proofpoint

Outbound Email Security and Content Compliance in Today's Enterprise, 2005

Results from a survey by Proofpoint, Inc. fielded by Forrester Consulting on outbound email content issues, May 2005

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

Recent events—including widely-publicized, large-scale breaches of personal financial information and the passage of an increasing number of regulations governing privacy and data security—have put a spotlight on outbound email security.

Contents

Outbound Email Security and Content Compliance in Today's Enterprise, 2005

The Bottom Line

Fast facts from Proofpoint's May 2005 survey of 332 email decision makers at US enterprises with more than 1000 employees:

- **More than a third of companies (36.1%) employ staff to read or otherwise analyze outbound email.** 40% of companies with more than 20,000 employees do this.
- **Leaks of proprietary information and valuable intellectual property and ensuring compliance with internal corporate email policies** are the top outbound email concerns among large companies.
- Companies estimate that almost **1 in 4 outgoing emails (24.7%) contains content that poses a legal, financial or regulatory risk.** The most common form of such "non-compliant" email contains confidential or proprietary business information.
- **More than a 1 in 4 companies (27.1%) have terminated an employee for violating email policies in the past 12 months.** More than half (50.6%) of companies have disciplined an employee for violating email policies in the past 12 months.
- **More than 1 in 3 companies (35.2%) investigated a suspected email leak of confidential or proprietary information in the past 12 months.** More than 30% of companies investigated a suspected violation of privacy or data protection regulations in the past 12 months.
- **More than 10% (10.5%) 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, more than **70% of companies are "very concerned" or "concerned" about web-based email (e.g., Hotmail, Gmail, etc.) as a conduit for exposure of confidential information.** More than 60% of companies shared those concerns about Instant Messaging applications.
- **Nearly one half (49.3%) of large companies said it was "very important" to reduce the risks associated with outbound email in the next 12 months.**
- A free copy of this report can be downloaded by visiting: **http://www.proofpoint.com/outbound**

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 are becoming increasingly concerned about creating, managing and enforcing outbound email policies that ensure that messages leaving the organization comply with both internal rules as well as 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.

Recent events—including widely-publicized, large-scale breaches of personal financial information and the passage of an increasing number of regulations governing privacy and data security—have put a spotlight on IT security and the security of email in particular.

Increased Risk

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.

About the Study

While a great deal is known about inbound message-borne threats—including spam and viruses—relatively little attention has been paid to the issue of outbound email content. This annual survey, now in its second year, was designed to examine (1) the level of concern about the content of email leaving large organizations, (2) the technologies those organizations have put in place to mitigate risks associated with outbound email and (3) the state of email-related policy implementation and enforcement in large organizations.

On behalf of Proofpoint, Inc., Forrester Consulting fielded an online survey of email decision makers at US businesses. Respondents were asked about their concerns, priorities and plans related to the content of email leaving their organizations. Forrester gathered 332 responses from companies with 1,000 or more employees. Respondents were qualified based on their knowledge of their company's email technologies.

Survey Respondents

US enterprises with 1,000 or more employees were surveyed. Valid responses were received from 332 email decision makers. See Appendix for full demographic details.

Concerns about Outbound Email Compliance and Security

Respondents were asked to rate their current level of concern around a variety of compliance and security issues related to the content of email leaving their organizations. The survey asked about level of concern around the following seven outbound email topics:

Internal email policies
Ensuring that outbound email complies with internal corporate email policies

HIPAA regulations
Ensuring that outbound email complies with HIPAA regulations regarding confidentiality of protected health information and diagnostic codes

Personal and financial privacy regulations
Ensuring that outbound email complies with privacy regulations (such as Gramm-Leach-Bliley) regarding the confidentiality of personal identity and financial information

Financial disclosure
Ensuring that outbound email complies with financial disclosure regulations (such as Sarbanes-Oxley, SEC regulations, NASD regulations)

Valuable IP and trade secrets
Ensuring that email cannot be used to disseminate company trade secrets or other types of valuable intellectual property

Confidential memos
Ensuring that email cannot be used to disseminate confidential internal memos outside the organization

Inappropriate content and attachments
Monitoring email for offensive or otherwise inappropriate content and attachments

The Top Outbound Email Concerns

Though the top concerns vary by company size, respondents showed a high level of concern in all seven areas. Figure 1 shows the percentage of respondents who reported being "very concerned" or "concerned" about each of the topic areas for both this year's survey (2005) and last year's survey (2004, which gathered 140 responses). Respondents demonstrated a high level of concern across all categories.

Summary

Ensuring that email cannot be used to disseminate company trade secrets and valuable intellectual property was the number one concern expressed by respondents. Concerns about ensuring compliance with both internal email policies and external regulations also increased noticeably this year.

Top Outbound Email Concerns (All Companies)

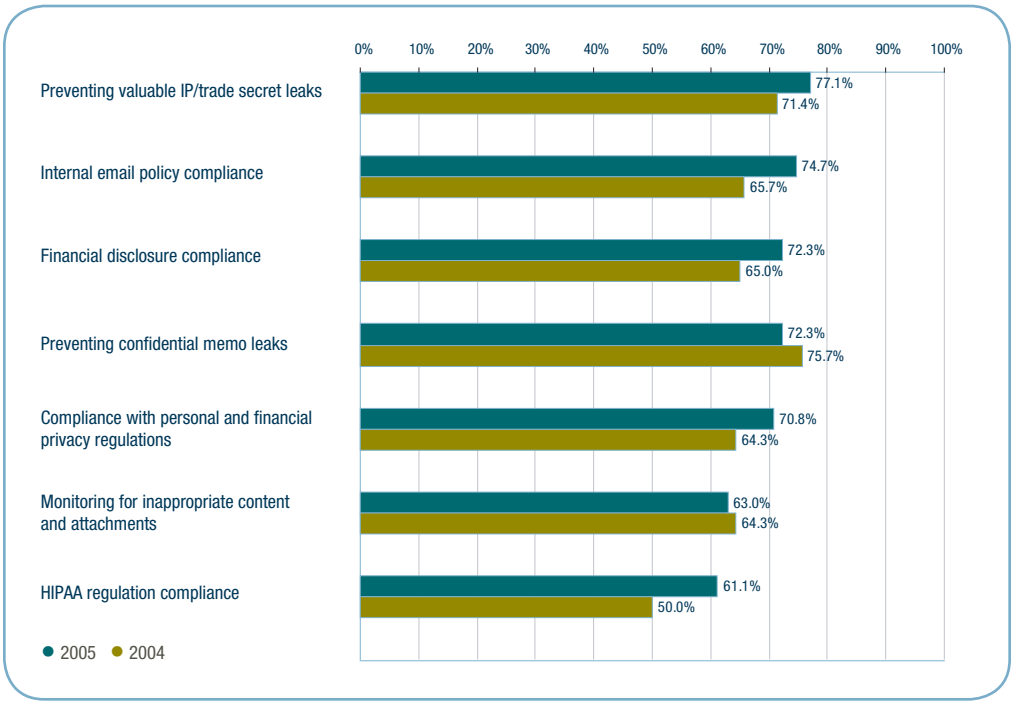

Figure 1: Respondents who reported being "very concerned" or "concerned" about outbound email compliance issues, 2005 and 2004 results compared.

Increased Concern About Intellectual Property Protection and Policy/Regulatory Compliance

In the 2004 survey, respondents expressed the most concern about confidential memos (75.7% concerned or very concerned) and intellectual property (71.4%) leaving their organizations via email. This year, results are slightly different with the highest level of concern being expressed about leakage of intellectual property or trade secrets via email (77.1%), followed by ensuring compliance with internal corporate email policies (74.7%).

Figure 1 shows that respondents reported a higher level of concern in most categories this year. Most notably, concerns about compliance with both internal policies and external regulations are markedly higher. 72.3% of companies expressed a high level of concern about compliance with financial disclosure regulations even though many of those regulations do not directly apply to the companies themselves (slightly more than half of responding companies are publicly traded).

Concern about compliance with privacy regulations (such as Gramm-Leach-Bliley), designed to protect consumer financial data, was also up (70.8%), possibly motivated by the large number of high-profile cases of identity theft and data loss reported over the past year. And, as the healthcare privacy regulations specified by HIPAA went into effect, it was no surprise to see large enterprises increasingly concerned about email compliance with those regulations (61.1% up from just 50% in 2004).

The level of concern about leakage of specific confidential memos fell slightly this year (from 75.5% to 72.3%) as did concern about offensive and inappropriate content in email (from 64.3% to 63.0%).

Overall, large organizations seem more aware of the regulatory issues that potentially impact their use of email and much more concerned about ensuring compliance with their own internal email policies than in 2004.

Top Outbound Email Concerns by Company Size

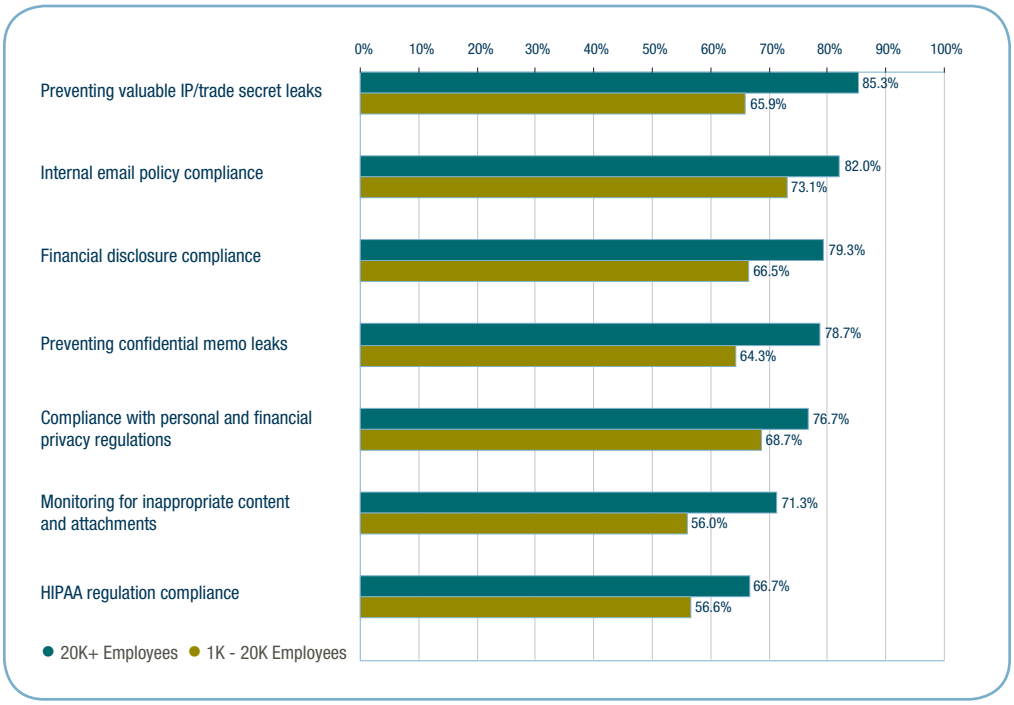

Figure 2: Respondents who reported being "very concerned" or "concerned" about outbound email compliance issues, by company size.

Top Concerns Vary by Company Size

Examining the survey responses sorted by company size (Figure 2) shows some interesting differences between companies with more than 20,000 employees and those with 1000 to 20,000 employees. As found in the 2004 survey, the largest companies show the greatest concern across all categories. Ensuring compliance with internal email policies and protecting trade secrets and valuable intellectual property are the top concerns in large companies.

Among the smaller companies, the top concerns are protecting trade secrets/intellectual property and ensuring that email cannot be used to disseminate confidential internal memos.

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 as follows:

34.9% Confidential or proprietary business information about your organization

29.8% Adult, obscene or potentially offensive content

14.5% Valuable intellectual property or trade secrets which should not leave the organization

10.2% Personal healthcare, financial or identity data which may violate privacy and data protection regulations

10.5% Don't know

Nearly 25% of Outbound Email Poses a Risk

When 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?", 40.7% of

Summary

The largest companies (those with 20,000 or more employees) exhibit an extremely high level of concern about outbound email content and compliance issues.

respondents 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.

Of the 59.3% of respondents that could answer this question, the mean answer was that an estimated 24.7% of outbound email poses a legal, financial or regulatory risk to their organizations.

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. At the same time, manual processes—such as conducting regular audits of outbound email content and employing staff to read outbound email—are surprisingly common.

Figure 3 below shows the techniques and technologies the survey asked about and the percentage of companies that have already deployed each. Figure 4 on page 8 shows the same information, but only for those companies with more than 20,000 employees.

They're Reading Your Email

As in 2004, one of the most surprising results of the survey was the high percentage of organizations that reported that they employ staff to monitor outbound email content (see Figures 3 and 4).

Out of all respondents, more than a third—36.1%—reported that they employ staff to monitor (read or otherwise analyze) outbound email. An additional 26.5% of companies said that they intend to deploy such staff in the future. Even more companies—46.4%—conduct regular audits of outbound email content.

These techniques are even more prevalent in large organizations—40% of companies with more than 20,000 employees employ staff to monitor outbound email. Of these companies, another 32% said they intend to deploy such staff in the future. More than half of the large companies—56%—reported that they conduct regular audits of outbound email content.

Adoption of Techniques and Technologies to Mitigate Outbound Email Risks (All Companies)

Summary

63% of companies surveyed either employ or intend to employ staff to monitor (read or otherwise analyze) the content of outbound email. Though concern about the risks of outbound email content are quite high, adoption of technology solutions to mitigate such risks is relatively low.

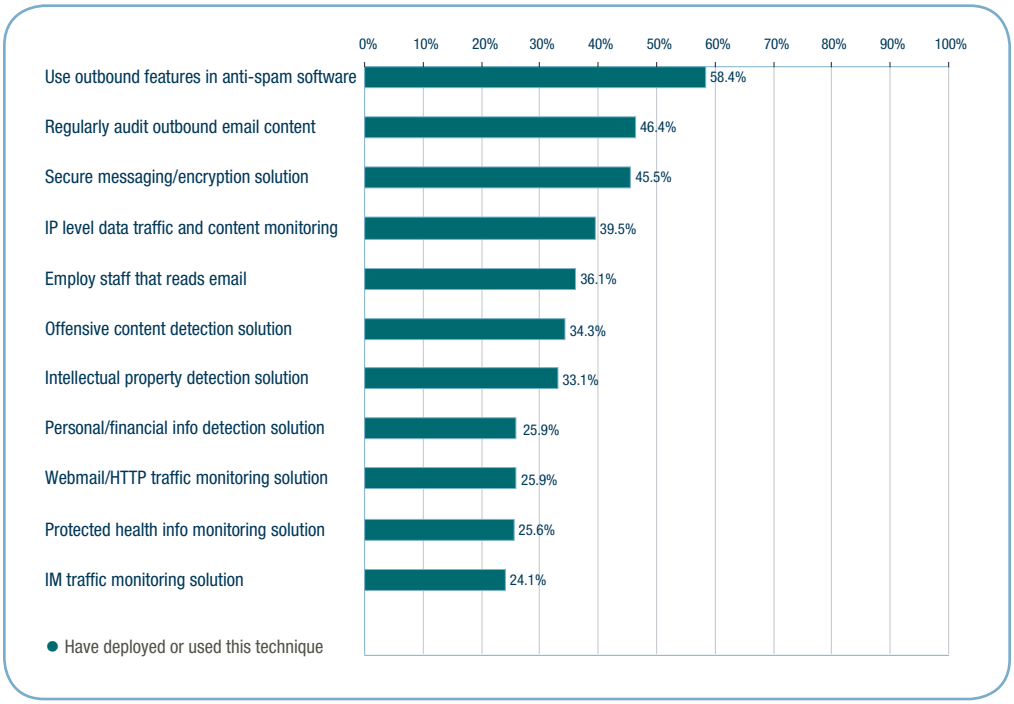

Figure 3: Adoption of techniques and technologies to mitigate outbound email risks—data from all respondents.

Adoption of Technology Solutions for Mitigating Outbound Email Risk

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 (58.4%) of surveyed companies 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

Secure messaging (encryption) systems are the next most popular technology, with 45.5% of 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.

Internet Protocol monitoring

More than a third of respondents (39.5%) said that they have deployed a technology solution for monitoring data traffic and content at the Internet Protocol (IP) level.

Various compliance solutions

Roughly a third of respondents said they have deployed technology for detecting vulgar or offensive content in outbound email (34.2%) or technology for detecting intellectual property in outbound email (33.1%). Less than a third of respondents (25.9%) said they had deployed technology for detecting personal financial information (such as social security numbers) in outbound email. Roughly a quarter (25.6%) of respondents said they had deployed a technology solution for detecting protected health information in email.

Webmail monitoring

Roughly a quarter of respondents (25.9%) 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 47.9% of respondents said that they intend to deploy such technology in the future. Webmail is clearly a key area of concern for enterprises as discussed in "Other Conduits for Exposure of Confidential Information," below.

IM monitoring

Nearly a quarter (24.1%) of respondents said they had deployed a technology solution for monitoring content in Instant Messaging traffic. Another 47.3% of respondents said that they intend to deploy such technology in the future. In addition to webmail, IM is a key area of concern as discussed in "Other Conduits for Exposure of Confidential Information," below.

Summary

The largest companies are more likely to use technology to reduce risks associated with outbound email. They are also much more likely to employ staff that reads outbound email—40% reported doing so. More than half reported conducting regular audits of outbound email content.

Adoption of Techniques and Technologies to Mitigate Outbound Email Risks (20,000+ Employee Companies)

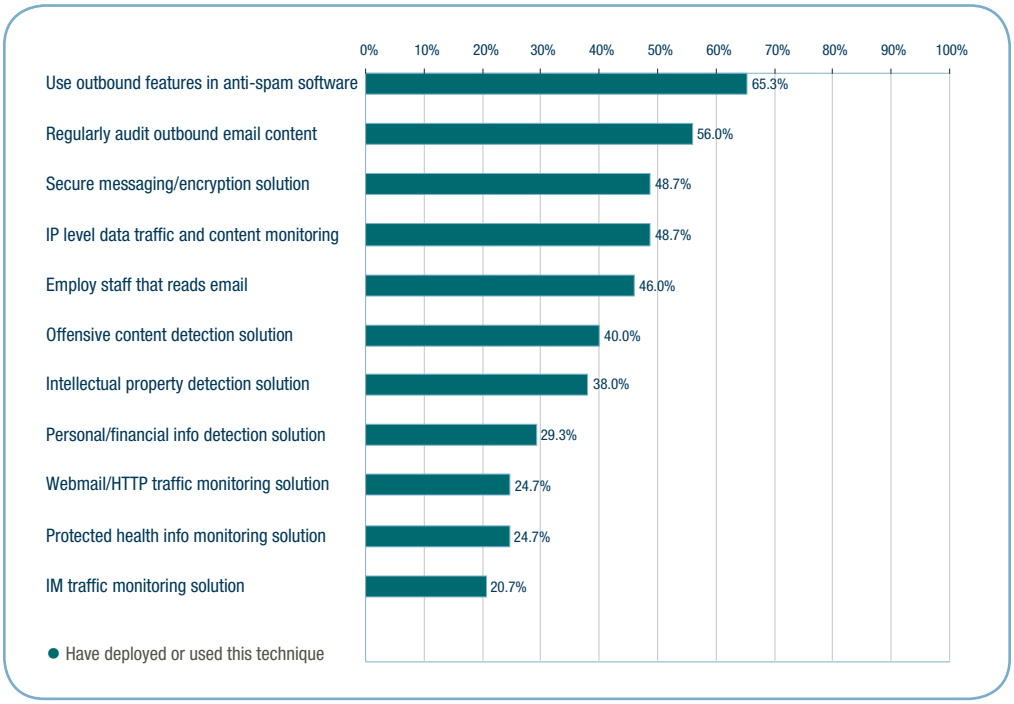

Figure 4: Adoption of techniques and technologies to mitigate outbound email risks in large organizations.

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.

Not surprisingly, companies expressed a similar level of concern about web-based email (71.4% were “very concerned” or “concerned”) as they do about the corporate email system. 62% of respondents expressed a high level of concern around Instant Messaging (IM) applications. They were less concerned about other outbound data streams—including FTP, blog and message board postings, and peer-to-peer networks—but more than 50% of respondents showed a high level of concern about each of these technologies.

Level of Concern Around Other Potential Conduits for Exposure of Confidential Info (All Companies)

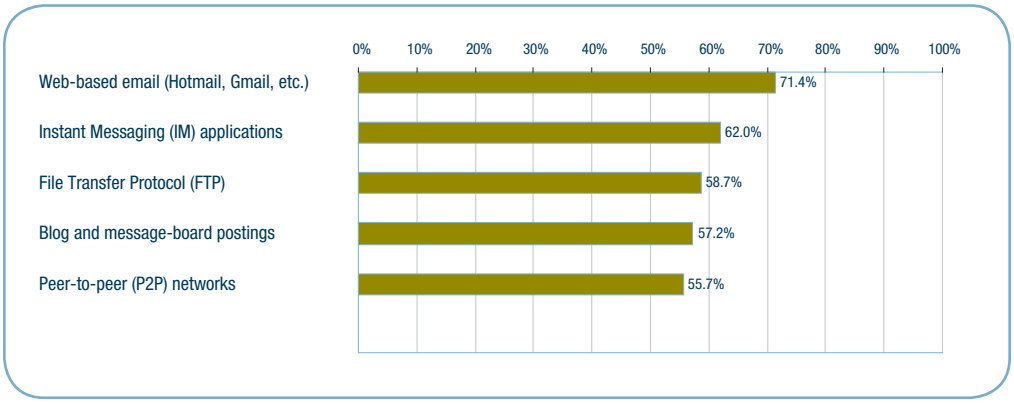

Figure 5: Respondents who reported being "very concerned" or "concerned" about other conduits.

Summary

Companies are nearly as concerned about web-based email services, such as Hotmail and Gmail, as conduits for the exposure of confidential info as they are about the corporate email system.

The Email 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. 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" seven different email-related policies. The responses are summarized in Figure 6, on the next page. In general, policy adoption was quite high. 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) for the following 7 policy types:

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. 87.7% of companies reported having some type of policy. Only 4.5% of companies reported having no formal email acceptable use policy. Respondents were also asked if they had deployed technology to help enforce such policies, but only 17.5% reported having done so.

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 prohibit transmitting certain types of health data in an unencrypted state. 69.3% of respondents reported having some type of acceptable encryption policy. 16.3% of companies reported having no such 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. 70.5% reported having such a policy. 14.2% of respondents said they had no formal policy in this area.

Automatically forwarded email policy

A policy that governs the automatic forwarding of email to external destinations. 64.8% reported implementation of this policy. 22.9% of respondents reported no formal policy for automatically forwarded email.

Ethics policy

A policy that defines ethical and unethical business practices to be adhered to by employees and executives and may include disclosure rules, conflict of interest rules, communication guidelines, etc. More than half (51.8%) of the respondents said their company had a detailed written ethics policy in place. Another 34.9% reported having a simple written policy. Only 3.7% of respondents reported no formal ethics policy.

Information sensitivity policy or content classification policy

A policy that defines requirements for classifying and securing your 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. 81.3% reported having a simple or detailed written policy. 9.6% of respondents reported no formal policy in this area.

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. 74.4% of companies have such a policy. 14.5% of companies reported having no formal risk assessment 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, but companies across industries seem concerned with this issue as 74.4% reported having a simple or detailed written policy. 14.5% had no formal email retention policy.

Implementation of Email-Related Security Policies (All Companies)

Summary

Most respondents reported having a variety of email-related security policies in place. 87.7% of companies reported having either a simple or detailed acceptable use policy for email.

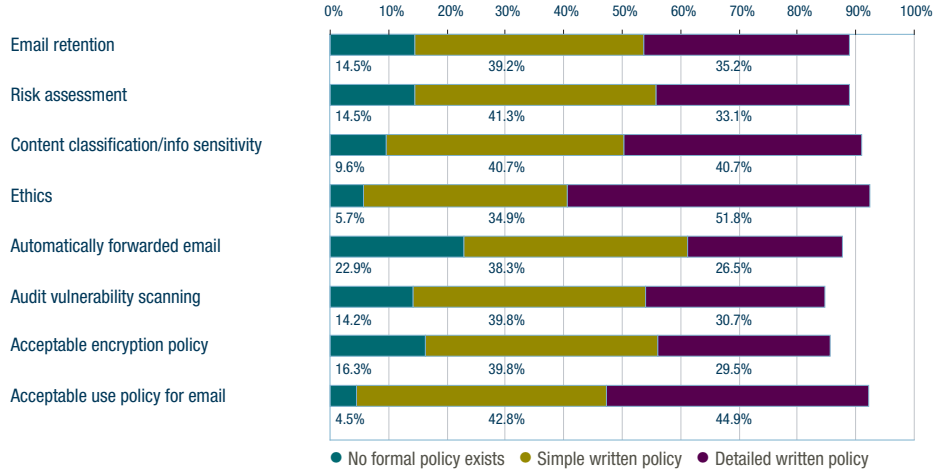

Figure 6: Implementation of various email-related policies—data from all respondents.

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 seven different policy enforcement-related events in the past 12 months. Responses are summarized in Figure 7, on the next page. Figure 7 shows the aggregate responses for all companies (blue colored bars) along with the responses from only those companies with more than 20,000 employees (olive colored bars).

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 organizations (53.9%) 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 (68% reported doing so).
- **Email regulation training**
  43.7% of organizations formally trained employees about external regulations that apply to that organization's use of email. Again, large organizations are more likely to have conducted such training (62% reported doing so).

Discipline and Termination of Employees for Violating Email Policies

Approximately half (50.6%) of respondents said their organization had disciplined an employee for violating email policies in the past 12 months. The largest companies were less likely to have done so—40% for companies with more than 20,000 employees compared to 59.3% for companies with between 1000 and 20,000 employees. More than a quarter (27.1%) of respondents said their organization had terminated an employee for violating email policies in the past 12 months. Again, such terminations were less common in the largest companies—22.7% of companies with more than 20,000 employees versus 30.8% of companies with 1000 to 20,000 employees.

Which of the Following did Your Organization Experience in the Last 12 Months?

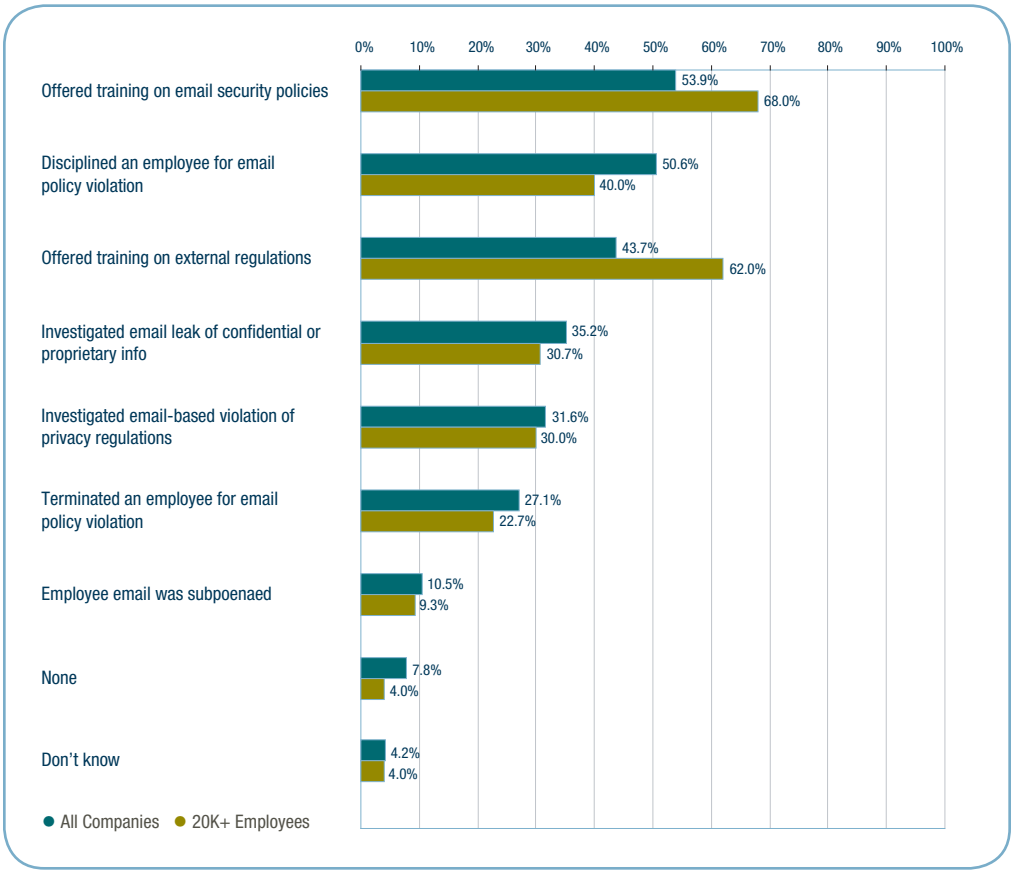

Figure 7: Reported policy enforcement events—aggregate data from all companies compared to data from larger companies only.

Investigation of Compliance Violations and Leaks of Confidential Information

Companies are justifiably concerned about outbound email content, based on the surprising 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 (35.2%) report that they investigated a suspected leak of confidential or proprietary information via email in the past 12 months. The largest companies reported fewer leaks—30.7% of companies with more than 20,000 employees versus 39% of companies with 1000 to 20,000 employees.

Regulatory Compliance Violations

31.8% of companies report that they investigated a suspected violation of privacy or data protection regulations related to email in the past 12 months. The largest companies reported fewer violations—30% of companies with more than 20,000 employees versus 33% of companies with 1000 to 20,000 employees.

Summary

More than half of companies disciplining an employee for violating email policies in the past 12 months. More than a quarter of companies had terminated an employee for email policy violations in the past 12 months.

Even though email security policy adoption is extremely high, only slightly more than half (53.9%) of companies formally trained employees on these policies in the past year.

Suspected leaks of confidential info and suspected violations of privacy or data protection regulations were fairly common.

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). More than one in 10 organizations (10.5%) reported having to produce employee email in the past year. Subpoenaing of employee email was slightly less common at the largest companies—9.3% reporting such an event—versus the 11.5% of companies with 1000 to 20,000 employees.

Importance of Reducing Outbound Email Content Risks

The continuing gap between the adoption of technology solutions for outbound email compliance and security (see "Adoption of Technology Solutions for Mitigating Outbound Email Risk" on page 7) and the level of concern around outbound email content (see "Concerns about Outbound Email Compliance and Security" on page 3) suggests that there is a continued urgency for organizations to reduce risks associated with outbound email content.

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 (57.8%) of all companies said that such reductions were "very important" or "important" in the next 12 months. An additional 17.8% said such reductions were "somewhat important."
- The largest companies display an even greater sense of urgency: Approximately one-half (49.3%) of companies with 20,000 or more employees said such risk reductions were "very important" in the next 12 months. Additionally, 19.3% of large companies said such reductions were "important" and 8% said such reductions were "somewhat important."

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

Summary

Approximately one-half of the largest companies consider it "very important" to reduce the legal and financial risks associated with outbound email in the next 12 months. A majority of all companies believe it's important to reduce outbound email risks in the coming year.

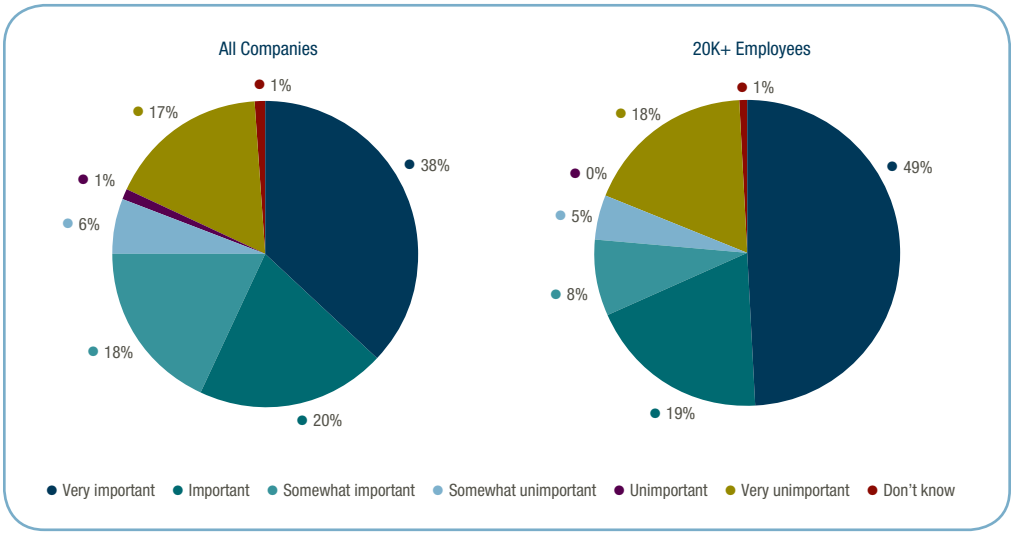

Figure 8: Importance of reducing risks associated with outbound email in the next 12 months.

Appendix: Respondent Demographics

Respondent Titles

The 332 respondents to this survey represented a wide variety of IT decision makers including respondents with the following titles:

CIO, CTO, or senior-most IT executive	18.7%
CSO, CISO, or senior-most IT security executive	0.9%
VP or executive of IT	10.5%
VP or executive of security	1.5%
Director or Manager of IT	29.5%
Director or Manager of security	5.4%
CFO, CEO, COO	9.0%
Compliance or Legal officer, or council	3.9%
Senior Finance executive	7.5%
Senior Human Resource executive	5.4%
Director or Manager of Messaging/Email Systems	7.5%

Respondent Company Sizes

The size of the surveyed organizations, based on number of employees, was reported as follows:

1000 to less than 5000	27.4%
5000 to less than 20,000	27.4%
20,000 or more	45.2%

Respondent Company Industries

Of the responding companies, 54.2% were publicly traded companies and 45.8% were privately held. These companies represented a wide variety of industries, reported as follows:

Primary production and raw materials	2.4%
Consumer products	13.6%
Chemicals and petroleum	2.1%
Pharma/biotech	0.9%
High-tech products	12.3%
Industrial products	3.0%
Retail	10.2%
Wholesale	3.0%
Transportation and logistics	6.3%
Professional services	4.5%
Construction and engineering	1.5%
Media, entertainment, and leisure	4.8%
Utilities	1.2%
Telecom carriers	2.7%
Financial services	10.2%
Insurance	3.0%
Government	6.6%
Higher education	2.7%
Healthcare	8.1%
Non-profit/other public services	0.6%

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.

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.
www.proofpoint.com/regulatory

Outbound Email Security and Content Compliance in Today's Enterprise, 2004
Summary of Proofpoint's 2004 survey on outbound email issues.
http://www.proofpoint.com/outbound2004

Products

Proofpoint Protection Server
Proofpoint Messging Security Gateway
Proofpoint Content Compliance
Proofpoint Digital Asset Security
Proofpoint Regulatory Compliance
Proofpoint Spam Detection
Proofpoint Virus Protection

For More Information

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

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. 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 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 optional 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 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.