.

Leaks of Confidential Info Via Social Networking Site Postings

New in the 2008 survey, 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, Orkut, Highfive, BeBo, LinkedIn, etc.). The increasing popularity of social networking services within the enterprise has created a new source of risk—at least for US, UK and Australian companies.

Somewhat surprisingly, more than one quarter (27%) of Australian companies report that they had investigated the exposure of confidential info via a post to a social networking site in the past 12 months. Social networking sites are extremely popular in Australia and that popularity seems to extend into the enterprise as well. Awareness of the risks posed by social networking sites may have been heightened in Australia by high-profile press coverage of various “scandals” involving social networking sites.

16% of UK and 12% of US companies also reported investigating a leak of confidential info via a post to a social networking site in the past 12 months. None of the German or French companies surveyed reported such an investigation.

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

New in the 2008 survey, respondents were asked if they had investigated the exposure of confidential, sensitive or private information via lost or stolen mobile devices (e.g., laptop, smartphone, mobile email device) or storage media. Lost or stolen devices and storage media have often been the root cause of high-profile data breaches, as has been widely reported in the press. The most obvious example in the past year is the loss of discs that contained information on 25 million UK citizens, reported in November of 2007.

Though investigations of email-based data leaks are more common, lost/stolen devices and storage media were a significant source of risk worldwide. More than a quarter of UK (28%) and US (27%) companies surveyed said that they had investigated the loss of confidential information via lost or stolen mobile devices or storage media. 17% of German, 10% of French and 13% of Australian companies reported likewise.

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 other regulatory body to produce employee email (i.e., had employee email been subpoenaed in the past 12 months).

Nearly one quarter (24%) of US companies surveyed reported having to produce employee email in the past year. Employee email was subpoenaed even more often in the largest US companies. More than a third (34%) of US companies with 20,000 employees reported having to produce employee email in the past year.

Elsewhere in the world, employee email is subpoenaed less frequently. 6% of UK, 10% of German, 10% of French and 3% of Australian companies reported that they had been ordered to produce employee email in the past 12 months.

Investigations of Potential Data Leaks and Compliance Violations, by Country, 2008

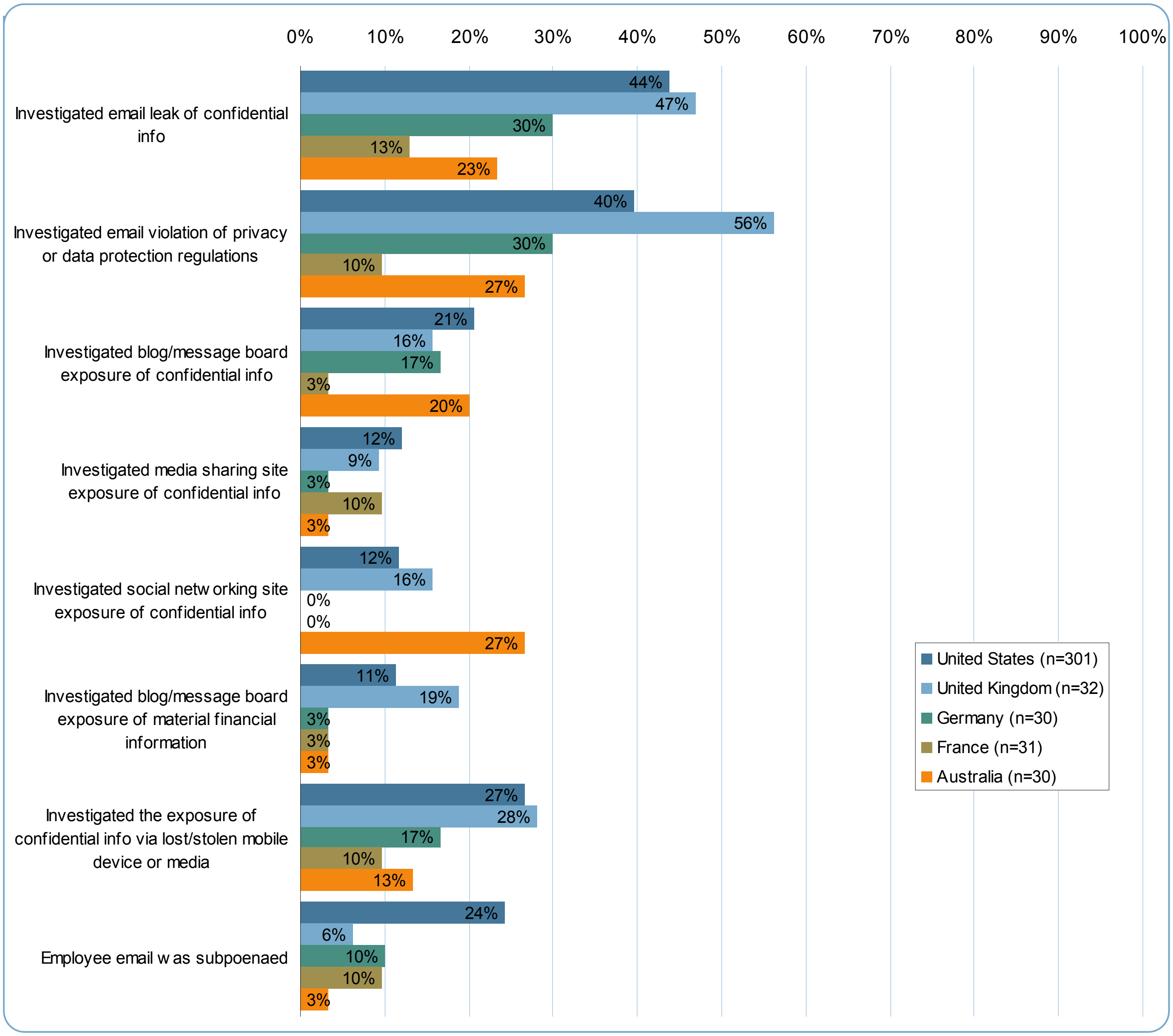

Figure 6: Percentage of US respondents who reported investigating various types of data loss events in the past 12 months.

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

As in past years, the 2008 survey asked respondents about various disciplinary actions, including termination, that they took against employees for violations of various messaging-related policy violations. The key findings are summarized, by country, in Figure 7 on page 19.

Discipline and Termination of Employees for Violating Email Policies

More than three quarters (78%) of UK respondents said they had disciplined an employee for violating email policies in the past 12 months. More than half (51%) of US respondents reported likewise. These results are consistent with previous findings for both the US and UK (e.g., in 2007, 52% of US companies reported this type of disciplinary action; in 2006, 70% of UK companies reported this type of disciplinary action). 43% of Australian companies, 30% of German companies and 29% of French companies reported likewise.

44% of UK companies, and more than a quarter (26%) of US companies reported that they terminated an employee for violating email policies in the past 12 months. 20% of Australian companies, 13% of French companies and 7% of German companies reported likewise.

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. 11% of US, 16% of UK, 13% of German, 3% of French and 17% of Australian companies surveyed said they had disciplined an employee for blog or message board policy violations in the past year.

Terminations were less frequent. 6% of US and UK, 3% of German and 7% of Australian companies reported terminating an employee for violating blog or message board policies in the past year. None of the French companies reported terminating an employee for this reason.

Results for the US were down over the prior year. For comparison, in 2007, 19% of US companies surveyed had disciplined an employee for blog/message board violations and 9% reported terminating an employee for the same reason.

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. As in 2007, it was somewhat surprising to see that US companies were more likely to discipline an employee for media sharing/posting violations than for blog/message board violations (in light of the fact that investigations of blog/message board-based leaks occur at nearly twice the rate of media sharing-based leaks).

In the US, 14% of companies surveyed reported disciplining an employee for violating media sharing/posting policies in the past 12 months (up from 11% in 2007). Australian companies were even more likely to have disciplined an employee for this reason—20% reported having done so. 9% of UK, 7% of German and 6% of French companies reported likewise.

As expected, terminations were less frequent, but more than 1 in 10 Australian companies (13%) surveyed reported that they had terminated an employee for violating media sharing/posting policies in the past 12 months. 5% of US, 3% of UK and 7% of German companies reported likewise. None of the French companies reported terminating an employee for this reason.

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.

Nearly a quarter of Australian companies (23%) reported that they had disciplined an employee for violating social networking policies in the past 12 months. While somewhat surprising, this seems consistent with the frequency of social networking-related data exposure investigations reported by the Australian survey respondents.

Such disciplinary actions were less frequent in other countries with 13% of US, 16% of UK and 3% of French companies reporting that this type of disciplinary action in the past 12 months. None of the German companies surveyed reported disciplining an employee for this reason.

Terminations for violations of social networking policy were rare. 4% of US and 6% of UK respondents said they had terminated an employee for violating the company's social networking policy in the past 12 months. None of the German, French or Australian companies reported terminating an employee for this reason.

Discipline and Termination Actions Taken by Companies, by Country, 2008

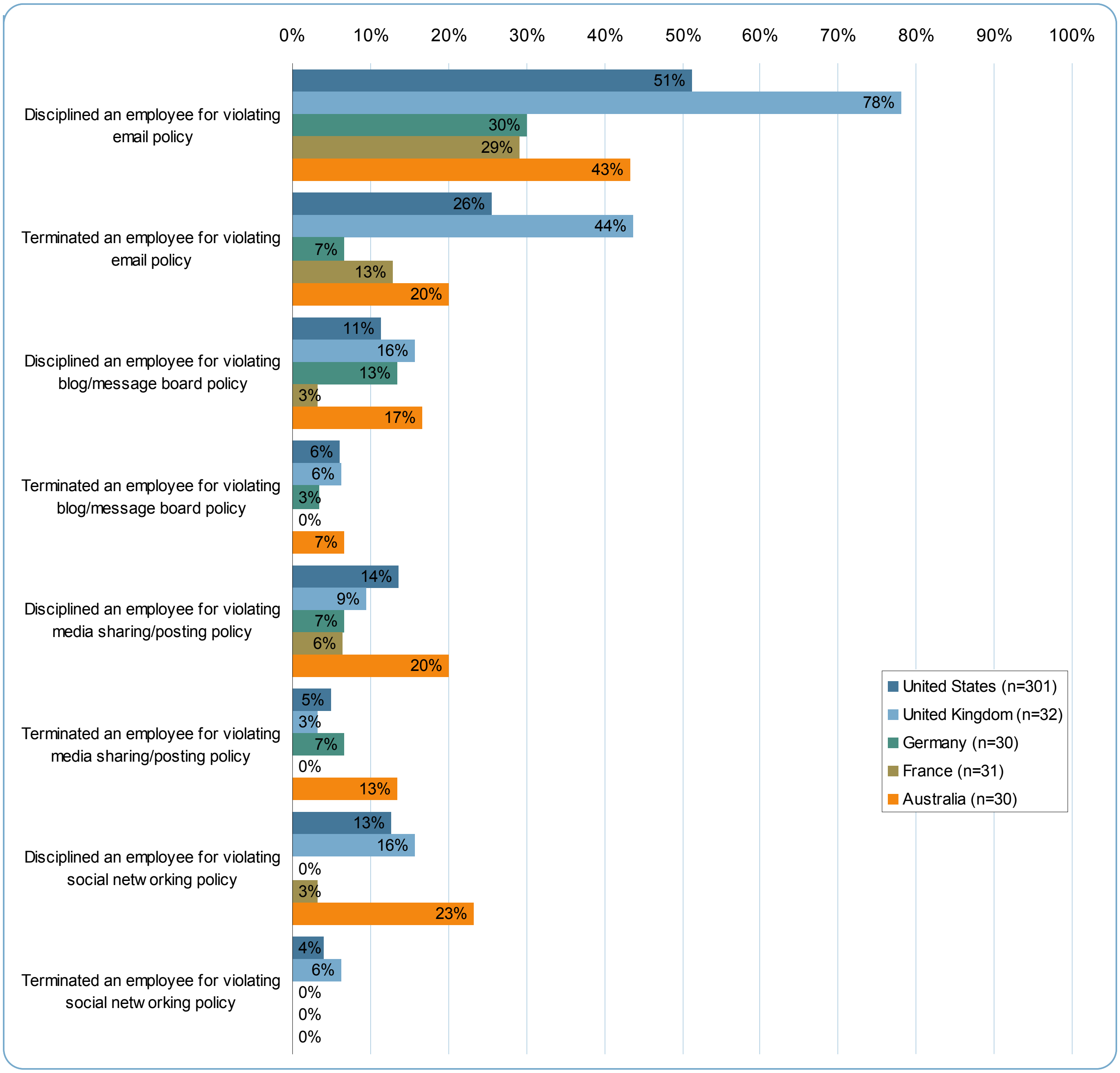

Figure 7: Percentage of respondents, by country, who reported various types of disciplinary actions against employees for messaging-related policy violations in the past 12 months.

Exposure and Theft of Sensitive Information

In addition to the questions about *investigations* of various 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. While responses varied by geography, it’s clear that exposure and theft of sensitive information remains a real risk. Figure 8 on the next page shows responses to these questions by country.

Improper Exposure or Theft of Customer Information

Globally, 16% of companies reported that they had been impacted by improper exposure or theft of customer information in the past 12 months.

Improper exposure or theft of customer information was reported most frequently in the US, with 18% of US companies surveyed reporting that their business had been impacted by such exposure in the past 12 months. US companies with more than 20,000 employees were even more likely to report customer information theft (23% said they experienced such exposure).

The UK and Australia had the second highest frequency of customer information exposure or theft with 13% of respondents reporting such an incident in the past 12 months. 10% of French respondents and 7% of German respondents reported such an exposure.

Improper Exposure or Theft of Intellectual Property

Globally, 16% of companies reported that they had been impacted by improper exposure or theft of intellectual property in the past 12 months.

Improper exposure or theft of intellectual property was reported most frequently in Australia, with 23% of Australian companies surveyed reporting that they had been impacted by such exposure in the past 12 months. Germany and the UK had the second highest frequency of intellectual property exposure or theft with 20% and 19% of companies, respectively, reporting such an incident in the past 12 months. 14% of US companies and 13% of French companies reported such an exposure.

Exposure of Sensitive or Embarrassing Information

Globally, nearly one quarter (24%) of companies reported that their business had been impacted by the exposure of sensitive or embarrassing information in the past 12 months.

Exposure of sensitive or embarrassing information was reported most frequently in France, with 35% of French companies surveyed reporting that they had been impacted by such an exposure in the past 12 months. Germany had the second highest frequency of sensitive or embarrassing information exposure with 30% of companies reporting such an incident in the past 12 months. One quarter (25%) of UK companies reported such an exposure. Nearly the same percentage (23%) of US and Australian companies reported such an exposure.

Exposure or Theft of Sensitive Information, by Country, 2008

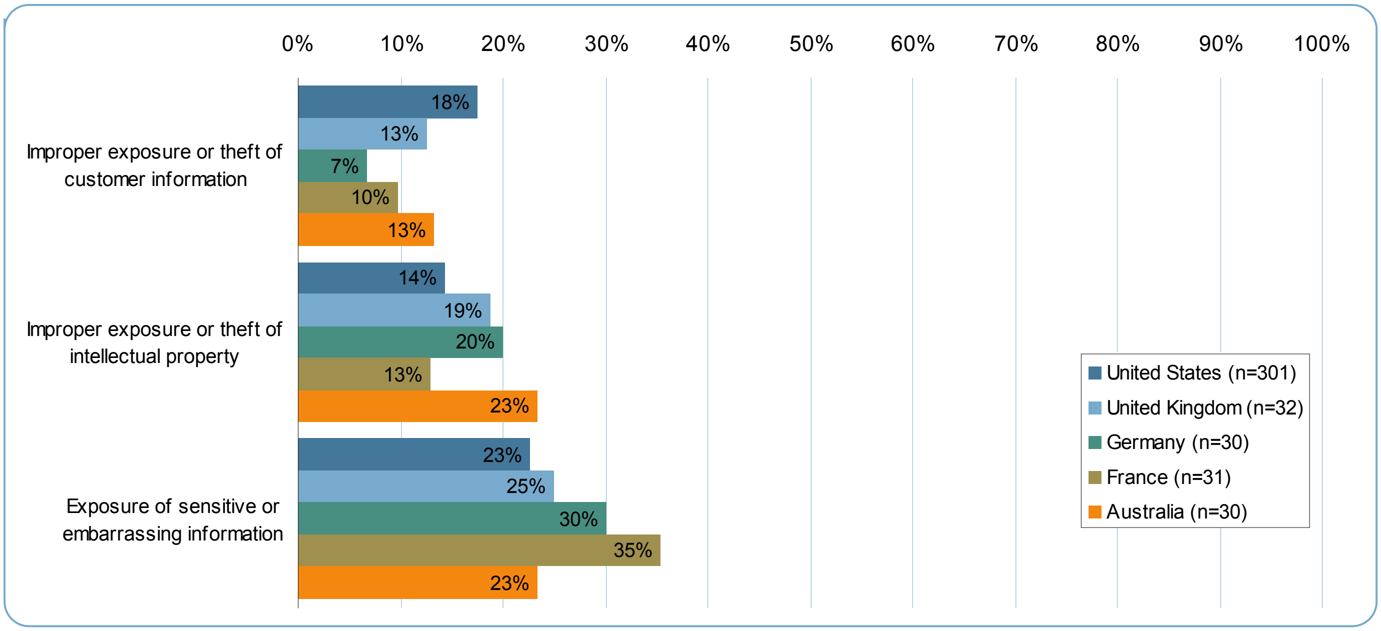

Figure 8: Percent of companies impacted by exposure or theft of various types of sensitive information in the past 12 months, by country.

Importance of Reducing the Risks Associated with the Content of 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?"

More than half of respondents surveyed in the US, UK and Germany 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 (57%, 50% and 60%, respectively). French respondents expressed a lesser sense of urgency with 39% of respondents saying it was "important" or "very important."

The responses, broken out by country, are summarized in Figure 9, on the next page.

Importance of Reducing Risks Associated with Outbound Email, by Country, 2008

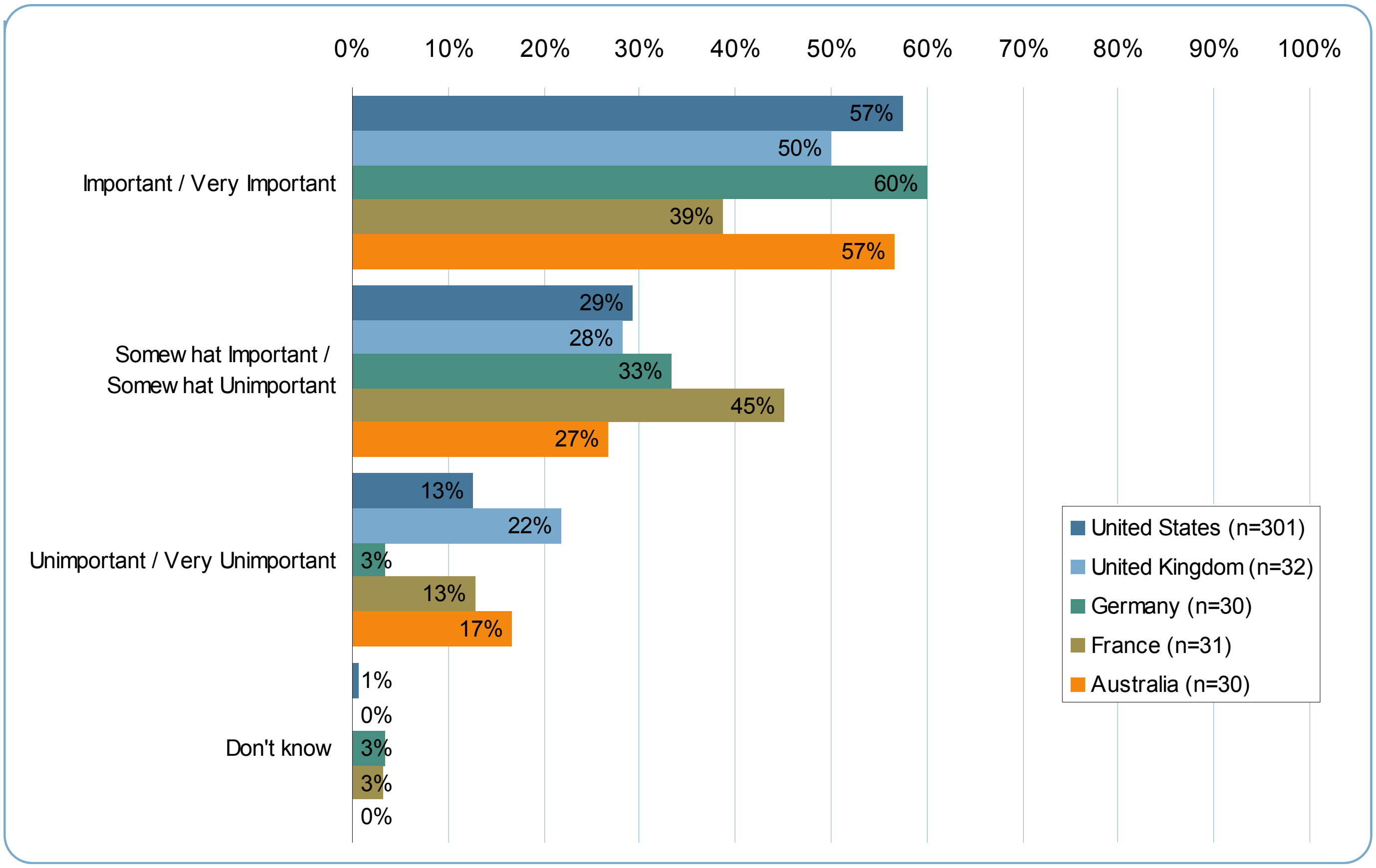

Figure 9: Importance of reducing the legal and financial risks associated with outbound email in the next 12 months, by country.

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?”

More than half of respondents surveyed in the US, Germany and Australia 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 (51%, 57% and 70%, respectively). UK and French respondents expressed a lesser sense of urgency (with 34% and 45% of respondents, respectively, saying it was “important” or “very important” to reduce HTTP risks).

The responses, broken out by country, are summarized in Figure 10, on the next page.

Importance of Reducing Risks Associated with Outbound HTTP Content, by Country, 2008

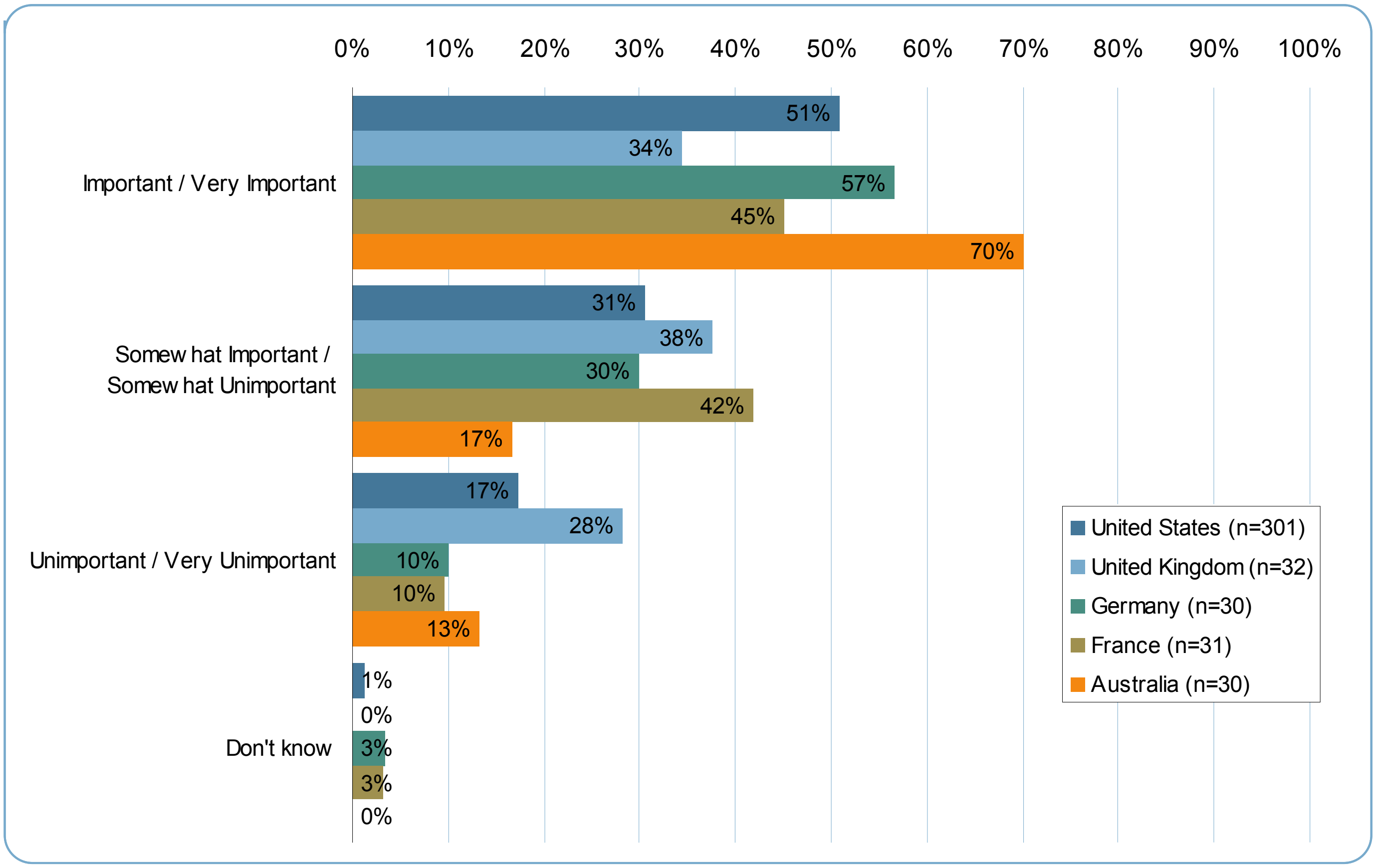

Figure 10: Importance of reducing the legal and financial risks associated with outbound HTTP content (e.g., webmail, blog and message board postings, etc.) in the next 12 months, by country.

Appendix: Respondent Demographics

Respondent Titles

The 301 US, 32 UK, 30 German, 31 French and 30 Australian respondents to this survey represented a wide variety of IT decision makers including respondents with the following titles:

Title	US	UK	Germany	France	Australia
CIO, CTO, or senior-most IT executive	20%	9%	13%	65%	13%
CSO, CISO, or senior-most IT security executive	2%	0%	3%	13%	0%
VP or executive of IT	18%	16%	23%	0%	10%
VP or executive of security	2%	3%	7%	0%	0%
Director or manager of IT	54%	72%	20%	16%	73%
Director or manager of security	3%	0%	0%	6%	0%
CFO, CEO, COO	0%	0%	17%	0%	0%
Compliance or legal officer, or counsel	0%	0%	3%	0%	0%
Senior finance executive	0%	0%	3%	0%	0%
Senior human resource executive	0%	0%	7%	0%	0%
Director or manager of messaging/email systems	1%	0%	3%	0%	3%

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	US	UK	Germany	France	Australia
1,000 to fewer than 5,000	38%	34%	57%	19%	47%
5,000 to fewer than 20,000	31%	22%	13%	35%	33%
20,000 or more	31%	44%	30%	45%	20%

Ownership	US	UK	Germany	France	Australia
Publicly traded	56%	69%	67%	65%	40%
Privately held	44%	31%	33%	35%	60%

Respondent Company Industries

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

Industry Group	US	UK	Germany	France	Australia
Primary production and raw materials manufacturing	2%	0%	0%	0%	0%
Consumer products manufacturing	4%	9%	13%	10%	3%
Chemical and petroleum manufacturing	2%	3%	3%	3%	0%
Pharma/biotech manufacturing	2%	0%	0%	10%	0%
High-tech products manufacturing	6%	6%	10%	10%	3%
Industrial products manufacturing	7%	3%	20%	10%	0%
Retail	7%	3%	7%	3%	17%
Wholesale	3%	0%	0%	3%	0%
Transportation and logistics	3%	9%	3%	10%	0%
Professional services (consulting, legal, etc.)	9%	3%	7%	3%	10%
Construction and engineering	3%	6%	0%	3%	13%
Media, entertainment, and leisure	3%	0%	0%	6%	7%
Utilities	2%	3%	0%	10%	0%
Telecom carriers	3%	3%	7%	10%	3%
Financial services	15%	19%	10%	0%	10%
Insurance	3%	0%	10%	3%	0%
Government	8%	19%	0%	6%	13%
Higher education	8%	3%	3%	0%	10%
Healthcare	8%	6%	3%	0%	3%
Non-profit/other public services	1%	3%	3%	0%	7%

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/outbound2007

http://www.proofpoint.com/outbound2006

http://www.proofpoint.com/outbound2005

http://www.proofpoint.com/outbound2004

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 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 unified email security and data loss prevention solutions for enterprises, universities, government organizations and ISPs to defend against inbound threats such as spam and viruses, prevent leaks of confidential and private information across all protocols, and encrypt sensitive emails. Proofpoint's products are controlled by a single management and policy console and are powered by Proofpoint MLX™ technology, an advanced machine learning system developed by Proofpoint scientists and engineers.

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

Proofpoint's appliance, virtual appliance, software and hosted service 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 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, GLBA and PCI. Predefined 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™ module 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.

For More Information

Proofpoint, Inc. US
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
The Oxford Science Park,
Magdalen Centre
Robert Robinson Avenue
Oxford, UK
OX4 4GA
T +44 (0) 1865 784808
F +44 (0) 1865 784809
E info@proofpoint.com
www.proofpoint.com

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

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