

## WHITE PAPER

---

# Data Protection and Compliance: Improve Security, Manage Risk, and Lower Costs

Sponsored by: Accenture and Symantec

---

Irida Xheneti  
May 2009

## IDC OPINION

In today's business environment, a variety of business models and solutions have emerged to ensure business success. At the forefront of success lies information, which has become the single most important asset to an organization's success, whether it's customer information, confidential corporate information, or financial information. Due to the increased dissemination of information through various means, organizations are now preoccupied with ensuring that information assets remain secure and readily available to their remote employees, customers, and partners. To meet these business objectives, enterprises are heavily investing in technologies and services that will enable them to be competitive and to reach their business objectives. With technology advancements and the move toward an open IT infrastructure required to stay competitive comes a plethora of security vulnerabilities, business disruption, and security infrastructure challenges, such as data breaches, data loss, noncompliance, decreased customer confidence, and many more. This landscape becomes more complex during a downturn in the economy, when data breaches increase while organizations look to cut costs and remain secure and compliant with industry regulations. IDC recommends that enterprises use the following strategy to ensure the integrity and security of their enterprise IT infrastructure:

- ☒ **Conduct periodic security and compliance assessments.** Enterprises should consider periodic security architecture assessments and compliance audits to better understand their security and risk posture to implement the right security and compliance solutions.
- ☒ **Understand the business as well as the security threats and their impact on the business.** Through periodic assessments, a trusted security partner relationship, and a proactive security strategy, enterprises will be able to better understand the business value of their security investments. By better understanding their business and the impact of security threats on their business, customers will be able to prioritize their security investments accordingly as well as determine the best method to remediate threats.
- ☒ **Consider off-loading cost and managing risk.** For many companies, resource constraints can compromise the development of a comprehensive security strategy. As a response to this situation, many service providers have developed cost-effective security solutions to enable customers to reduce cost and focus resources on core business while gaining access to security skills and expertise that the organization may lack. The use of third-party service providers also can enable organizations to improve their internal processes and procedures to meet compliance regulations and manage risk proactively.

This white paper is based on a survey of more than 250 IT security senior executives at Fortune 5000 organizations in the United States and Europe.

## **SITUATION OVERVIEW**

Enterprise security has become a mission-critical component of the IT infrastructure and an important business enabler. Recent data breaches, customer data loss, and compliance regulations have dramatically altered the perception of IT security investments and have propelled the security conversation to the C-level suite due to how closely security is tied to business results and brand image. This change in security perception and the increased level of attention from C-level executives serve as evidence of the evolution of security's place in the IT infrastructure ecosystem.

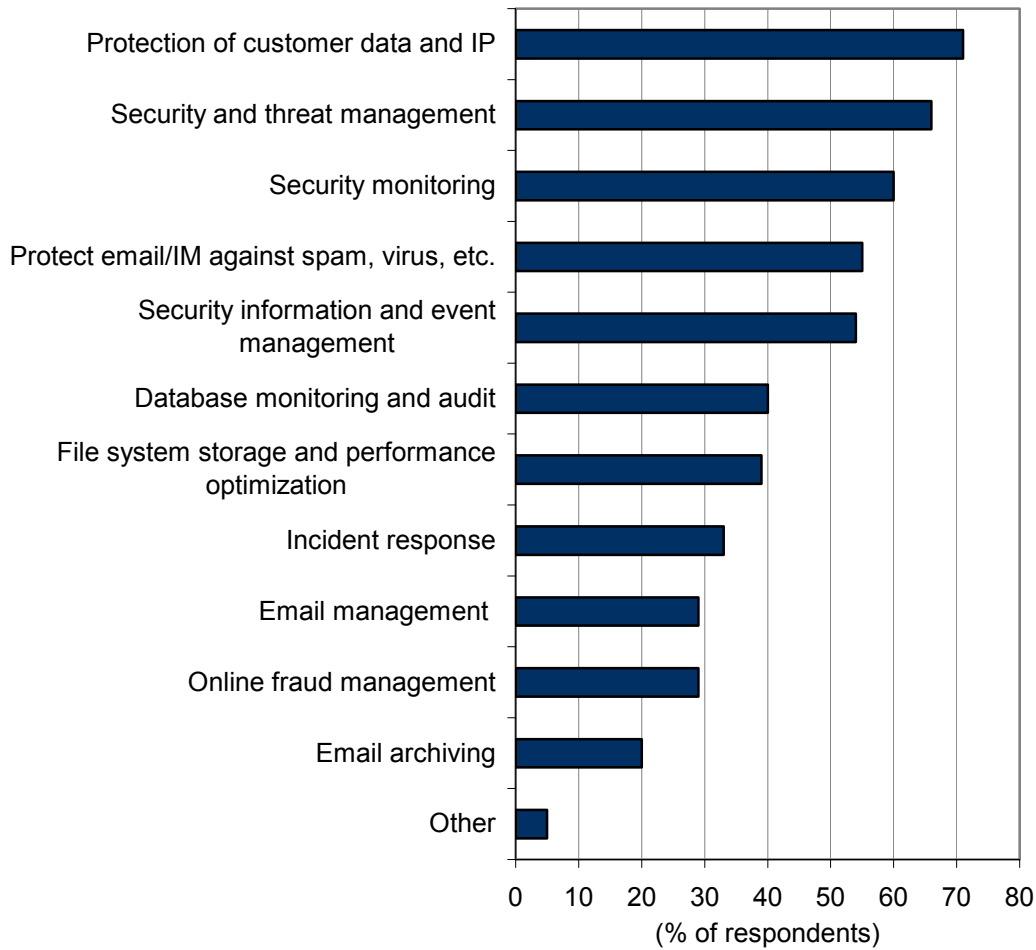
In the current economic environment, when customers are cutting discretionary spending and placing IT projects on hold, IDC believes that security spending will continue to exhibit healthy growth rates and will not be as significantly impacted as other spending by this downturn. Companies will continue to invest in protecting critical IT assets and information but will increasingly need to find ways to justify their investments at a time when IT spend will come under heavy scrutiny.

When customers were asked what additional measures would be needed to justify IT security spend, 52% stated that additional return on investment (ROI) analysis performed in-house would be required, while 36% would hold off on any security investments unless a security breach or event occurred. IDC believes that despite the desire to perform in-house ROI analysis, many companies may lack the skills necessary to adequately measure ROI. As a result, IDC believes that there is an opportunity for security providers that can demonstrate an approach to measuring ROI that is far superior to what an organization can achieve on its own. Additionally, an approach that has achieved proven results will also be highly valued.

IDC continues to see many enterprises continue to proactively manage risk for their IT infrastructures, and we believe that this trend will only intensify as security vulnerabilities evolve. As the security threat landscape evolves, companies are investing in a number of areas to defend against a variety of internal and external threats. As a result, many companies are prioritizing security investments based on the overall impact on the business. According to survey results, the primary focus areas for enterprises are protection of customer data and intellectual property (IP), security and threat management, and security monitoring (see Figure 1).

**FIGURE 1**

Top IT Security Projects



Source: IDC, 2009

**Compliance**

Evolving government and industry regulation requirements continue to be a significant driver for security. Initiatives to protect consumers and enterprises have become a complex challenge for many enterprise customers as they open their IT infrastructure for their customers and partners to access and also maintain transparency to meet compliance regulations.

Regulations such as the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act (SOX), ISO 17799/27000 series, ITIL, PCI, EU Data Protection Directive, PIPEDA, and USA PATRIOT Act require companies to develop a set of security best practices, assess their compliance road maps, and implement the right policies to protect customer and enterprise information. Furthermore, meeting these mandates can be very difficult for companies that lack the internal resources to implement the appropriate tasks.

IDC surveyed customers in both the United States and Europe to better understand the types of tools used to report and achieve compliance with industry and government regulations as well as to understand the specific types of compliance regulations impacting businesses in each region and the effectiveness of the compliance solutions available in the market today.

Figure 2 demonstrates spending on specific regulations by region for the next 12 months. The priorities for the U.S. region are HIPAA, primarily driven by the healthcare industry and the increased need to securely store and access customer information, and Sarbanes-Oxley, primarily driven by the need to regulate and establish standards within all U.S. public company boards and management and public account firms as well as the need to strengthen corporate accounting controls. It's important to note that HIPAA and Sarbanes-Oxley also impact organizations with operations in the European region.

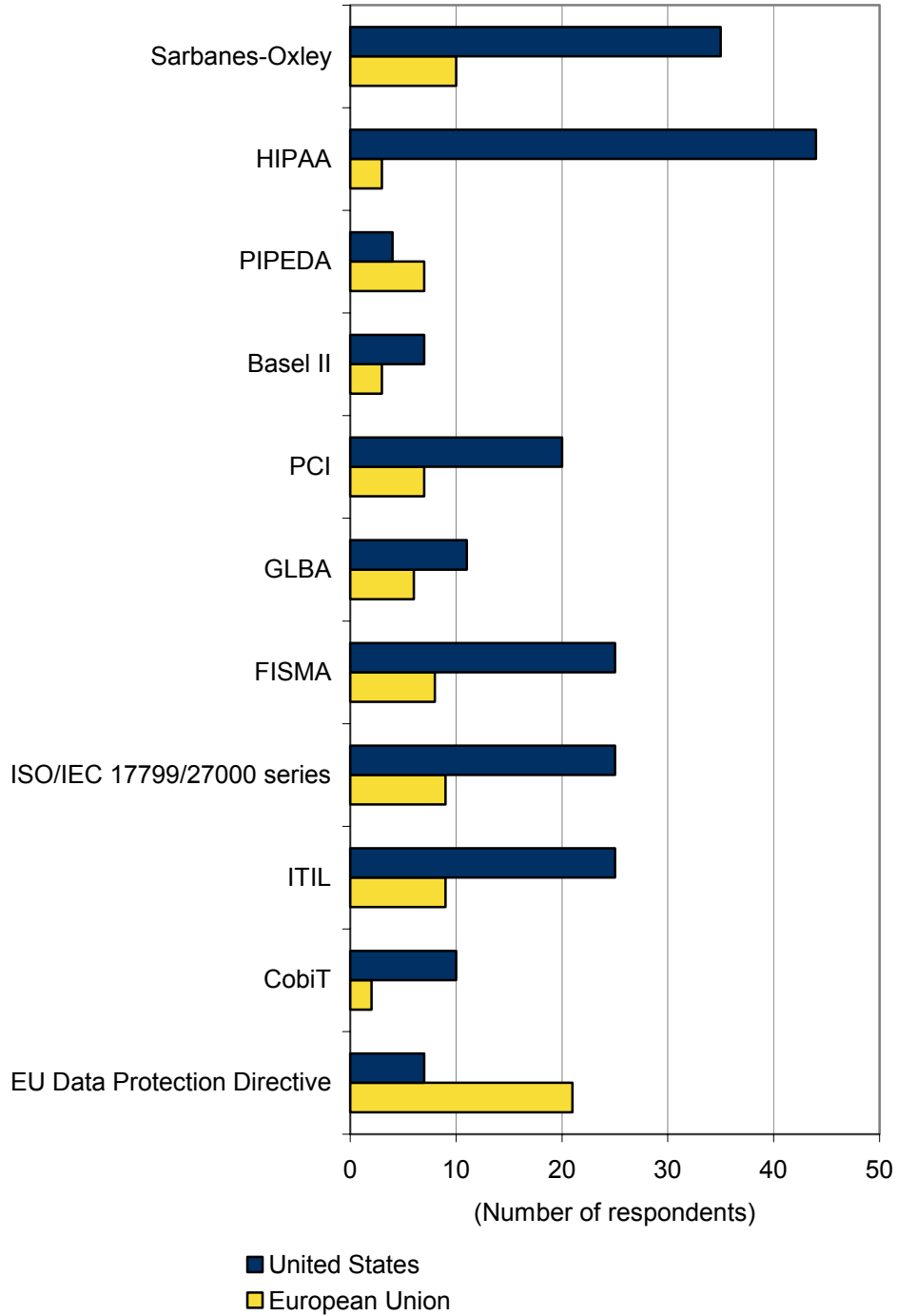
ISO/IEC 17799/27000, which consists of a series of guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization, continues to show strong customer spending; ITIL is driven by the need to manage, develop, and operate the IT infrastructure; the EU Data Protection Directive is primarily driven by the need of the 25 EU states to adhere to strict standards when monitoring employee activity and collecting personally identifiable information (PII); PCI is a multifaceted security standard that was derived by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. to help facilitate the broad adoption of consistent data security measures on a global basis. This regulation has primarily had an impact on the financial services, retail, and manufacturing verticals where protecting cardholder information has been a primary concern.

The European region has experienced the same trends as the U.S. region with the exception of a few regulations that are unique to the European region. The EU Data Protection Directive is the primary regulation in which customers expect to invest during the next 12 months. PIPEDA, consisting of requirements to support and promote electronic commerce by protecting personal information that is collected, used, or disclosed in certain circumstances, is another regulation in which customers in the European region expect to invest during the next 12 months.

Companies are using a variety of methods to meet compliance regulations. According to survey results, 38% of respondents use third-party tools and products to meet compliance regulations, 34% of respondents use tools developed in-house, and 27% of respondents use service providers to assist them with their compliance initiatives. These results portray a significant trend in the market where customers are starting to deploy more third-party tools to alleviate complexity and improve their internal processes and procedures.

**FIGURE 2**

Compliance Regulations Spending Focus by Region in the Next 12 Months



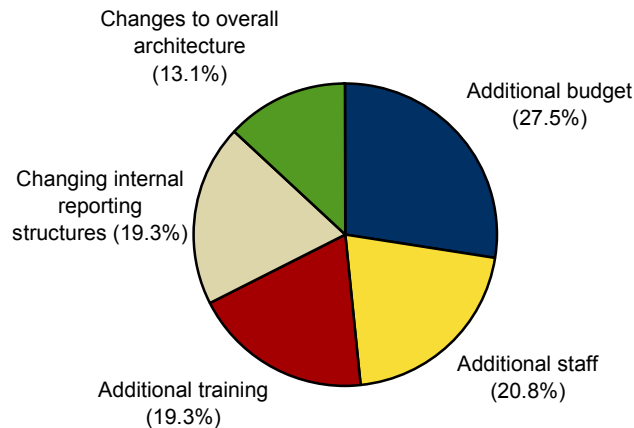
Source: IDC, 2009

IDC also discovered that customers are utilizing several methods to discover internal security vulnerabilities and ensure that their enterprises meet compliance regulations. Fifty-five percent (55%) of respondents use in-house assessment solutions to discover internal security vulnerabilities, while 42% of respondents utilize third-party assessment solutions. This trend comes as a result of the sensitivity of work around discovering potential vulnerabilities. However, this is a great opportunity for service providers to demonstrate to customers the risk they could be exposing the enterprise to by using only in-house solutions. This could result from a lack of up-to-date vulnerabilities information, which is where the third-party assessment solutions really demonstrate value. To meet future compliance regulations, customers feel the pressure of requiring additional staff, additional training, and additional budget, as illustrated in Figure 3. This represents a significant increase in cost and, given the current economic downturn, becomes a very difficult task for many enterprises looking to reduce cost.

Building a strong value proposition around cost reductions and risk sharing with a third party will resonate strongly with companies that want to invest in minimizing their security profile but lack the resources to do so in an adequate manner. Through a service provider model, customers can leverage their IT security expertise and experience in delivering large IT projects in complex environments while allowing customers to concentrate on their core business. In the current economic environment, IDC believes that outsourcing of security services will become more commonplace as organizations look to reduce costs and streamline their security operations.

**FIGURE 3**

Business Impact from Compliance Regulations



Source: IDC, 2009

Furthermore, as organizations look for trusted third-party providers to help manage their operations, a clear picture of customer selection criteria has evolved. Through this survey, IDC discovered that the top 3 service provider qualifications are security expertise, IT expertise, and demonstrated effectiveness in delivering large and complex projects. IDC believes that these market dynamics will evolve over time and that more enterprises will look to utilize more third-party solutions as organizations gain a better understanding of the relationship between cost and risk.

---

## **Securing the IT Infrastructure**

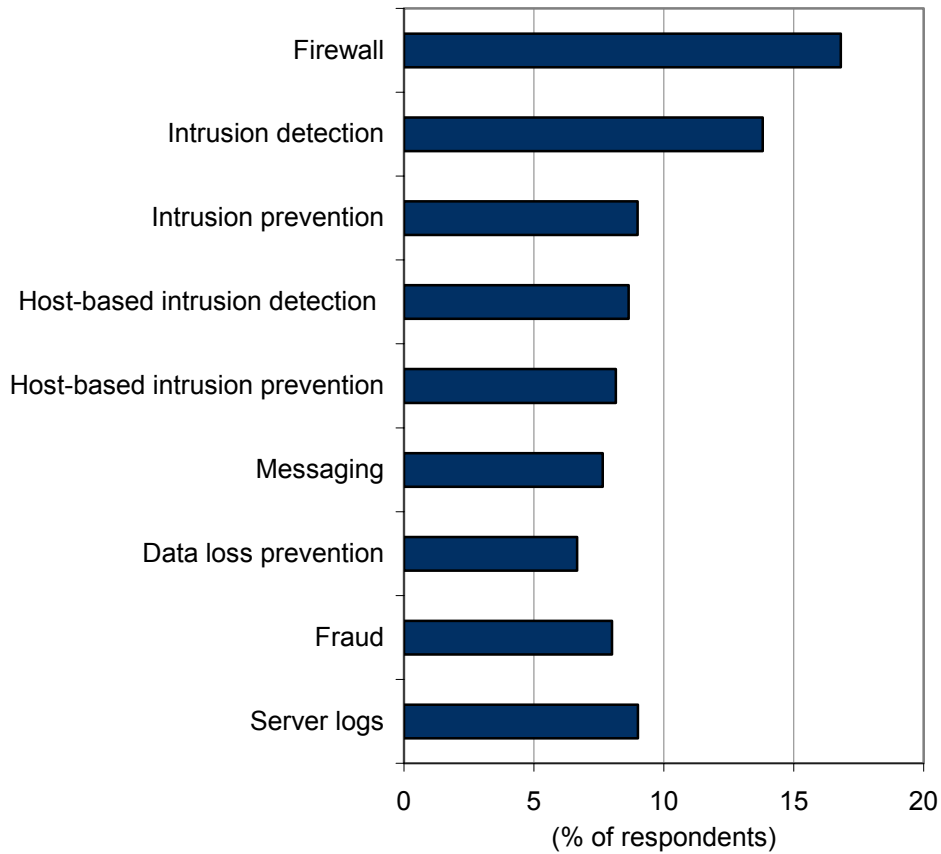
Today's technology is evolving rapidly and is having a tremendous impact on businesses. New mobile devices, VoIP communications, and wireless networks, as well as many other new technologies, become potential sources of security vulnerabilities. While these new technologies increase productivity, they also pose a significant threat to the enterprise infrastructure by increasing the potential number of internal and external vulnerabilities. Furthermore, during this economic slowdown, many organizations are going through major organizational restructuring. During this process, many identity access gaps will need to be secured to protect the enterprise from any disgruntled employees and data loss. Therefore, while securing the perimeter is a priority, internal threats constitute a silent threat to an organization. To address these security concerns, organizations need to have a proactive risk management strategy that enables them to identify and prioritize the most critical assets that need to be secured and that allows them to verify that proprietary data is not leaving the network perimeter. According to the customers surveyed, 43% of respondents utilize both internal assessments and third-party assessments to help them identify the most critical assets that will need to be protected, while 37% of respondents utilize only internal assessment processes and 21% use only third-party assessments. Again, this finding indicates that customers' perception of utilizing third-party solutions has evolved, and IDC believes that this trend will continue to progress as customers develop trusted advisor relationships with service providers.

Furthermore, organizations need a secure and cost-effective way to manage their networks, systems, and applications, as well as their information assets, while staying focused on their primary business. In addition, security processes require constant review as well as policy enforcement, given the volume and severity of external threats such as viruses, spam, and denial of service and internal threats such as data leakage and new emerging vulnerabilities from the deployment of new technologies. IDC discovered that 75% of customers surveyed have deployed a proactive information security and event management strategy, while the rest still employ a reactive security strategy.

Customers also relayed that their security monitoring spending is primarily focused on firewall and data loss prevention solutions in both the United States and Europe. As important confidential information travels through a variety of technologies (laptops, mobile devices, portable hard drives), customers are increasingly concerned with data loss prevention. To add to that complexity, compliance regulations have also driven a portion of the spending around firewall and data loss prevention solutions. IDC expects this trend to continue for the next five years as customers will look to reduce the complexity and high cost of security and seek to improve internal security architecture and procedures (see Figure 4).

**FIGURE 4**

Spending Focused on Security Monitoring



Source: IDC, 2009

## FUTURE OUTLOOK

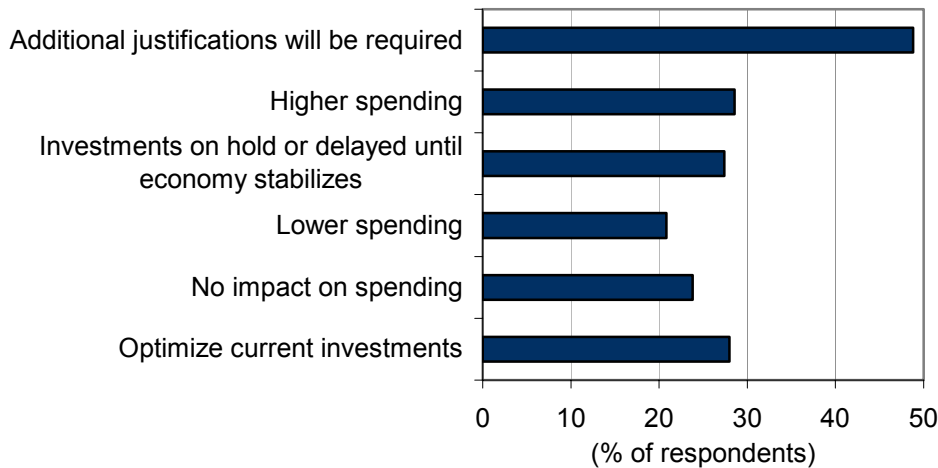
As IT budgets undergo cutbacks, security spending will not be one of the areas significantly affected by this economic downturn. Increased complexity around compliance, new technologies such as virtualization and mobility, and the impact of the economic downturn will continue to fuel customer demand for security consulting and security operations services to remain competitive in a crowded marketplace and stay compliant with industry regulations.

As organizations shift into conservative spending modes and reduce overall IT spending, security services will exhibit a more optimistic forecast over the next four years given the critical business impact of security on an organization's operations. The security services market will reveal strong customer demand for security consulting and security operations services.

IDC believes that as customers place expenditures on hold until uncertainty around the economic landscape clears up, 49% of survey respondents will be looking for further justification for their business-critical security investments. Services that are not considered business critical, such as education and training services, will be significantly reduced. See Figure 5 for additional information.

**FIGURE 5**

**Economic Crisis Impact on Security Investments**



Source: IDC, 2009

**CHALLENGES/OPPORTUNITIES**

- ☒ Enable customers to better understand cost versus risk to determine whether to develop in-house solutions or use a third party, or both. Service providers will need to demonstrate their security capabilities, IT capabilities, and effectiveness in delivering large and complex projects. To demonstrate value, service providers should leverage their partnerships and utilize the synergies to drive customer intimacy.
  
- ☒ Build strong relationships with the C-suite and develop a diversified go-to-market strategy, as security challenges ultimately translate into business challenges that require multitiered engagement models. Leverage core competencies associated with security and IT to build a strong value proposition. The economic downturn presents a challenge for service providers because it is leading to more scrutinized IT projects. IDC believes that by arming customers with further justification for their IT security investments, service providers will be able to overcome this challenge. They should provide their customers with a cost versus risk approach for their IT projects so that they can prioritize the most business-critical investments.

- ☒ Gain customer mindshare around compliance, information security and event management, and security monitoring by demonstrating core competency through customer case studies. By understanding customers' business and the threat landscape, service providers will enable customers to prioritize their security investments.

## **METHODOLOGY**

Respondents were invited via email to participate in an online survey regarding security and compliance enterprise services.

To qualify for this study, respondents needed to have 1,000 or more employees and be located in the United States or Europe. In addition, respondents needed to be in a senior-level security position (e.g., CSO, CISO, director of security, VP of infrastructure).

Two hundred and sixty six respondents successfully completed the survey. Fifty-nine percent (59%) of respondents were based in the United States, and 41% were based in Europe.

The survey was conducted in November 2008.

Data presented in this document is consistent with data in recent IDC studies and research.

---

## **Copyright Notice**

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2009 IDC. Reproduction without written permission is completely forbidden.