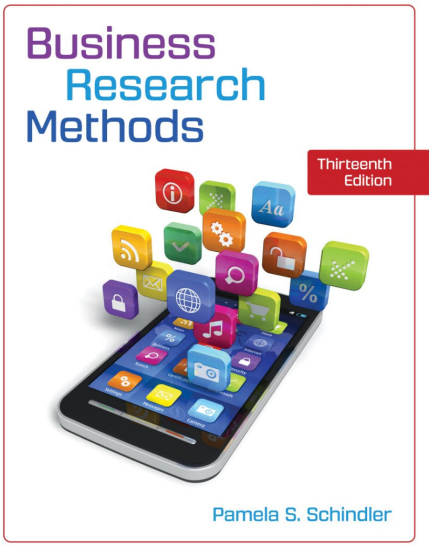


Outbound Email Security and Content Compliance in Today's Enterprise

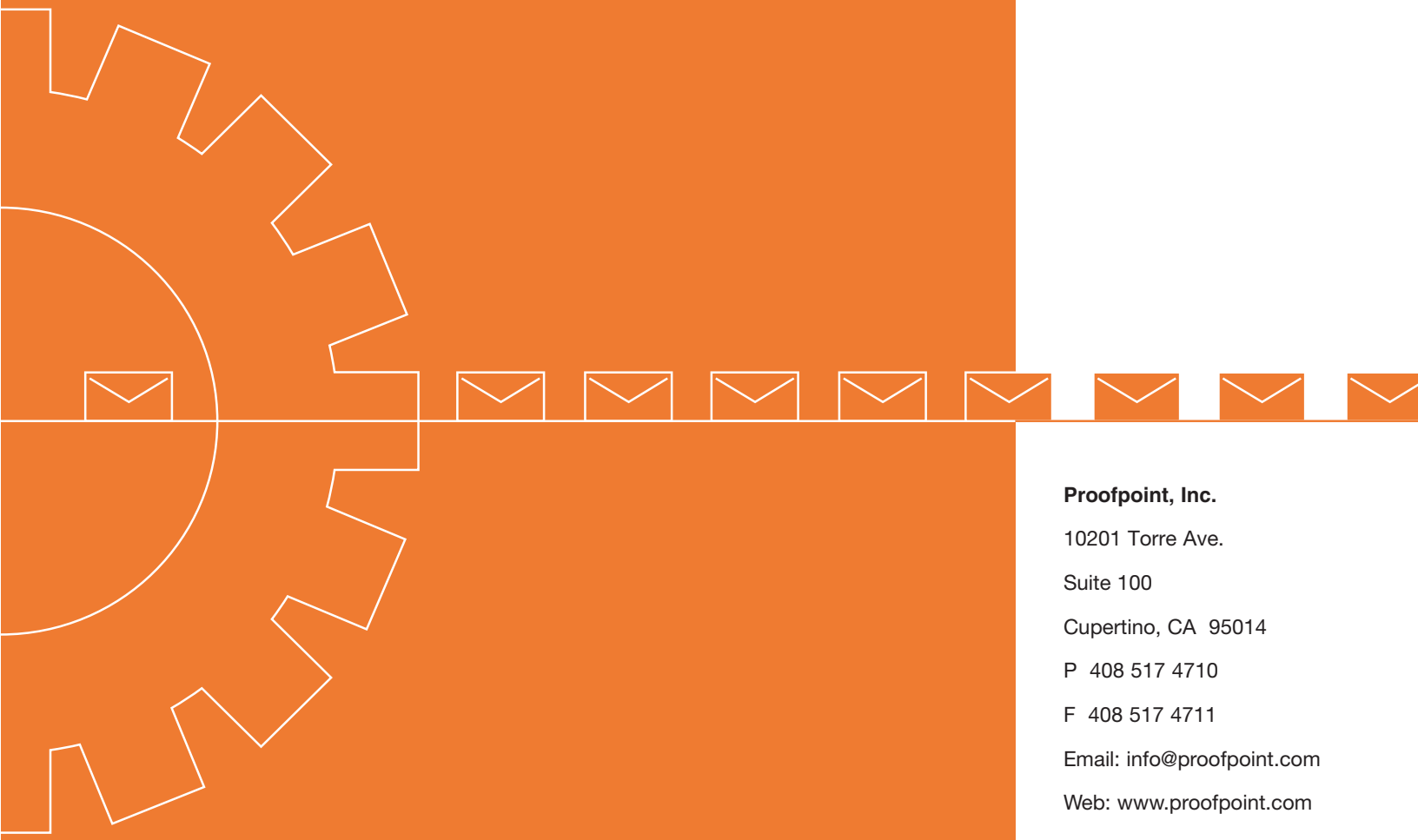
Results from an Omnibus Study by Forrester Consulting on Outbound Email Content Issues, June 2004

proofpoint™

Outbound Email Security and Content Compliance in Today's Enterprise

Results from an Omnibus Study by Forrester Consulting on Outbound Email Content Issues, June 2004

proofpoint™



Proofpoint, Inc.

10201 Torre Ave.

Suite 100

Cupertino, CA 95014

P 408 517 4710

F 408 517 4711

Email: info@proofpoint.com

Web: www.proofpoint.com

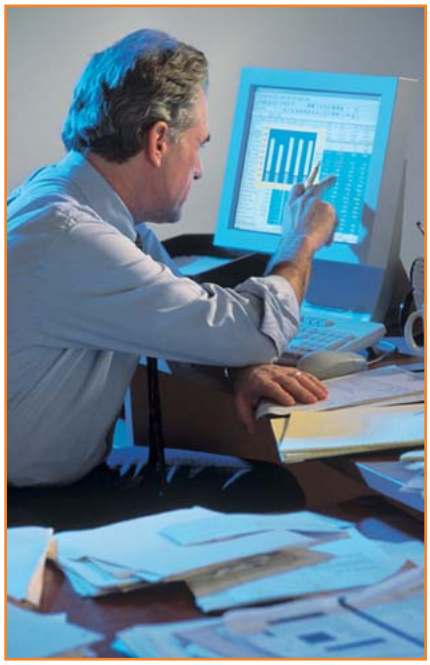
The Bottom Line

More than 43% of large corporations employ staff to monitor out-bound email.

Confidential memo and intellectual property leaks are the top outbound email concerns among large companies.

Nearly 75% of large corporations rate outbound email risk mitigation as "important" or "very important" over the next 12 months. This number rises to 95% when confined to the financial services and insurance industries.

Almost 93% of respondents indicated that it was "important" or "very important" to have outbound messaging compliance technology integrated with inbound anti-spam and anti-virus solutions



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.

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 survey was designed to examine the level of concern about the content of email leaving large organizations and the technologies those organizations have put in place to mitigate the risks associated with outbound email.

On behalf of Proofpoint, Inc., Forrester Consulting fielded an online survey of technology decision makers at North American businesses. Respondents were asked about their concerns, priorities and plans related to the content of email leaving their organizations. Forrester gathered 140 responses from companies with 1,000 or more employees. Respondents were qualified based on their knowledge of their company's email technologies.

Enterprise 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 and financial information
- **Financial disclosure:** Ensuring that outbound email complies with financial disclosure regulations (such as Sarbanes-Oxley, SEC regulations, NASD regulations)
- **Valuable IP/trade secrets:** Ensuring that email cannot be used to disseminate company trade secrets or valuable intellectual property
- **Confidential memos:** Ensuring that email cannot be used to disseminate confidential internal memos
- **Inappropriate content and attachments:** Monitoring email for offensive or otherwise inappropriate content and attachments

Though the top concerns vary by company size, respondents showed a high level of concern in all seven areas. Figure 1 on page 2 shows the percentage of respondents who reported being "very concerned" or "concerned" about each of the topic areas.

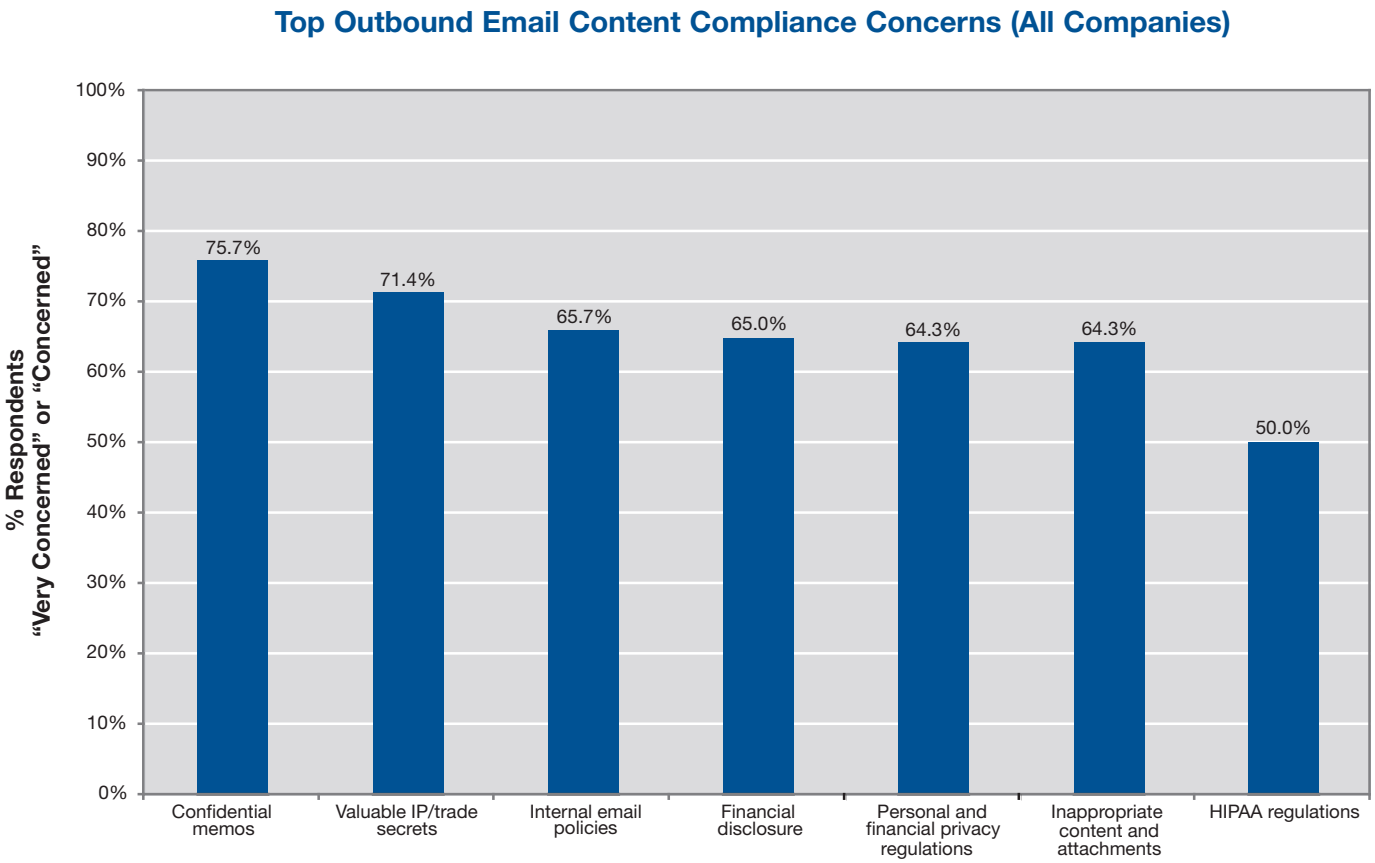


Figure 1: Respondents who reported being "concerned" or "very concerned" about outbound email compliance issues

Regulatory Concerns Take a Back Seat to Protecting Company Assets

Respondents expressed the most concern about confidential memos (75.7% concerned or very concerned) and intellectual property (71.4%) leaving their organizations via email. Though ensuring that outbound email complies with external regulations — related to financial disclosure, personal information and protected health information — is also of concern, the top concerns relate to keeping the *company's* confidential info and proprietary intellectual property private.

Examining the aggregate responses from all companies, the level of concern about enforcing the organization's own internal email policies was roughly the same (65.7%) as the concern around financial disclosure (65.0%), personal/financial privacy regulations (64.3%) and inappropriate content (64.3%). Though compliance with HIPAA regulations ranked as the lowest concern, fully half (50.0%) of all respondents reported being concerned or very concerned about this area.

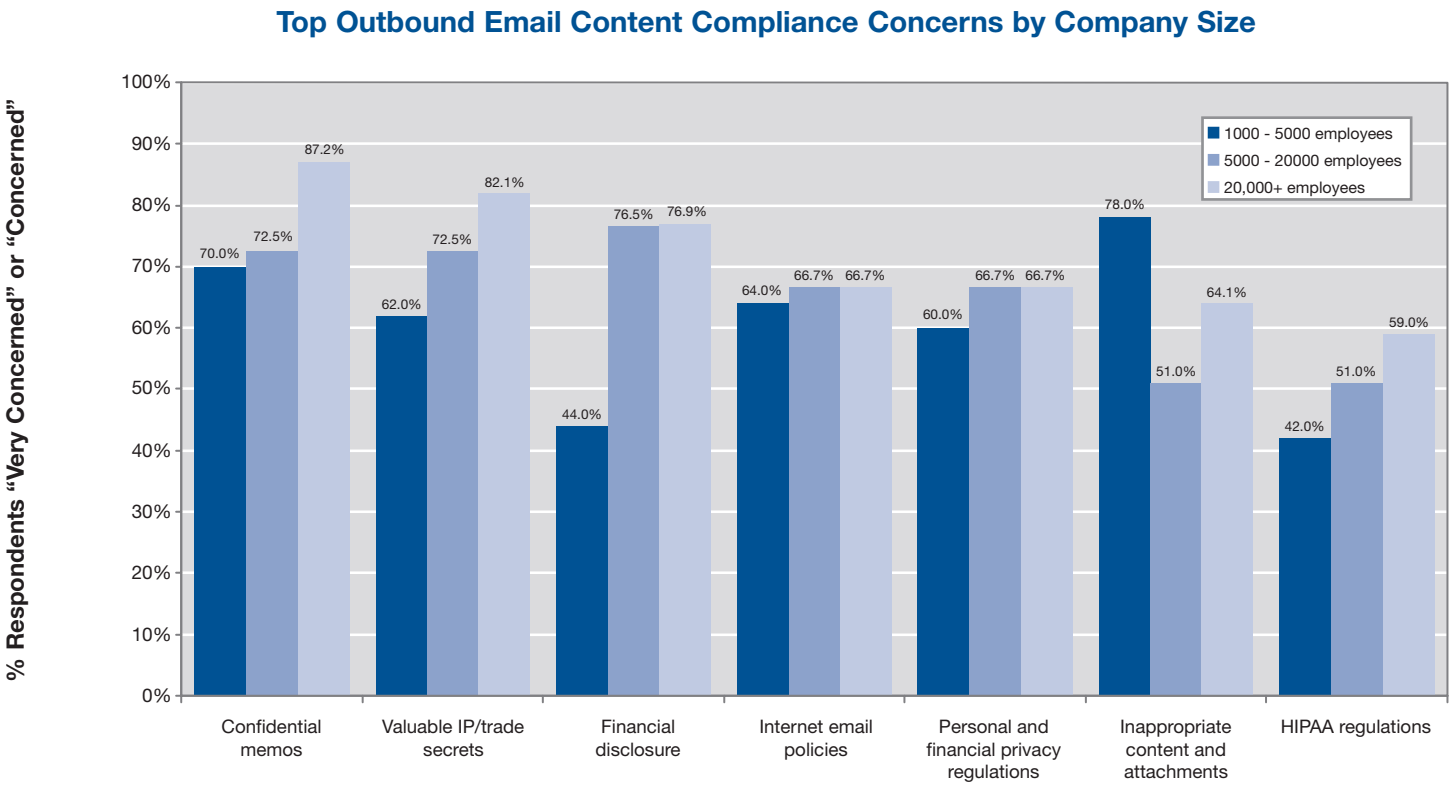


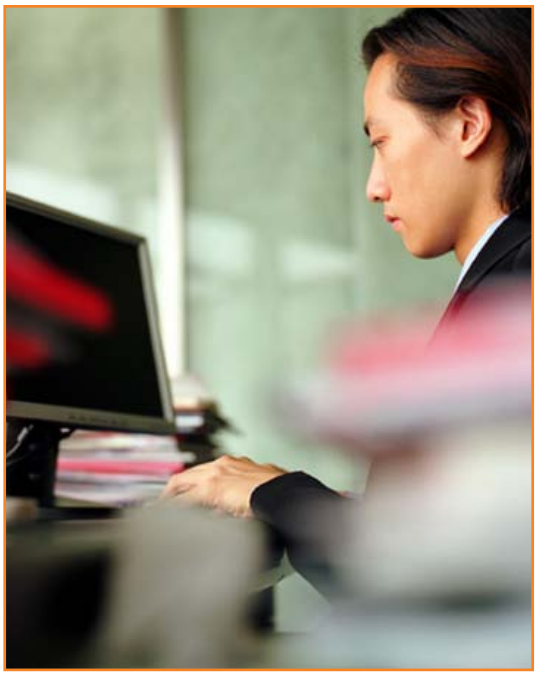
Figure 2: Level of concern of outbound email messages, by company size

Top Concerns Vary by Company Size

Examining the survey responses sorted by company size shows some interesting differences between companies with 1,000 to 5,000 employees, those with 5,000 to 20,000 employees, and those with 20,000 or more employees (see Figure 2, above).

The largest companies show the greatest concern across all categories. Once again, protecting confidential memos and company trade secrets are the top two concerns for companies with more than 20,000 employees. Companies with 5,000 to 20,000 employees are slightly less concerned about these topics. Instead, financial disclosure issues are the top-rated concern for these organizations.

Among the smaller companies (with 1,000 – 5,000 employees), monitoring email for offensive or otherwise inappropriate content and attachments was the top concern (78.0% of respondents from those companies said they were "concerned" or "very concerned" about this topic). These companies were much more concerned about this topic than larger companies. With this one exception, smaller companies are generally less concerned about outbound email compliance issues, especially those related to financial disclosure and HIPAA regulations.



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. However, manual processes — employing staff to monitor outbound email and conducting regular audits of out-bound email content — are surprisingly common.

Figure 3 on page 5 shows the techniques and technologies the survey asked about and the percentage of companies that have already deployed each. Figure 4 on page 6 shows the same information, but just for companies with more than 20,000 employees.

They're Reading Your Email

One of the most surprising results of the survey was the high percentage of organizations that re-ported that they employ staff to monitor outbound email content. (See Figures 3 and 4 on the following pages.) Out of all respondents, 30.7% reported that they employ staff to monitor outbound email. An additional 9.3% of companies said that they intend to deploy such staff in the future.

This technique is even more prevalent in large organizations — 43.6% of companies with more than 20,000 employees employ staff to monitor outbound email. Of these companies, another 12.8% said they intend to deploy such staff in the future.

A similar percentage (32.9%) of companies report that they conduct regular audits of outbound email content. Again, this technique is more prevalent among companies with more than 20,000 employees (38.5% conduct such audits).

The prevalence of these techniques varies somewhat by vertical industry. Figure 5 on page 7 shows the percentage of companies, sorted by basic industry groupings, which report employing staff to monitor outbound email or conducting regular audits of outbound email content.

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

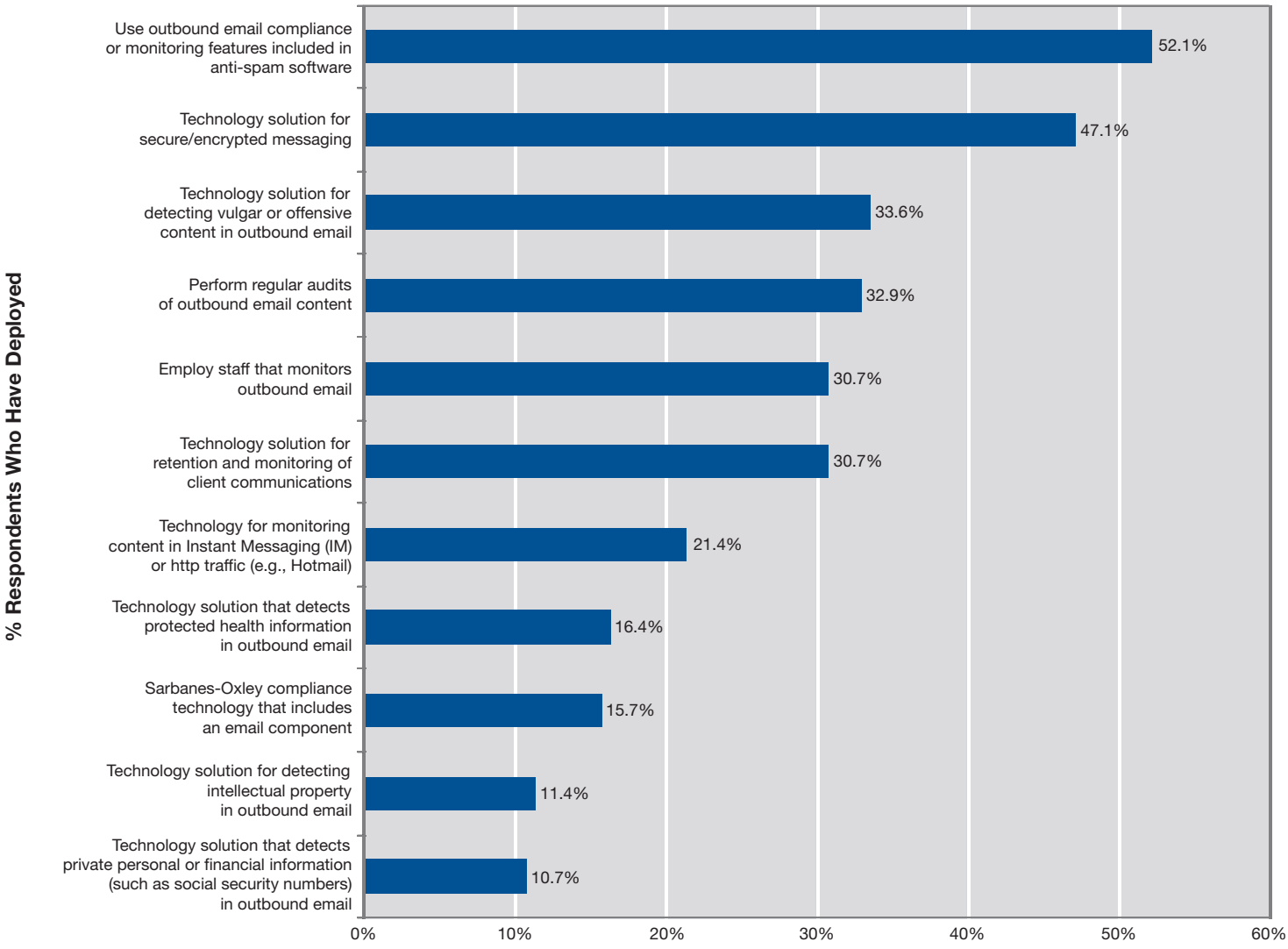


Figure 3: Adoption of techniques and technologies to mitigate outbound email risks — data from all respondents

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

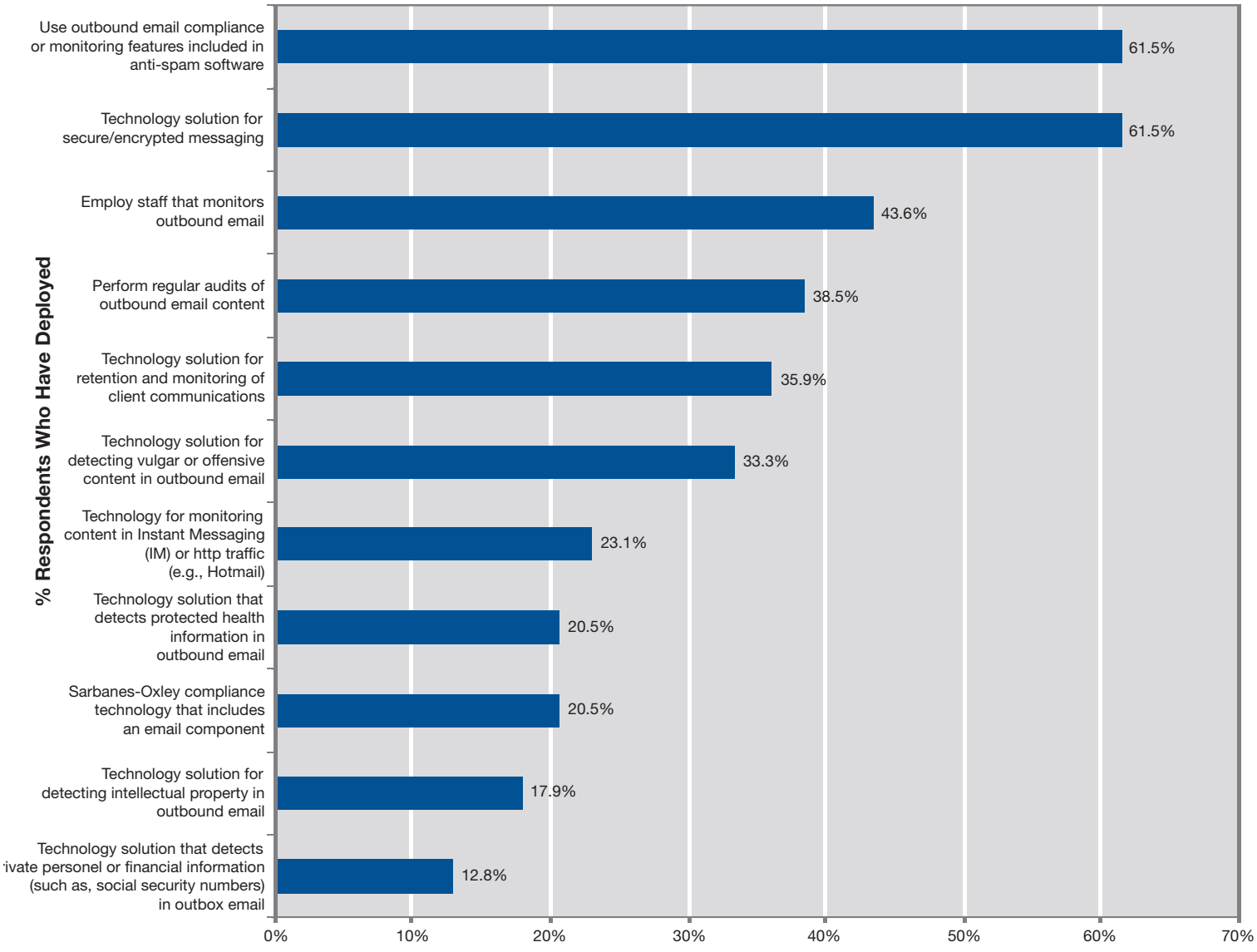


Figure 4: Adoption of techniques and technologies to mitigate outbound email risks in large organizations

Companies that Employ Staff to Monitor/Regularly Audit Outbound Email Content (By Industry)

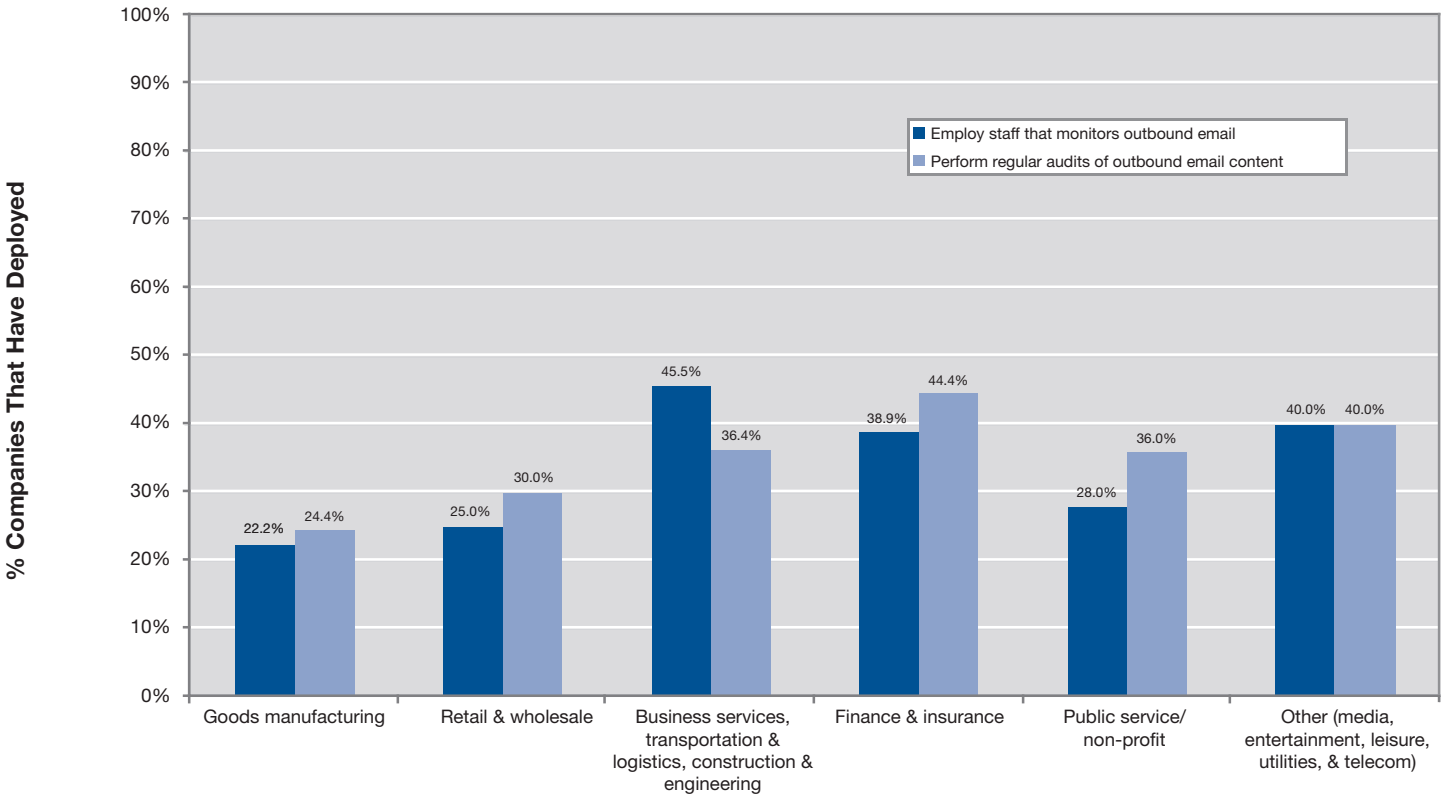


Figure 5: Who's reading your email?

Adoption of Technology Solutions for Mitigating Outbound Email Risk

In addition to the manual processes described in the previous section, the survey asked respondents about their deployment plans for a variety of outbound email compliance technologies. See again Figures 3 and 4 on pages 5 and 6. In general, large companies are more likely to have deployed these technologies.

More than half (52.1%) 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).

Messaging security systems are the next most popular technology, with 47.1% 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.

Roughly a third of respondents (33.6%) have deployed technology solutions for detecting vulgar or offensive content in outbound email messages.

More specific outbound email protection technologies are less well deployed in today's enterprise, including:

- Technology for retention and monitoring of client communications (30.7%)
- Technology for monitoring content in Instant Messaging or HTTP traffic (21.4%)
- Technology that detects protected health information (16.4%)
- Sarbanes-Oxley compliance technology that includes an email component (15.7%)
- Technology for detecting intellectual property in outbound email (11.4%)
- Technology that detects private personal or financial information in outbound email (10.7%)

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

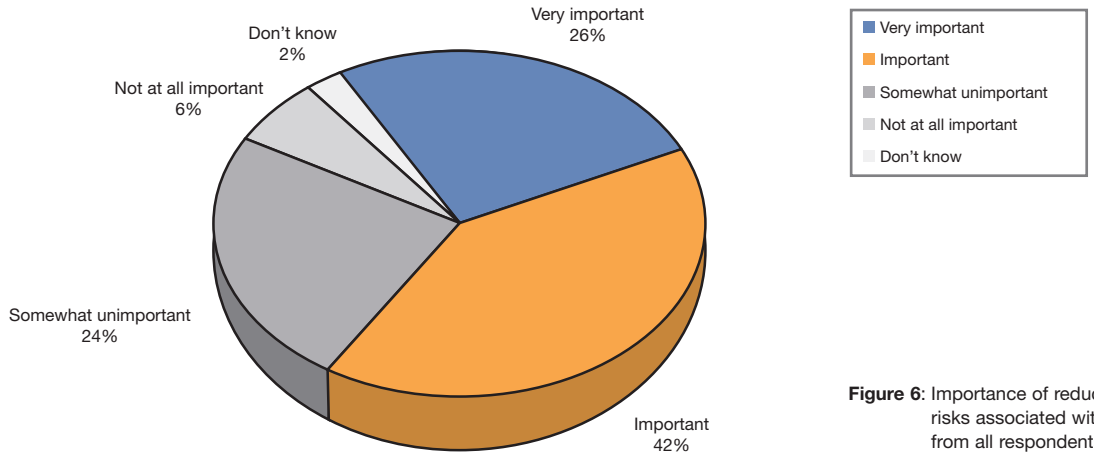


Figure 6: Importance of reducing legal and financial risks associated with outbound email — data from all respondents

Importance of Reducing Risks Associated with Outbound Email Content

The gap between the adoption of technology solutions for outbound email compliance/security (see "Adoption of Technology Solutions for Mitigating Outbound Email Risk" on page 7) and the level of concern around outbound email content (see "Enterprise Concerns about Outbound Email Compliance and Security" on page 1) suggests that there is a growing 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?"

- 68% of all companies said that such reductions were "very important" or "important" in the next 12 months (see Figure 6, above).
- Large companies display an even greater sense of urgency — 74% of companies with 20,000 or more employees said such risk reductions were "very important" or "important" (Figure 7 on page 8).

In both cases, only a small fraction of respondents said that such reductions were "not at all important" (6% of all companies and 5% of large companies).

Examining the data by industry shows that Financial Services and Insurance companies are the most concerned about reducing outbound email risks. 94.4% said it was "very important" or "important" to reduce the legal and financial risks associated with outbound email in the next 12 months.

Importance of Reducing Legal and Financial Risks Associated with Outbound Email in the Next 12 Months (Companies with 20,000+ Employees)

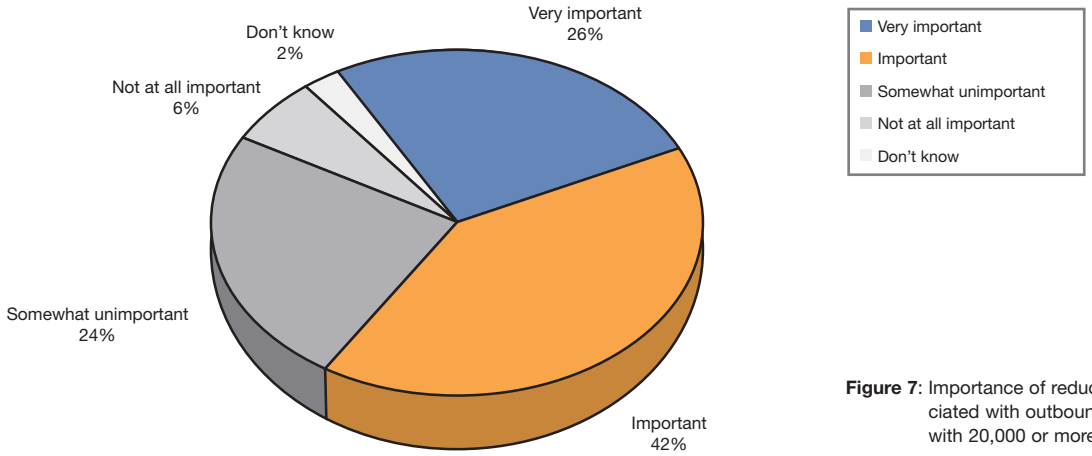


Figure 7: Importance of reducing legal and financial risks associated with outbound email — data from companies with 20,000 or more employees

Desired Features in Outbound Email Compliance Systems

The survey asked respondents to rate the importance of a wide variety of specific features and functionality provided by outbound email compliance systems. Highlights of the responses are summarized below.

Enterprises Desire a Platform Approach

The single feature rated as most important in an outbound email compliance solution was integration with anti-spam and anti-virus technology. Nearly all respondents (92.9%) rated this feature as "very important" or "important", suggesting that companies desire a single platform for mitigating both inbound and outbound messaging threats.

In addition, 75% of respondents said it was very important or important to be able to apply such a system to instant messaging streams (IM) or web-based email (e.g., Hotmail usage from inside the enterprise).

Most Desired Outbound Content Detection Features

Echoing the survey's findings about companies' current levels of concern around specific outbound email topics, the survey found:

- 82.9% of respondents rated the ability to detect breaches of specific confidential internal memos in outbound email as important or very important.
- 80.7% rated the ability to detect breaches of confidential company financial information in outbound email as important or very important.
- 77.9% rated the ability to detect breaches of intellectual property in outbound email as important or very important.

Desired Integration Points

The most desired integration points for outbound email compliance systems were as follows:

- 80.7% of respondents said that integration with secure/encrypted messaging systems was important or very important.
- 67.1% of respondents rated integration with archiving systems as important or very important.
- 56.4% of respondents rated integration with personnel/HR systems as important or very important.

About Proofpoint, Inc.

Proofpoint provides business software for large enterprises to stop spam, protect against email viruses, and ensure compliance with corporate policies and regulations throughout their messaging infrastructures. The company's flagship product, Proofpoint Protection Server™, is a software breakthrough that employs Proofpoint MLX™, an advanced machine learning technology that delivers adaptive protection to automatically defend organizations against emerging types of message-borne threats. This same technology is also available as a hardened, zero-administration appliance, the Proofpoint P-Series Appliance™.

Proofpoint Solutions for Outbound Email Compliance

Proofpoint's Content Compliance Module works in conjunction with an organization's established corporate policies to ensure that compliance is enforced throughout the company's email infrastructure. With the Content Compliance Module, companies can define policies and any suspect or non-compliant email is flagged and can be quarantined for further review or audit, prior to exposing the company to any liability.

Proofpoint helps customers gain control over their inbound email streams by eliminating spam and viruses, but also helps enforce corporate and external policies related outbound, reducing the risk of unauthorized communications such as:

- Confidential material that could be damaging in the hands of a competitor
- Offensive or restricted content, such as pornography or copyrighted material
- Financial information that could breach securities regulations and/or negatively impact a company's stock price
- Customer or patient information that could violate privacy policies or regulations such as Sarbanes-Oxley, HIPAA and Gramm-Leach-Bliley.

Proofpoint MLX™—Machine Learning Technology

Proofpoint's proprietary MLX technology is a machine learning system developed by scientists and engineers at Proofpoint's Anti-spam Laboratory for classifying email based on custom policies and definitions. MLX combines traditional spam techniques such as Bayesian analysis, with more advanced machine learning technologies such as Logistic Regression and Support Vector Machines to provide the industry's best spam-detection rates. Proofpoint's MLX technology is constantly learning from experience and, as a result, is able to stay ahead of new spamming techniques and predict the newest spam attacks as they occur (as opposed to reactive community or signature-based products that require prior review of each message before spam can be detected).

For More Information

proofpoint

19400 Stevens Creek Boulevard, Suite 100
Cupertino, CA 95014
Phone: 408-517-4710
Email: info@proofpoint.com
Web: www.proofpoint.com

Appendix: Respondent Demographics

The 140 respondents to this survey represented a wide variety of IT decision makers including:

Titles: % Respondents:

- CEO, CFO, COO or Senior Finance Executive: 1.4%
- CIO, CTO, CSO, or Senior-most IT Executive: 16.4%
- VP or Executive of IT: 7.9%
- Director or Manager of IT: 52.9%
- Director or Manager of Messaging/Email Systems: 2.8%
- Contributor to IT: 18.6.%

The size of the surveyed companies was reported as follows:

Number of Employees: % Respondents:

- 1000 to less than 5000: 35.7%
- 5000 to less than 20,000: 36.4%
- 20,000 or more: 27.9%

Of the responding companies, 55% were publicly traded companies and 45% were privately held. These companies represented a wide variety of industries, reported as follows:

Industry: % Respondents:

- Primary production and raw materials manufacturer: 5.0%
- Consumer products manufacturer (e.g., CPG): 12.9%
- Chemicals and petroleum manufacturer: 0.7%
- High-tech products manufacturer: 9.3%
- Industrial products manufacturer (e.g., automotive): 4.3%
- Retail (e.g., food and beverage): 7.1%
- Wholesale (e.g., durable and non-durable goods): 7.1%
- Transportation and logistics: 5.0%
- Professional services (e.g., consulting, accounting, legal, etc.): 8.6%
- Construction and engineering: 2.1%
- Media, entertainment, and leisure: 3.6%
- Utilities: 2.1%
- Telecom carriers: 1.4%
- Financial services: 6.4%
- Insurance: 6.4%
- Public services (e.g., government): 10.7%
- Non-profit: 7.1%

About this Report

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