

# Borderless security

Ernst & Young's 2010

Global Information Security Survey



Foreword .....	1
Borderless security .....	2
Data on the move.....	4
Processing in the clouds .....	8
Web connections.....	12
Summary .....	16
Survey approach.....	18
About Ernst & Young.....	20

# Foreword

The ways in which organizations interact with their people and with other organizations are changing at an unprecedented rate. Through mobile computing and new technologies like cloud computing and social media, the connections and flow of information now reach far beyond the walls of the conventional office.

The result is that the traditional boundaries of an organization are vanishing along with the traditional information security paradigm. Information security programs must expand and adapt to meet the demands of the new and existing enterprise in an evolving borderless world.

Our 2010 survey results are encouraging in that many organizations recognize the risks associated with current trends and new technologies. They are taking the necessary steps to protect their information – no matter where it resides – by adopting new solutions and improving overall information security program effectiveness. However, our survey also reveals that some organizations are challenged to keep pace with emerging threats and risks due to a more connected, virtual business environment.

The Ernst & Young Global Information Security Survey is one of the longest running annual surveys of its kind; we are very proud that for thirteen years our survey has helped our clients focus on the most critical risks, identify their strengths and weaknesses and improve their information security. We are also excited that this year's survey attracted nearly 1,600 participants from 56 countries, demonstrating that information security remains an important issue for our clients.

I would like to extend my warmest thanks to all of our survey participants for taking the time to share their views on information security.

My colleagues and I hope you find this survey report useful, informative and insightful. We would welcome the opportunity to speak with you personally about your specific information security risks and challenges, and believe that such discussions would assist you in addressing your borderless security issues, enabling you and your organization to achieve your full potential.

Paul

Paul van Kessel  
Global Leader,  
IT Risk and Assurance Services

# Borderless security

**60% of respondents perceived an increase in the level of risk they face due to the use of social networking, cloud computing and personal devices in the enterprise**

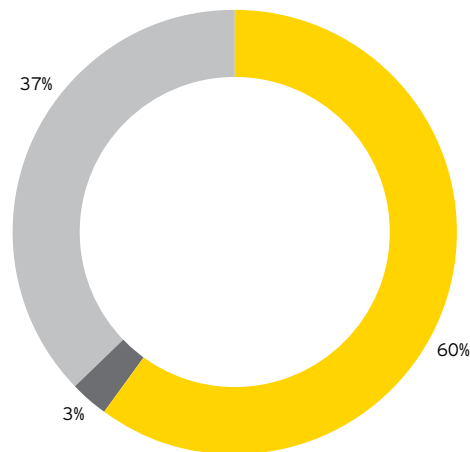
The trend toward anywhere, anytime access to information will continue changing the business environment, blurring the lines between home and office, co-worker and competitor, and removing traditional enterprise boundaries.

The pace of change is accelerating, and the companies that embrace it are more likely to fare better than those resisting it. Over the last year, we have witnessed a significant increase in the use of external service providers and the business adoption of new technologies such as cloud computing, social networking and Web 2.0. We have also seen technology advances that have provided an increasingly mobile workforce with seemingly endless ways to connect and interact with colleagues, customers and clients. Together, these changes are extending the enterprise – driving professional collaboration and personal interaction to new levels. These new technologies represent an opportunity for IT to deliver significant benefits to the organization and fulfill the initial promise – or hype – that many technologies have failed to live up to in the past.

However, new technology also means new risk.

The rising level of risk has not gone unnoticed by our survey participants; 60% of respondents perceived an increase in the level of risk they face due to the use of social networking, cloud computing and personal devices in the enterprise. It is in this changing and borderless environment that information security professionals must find a way to manage risks and protect their organizations' most critical information assets.

**Given current trends towards the use of such things as social networking, cloud computing and personal devices in the enterprise, have you seen or perceived a change in the risk environment facing your organization?**

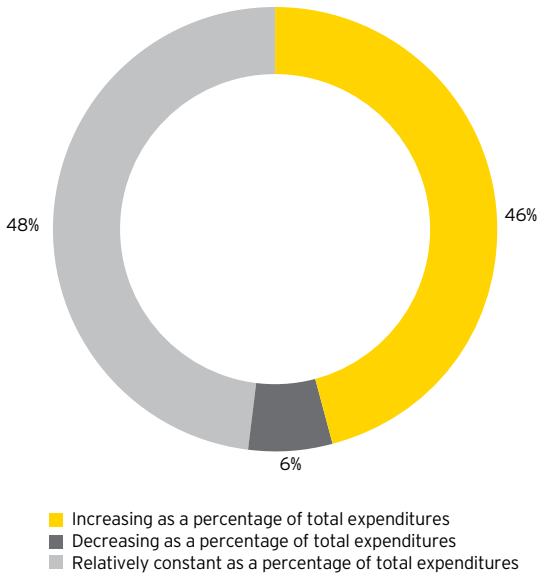


■ Yes, increasing level of risk  
■ No, decreasing level of risk  
■ Relatively constant level of risk

Shown: percentage of respondents

Despite continued economic pressures, organizations are spending more to address information security challenges, including those related to delivering security in a borderless environment. 46% of respondents indicated that their annual investment in information security is increasing, with only 6% planning to reduce their information security investment. Further investigation found that 55% of respondents are increasing the level of information security investment related to their top five areas of IT risk.

Which of the following statements best describes your organization's annual investment in information security?



Shown: percentage of respondents

---

**46% of respondents indicated that their annual investment in information security is increasing**

---

The survey findings are encouraging, but increasing investment alone will not provide guarantees of protection. Companies must also establish more comprehensive IT risk management programs that identify and address the risks associated with new and emerging technologies. Our survey revealed that this is one area that most organizations could improve upon, as only 30% of respondents indicated that they have an IT risk management program in place that is capable of addressing the increasing risks related to the use of new technologies.

In this report, we take a closer look at how organizations are specifically addressing their evolving information security needs in the changing, borderless environment. We also examine potential opportunities for improvement and identify important short and long-term trends that will shape information security in the coming years.



# Data on the move

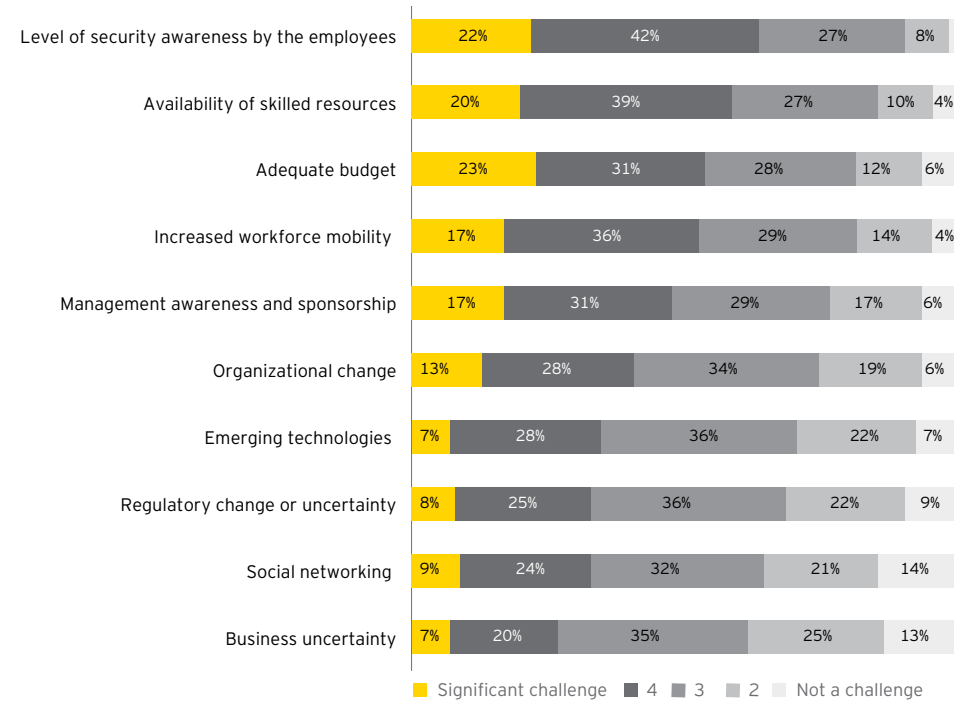
**53% of respondents indicated that increased workforce mobility is a significant or considerable challenge to effectively delivering their information security initiatives**

## The mobile workforce

As today's mobile workforce continues to grow, not only is the phrase "out of the office" becoming less relevant, but the flow of information in and out of the organization is also dramatically changing. Mobile computing devices (e.g., laptops, tablet PCs, multimedia-enabled smartphones) are in widespread use, allowing individuals to access and distribute business information from anywhere and at any time. Recent improvements in mobile applications, bandwidth and connectivity have made it possible to interact with information like never before: accessing information-intensive reports, retrieving corporate data and even conducting remote meetings from a mobile device.

The increasing demand for information from the mobile workforce is driving changes in the way organizations support and protect the flow of information. This presents a noteworthy challenge for many of our survey participants; 53% of respondents indicated that increased workforce mobility is a significant or considerable challenge to the effective delivery of their information security initiatives, especially when coupled a security-awareness challenge identified by 64% of respondents.

**What is the level of challenge related to effectively delivering your organization's information security initiatives for each of the following?**





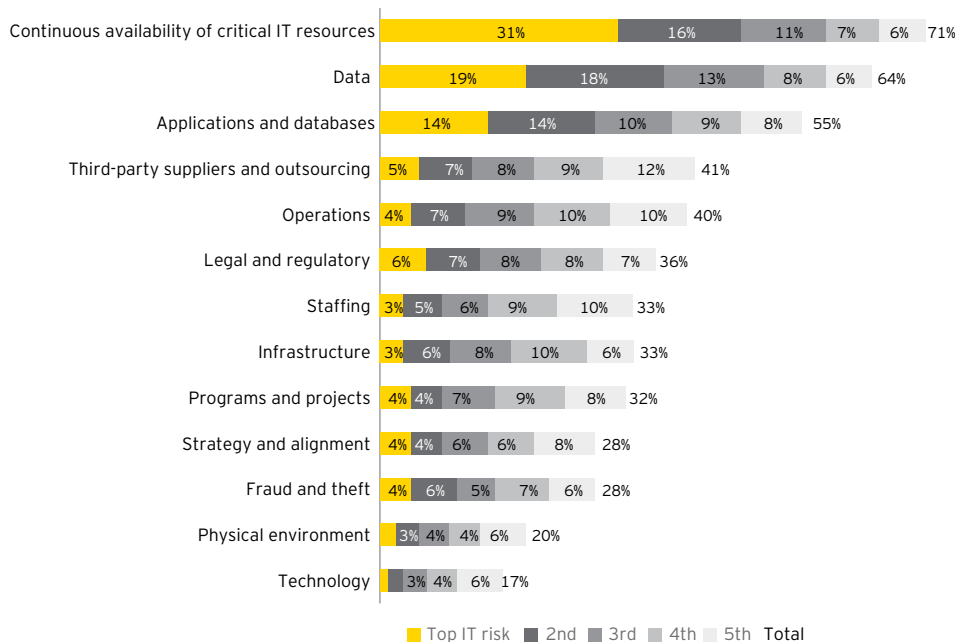
## Mobile computing risks

The increased use of mobile computing devices for business purposes is not without serious risks. The popularity and widespread use of these devices has led to the unwanted, but somewhat predictable, outcome of such devices becoming a target for computer viruses and sophisticated mobile malware. In addition, due to the small size of the portable devices, simple theft of the device is also a real concern.

The most serious risk associated with mobile computing is the potential loss or leakage of important business information. When we asked our survey participants to identify their top five areas of IT risk, 64% of respondents indicated that data (i.e., disclosure of sensitive data) was one of their top five IT risk areas, second only in overall ranking to the continuous availability of critical IT resources.

**64% of respondents indicated that data (i.e., disclosure of sensitive data) was one of their top five areas of IT risk**

From the following list, which are the top five areas of IT risk for your organization?



Shown: percentage of respondents

Furthermore, when we examined the risk environment in the context of the current trend toward the use of personal devices in the enterprise, 52% of our survey respondents perceived an increase in data leakage risks. (See page 10.)

# Data on the move (continued)

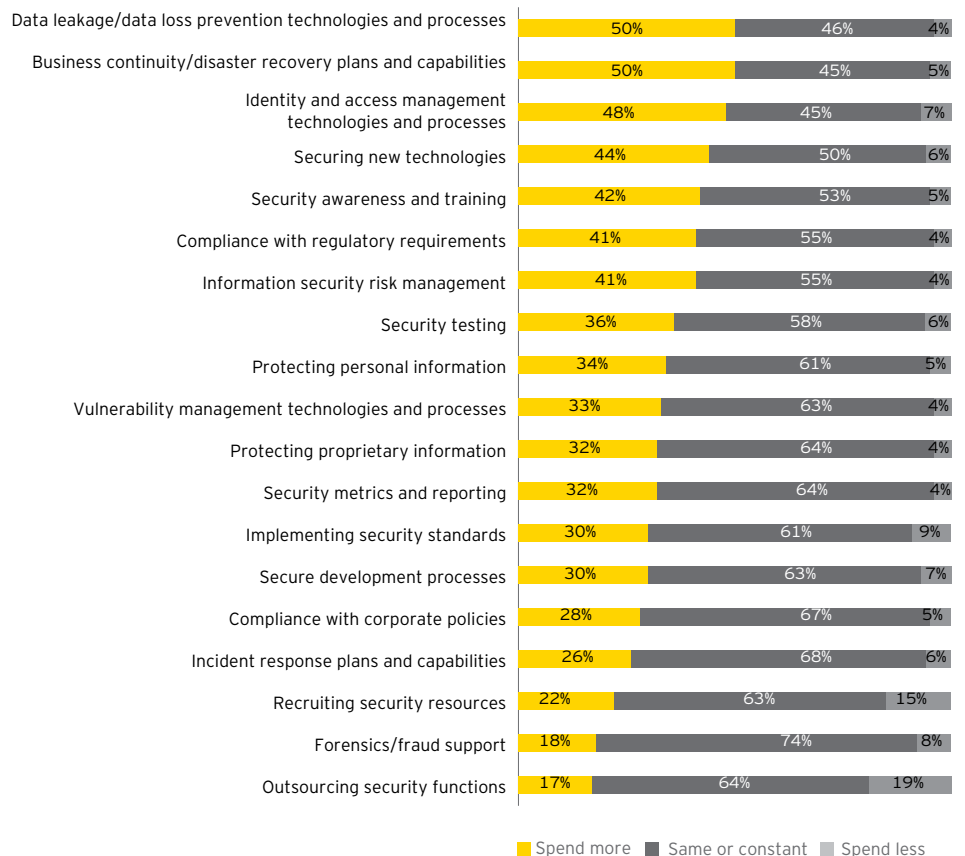
## 50% of respondents plan on spending more over the next year on data leakage/data loss prevention technologies and processes

### Plugging the leak

Based on our survey results, it appears that many organizations are recognizing the increased risks associated with mobile computing and are taking steps to address the issues. Survey results showed that 50% of respondents plan on spending more over the next year on data leakage/data loss prevention technologies and processes. This is a seven-percentage-point increase over last year and a clear indication that preventing data leakage is top of mind for many organizations.

Increased mobility and lack of control over end-user devices can also cause problems when trying to implement effective and efficient business continuity and disaster recovery capabilities – similarly identified by 50% of respondents as an area of increased expenditure.

Compared to the previous year, does your organization plan to spend more, less or relatively the same amount over the next year for the following activities?



Shown: percentage of respondents

### Data leakage prevention defined

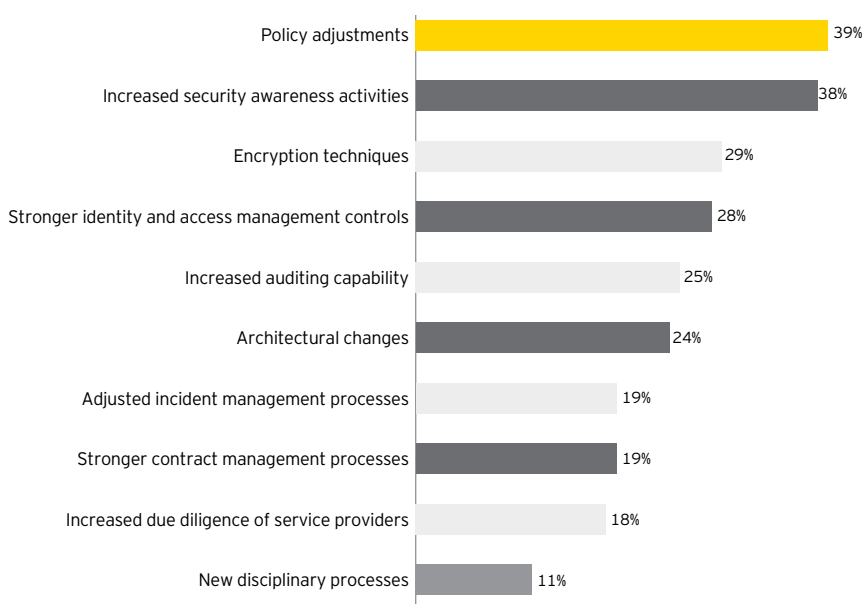
Data leakage prevention (also known as data loss prevention or information leak prevention) is the combination of tools and processes for identifying, monitoring and protecting sensitive data or information according to an organization's policies or government and industry regulations. Data leakage prevention services will typically focus on preventing specific data or information from leaking out of the organization and detecting any unauthorized access or transmission of sensitive data.



When we look closer at the steps organizations are taking to address the potential new risks, we found that 39% of respondents are making policy adjustments, 38% are increasing their security awareness activities, 29% are implementing encryption techniques, and 28% are implementing stronger identity and access management controls.

It is also important to note that 42% of our survey respondents currently have an IT risk management program in place, but only 30% have a program that also addresses the risks associated with mobile computing.

**Which of the following controls have you implemented to mitigate the new or increased risks?**



Shown: percentage of respondents

**Our perspective**

Our survey shows that as the mobile workforce continues to grow, so does the level of risk: many organizations are now recognizing this fact and are correspondingly increasing their investment in data leakage prevention technologies, encryption, and identity and access management services.

The risk of data loss is further amplified when the data provided to mobile devices is inappropriate or much more than needed to accomplish the task (e.g., an entire customer database). Companies must re-engineer information flows to ensure that only essential data is provided for mobile computing activities.

However, in addition to implementing new technology solutions and re-engineering information flows, companies must focus on informing their people about the risks. It is important that the business understands and accepts the risk created by the use of new technologies – this includes technologies personally adopted by their employees that may also be used for business purposes. To help manage these risks, information security policies should be reviewed and adjusted appropriately to establish acceptable use, and to define any specific restrictions related to mobile computing devices. The delivery of effective and regular security awareness training for the mobile workforce is also a critical success factor. Companies will need to increase these activities to keep pace with the changing environment.

As the mobile workforce continues to push the flow of information out beyond the traditional borders of the company, enterprise security must also encompass end-point devices to protect critical business information and provide better alignment with the organization's risk profile.

# Processing in the clouds

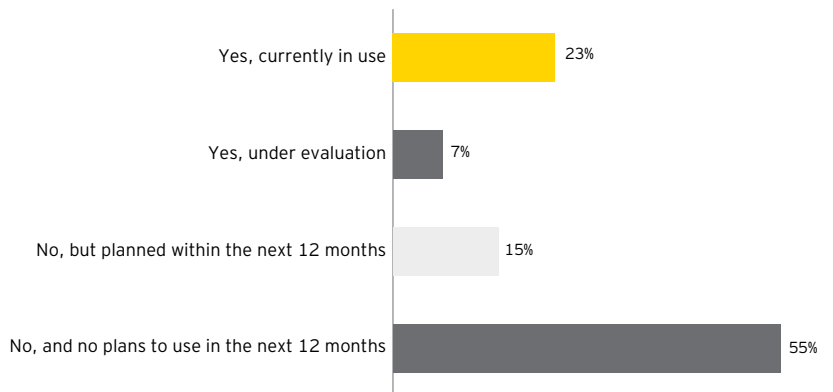
**45% of respondents are currently using, evaluating or are planning to use cloud computing services within the next 12 months**

## The cloud computing trend

Driven by pressures to reduce IT spending in the wake of an economic downturn and the need to enhance flexibility and speed of implementation, many companies are looking outside the organization for help. Their interest lies in computing services that require significantly less initial investment, fewer skilled internal IT resources and lower operating costs. As a result, cloud computing services are gaining greater adoption, and providers are expanding the range of services offered to include infrastructure (e.g., storage and CPU cycles), development platforms (e.g., open source, service-oriented architecture) and software (e.g., enterprise applications, office productivity, web-based email). In addition to having minimal up-front costs, cloud computing services are attractive because they offer shorter contract durations, on-demand scaling of resources, and a way to deliver leading IT services that would be beyond the budget threshold for many companies if delivered internally.

Our survey results showed that 23% of respondents are currently using cloud computing services, 7% are evaluating its use and 15% are planning to use within the next 12 months – a surprisingly high number given that the reliability and security level of many cloud services is still unknown. Despite an unproven track record, we expect cloud services to increase over the next few years as performance and benefits are demonstrated, offerings and capabilities expand, and cost-cutting pressures continue to force companies to look for alternative IT solutions.

## Does your organization currently use cloud-computing-based delivery solutions?



Shown: percentage of respondents

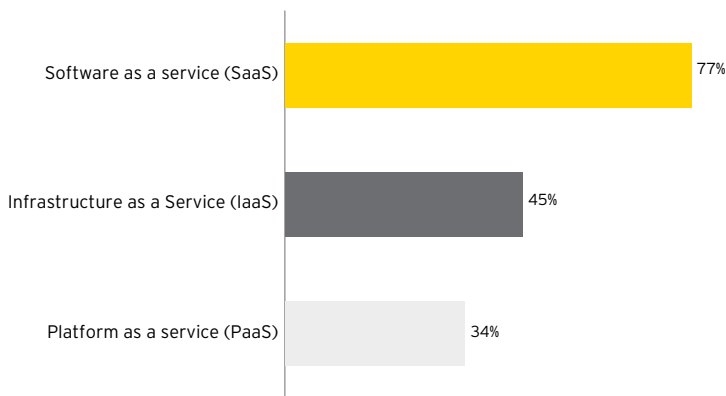
## Cloud computing defined

Cloud computing refers to pooled, on-demand computing resources across networks such as the internet as rapidly provisionable services (e.g., Software as a Service, Platform as a Service, Infrastructure as a Service). Cloud computing providers make use of several technologies, such as virtualization and service-oriented architecture, to efficiently deliver scalable computing services to customers.



In regard to the kind of cloud computing services being used, or planned to use, 77% of respondents indicated that they are using Software as a Service, 45% are using Infrastructure as a Service and 34% are using Platform as a Service as their cloud service model.

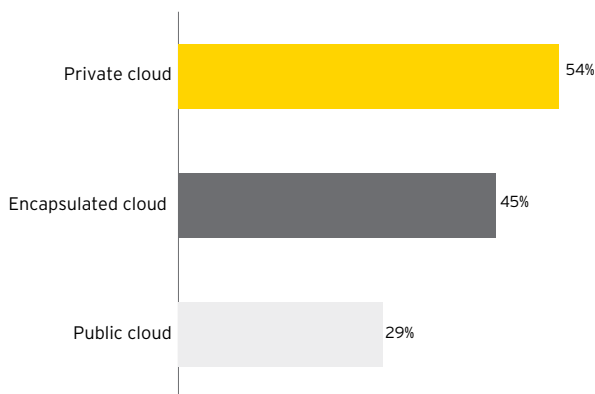
Which kind of cloud service are you using or do you plan to use?



Shown: percentage of respondents

Interestingly, 54% of respondents who use cloud services are using private clouds. These services dedicated solely for the organization – as opposed to being made available to the general public – may provide better data security, corporate governance and reliability. They do not, however, reach the full economic benefit potentials that a public cloud deployment model can provide. This supports the trend that we see within many organizations of adopting cloud technology while at the same time being cognizant of an infantile trust model for public cloud services.

Which kind of cloud technology are you using or do you plan to use?



Shown: percentage of respondents

## 77% of respondents who use cloud services indicated that they are using Software as a Service as the main cloud service model

### Cloud Software as a Service (SaaS) defined

The capability to use applications running on a cloud infrastructure that are accessible from various thin client devices (e.g., Web browser).

### Cloud Platform as a Service (PaaS) defined

The capability to deploy onto the cloud infrastructure custom or acquired applications created using programming languages and tools supported by the cloud provider.

### Cloud Infrastructure as a Service (IaaS) defined

The capability to provision processing, storage, networks, and other computing resources where the consumer is able to deploy and run software of choice, which can include operating systems and applications.

Source: National Institute of Standards and Technology (NIST)

# Processing in the clouds (continued)

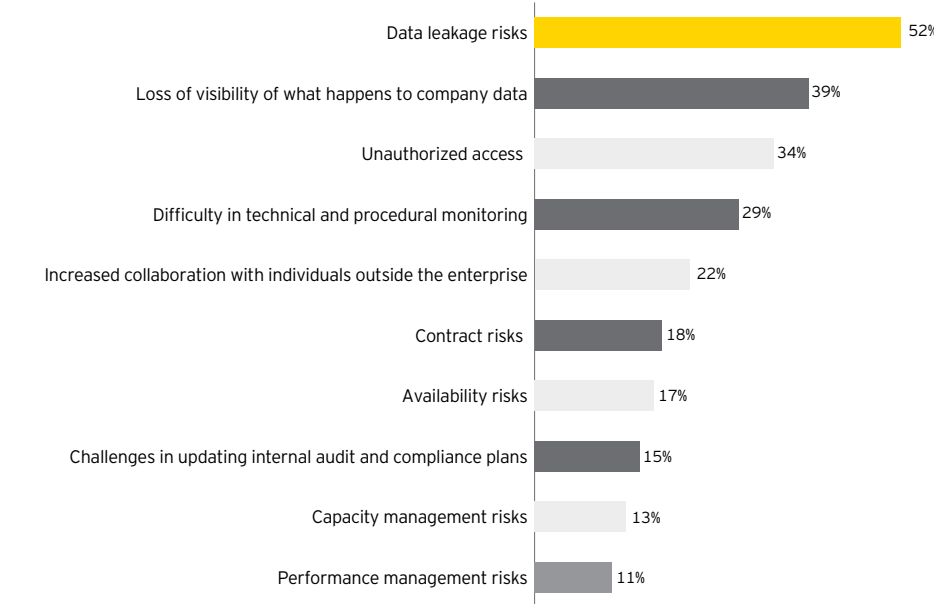
**39% of respondents cited the loss of visibility of what happens to company data as an increasing risk when using cloud-based services**

### Cloud computing risks

Although the potential benefits of cloud computing are very compelling, there are a number of important information security issues and risks that should be addressed before business critical applications are moved to the cloud. Due to the reliance on infrastructure that favors scalability and flexibility, cloud service providers may not be able to meet specific organizational or regulatory requirements for protecting sensitive information stored in the cloud. This means that not only will existing risks remain but new issues and risks will be introduced by adopting cloud computing.

The risks associated with cloud computing are not going undetected by our survey participants – data leakage was identified by 52% of respondents as an increasing risk resulting from current trends, and 39% of respondents cited the loss of visibility of what happens to company data as an increasing risk. Unauthorized access was also identified by 34% of respondents as increasing, which highlights the fact that many companies are concerned about giving up control of access to their business information and relying on the cloud to provide secure authentication, user credentials and role management.

Which of the following “new” or increased risks have you identified?



Shown: percentage of respondents

### Cloud attack: Economic Denial of Sustainability (EDoS) defined

During an EDoS cloud attack, a malicious attacker identifies an organization that relies upon on-demand cloud computing to conduct an aspect of its business. They then make bulk requests to it, to cause the cloud infrastructure to scale in response and increase the cost or reduce the quality of service for the organization.



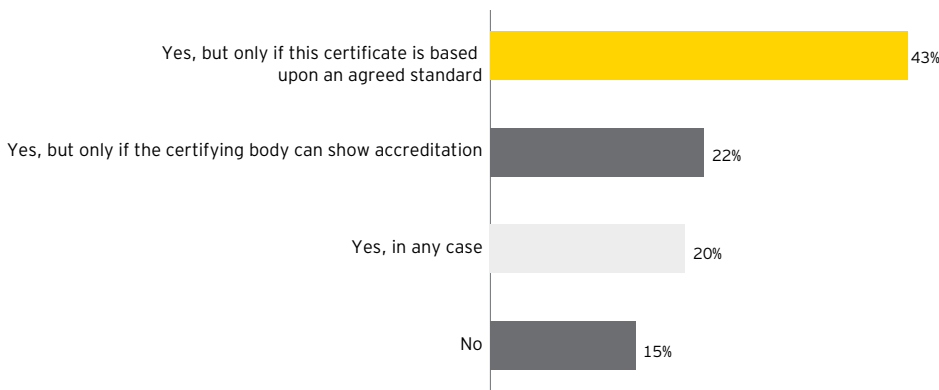
## Securing the cloud

The issues and risks related to cloud computing are significant, but most of them are not entirely new. Organizations can leverage lessons learned from managing IT outsourcing contracts – or from similar services that have been implemented behind the firewall – such as virtualization, which 76% of respondents are currently using.

Most importantly, organizations must define and establish minimum standards and security requirements for cloud services. Then, once a contract that meets the organization's performance and information security requirements is in place with the provider, the focus should turn to auditing and compliance. One-fourth of our survey respondents indicated that they have increased auditing capability and 19% of respondents have implemented stronger contract management processes to mitigate increased risks.

Certification is another option for evaluating or confirming the appropriateness of security controls for cloud services. When asked if an external certification of cloud service providers would increase trust, 85% of respondents said yes, with 43% stating that the certification should be based upon an agreed standard and 22% requiring accreditation for the certifying body.

### Would some kind of external certification of cloud service providers increase your trust in cloud computing?



Shown: percentage of respondents

### Our perspective

Our survey results show that the trend toward cloud computing services is one that will likely continue as more companies search for ways to reduce costs while at the same time deliver more IT functionality. Survey results also show that most organizations have identified the potential risks and are taking steps to address them, but as the request for cloud services may bypass the information security function, this will be a difficult and ongoing challenge.

Cloud computing will continue to mature and so will the security services offered by cloud providers. But companies do not need to wait until this happens to securely utilize cloud services. Organizations should assess the legal, organizational, and technological risks as well as the security issues related to placing information into the cloud. They should develop a strategy and an approach (that includes the information security function) to help define policies and guidelines, and set standards and minimum requirements, so that they can adopt cloud computing in as secure a manner as possible. Cloud computing may be a new technology trend, but like all new technologies with significant benefits, the security issues and risks must be addressed or the trend will end.



## Web connections

---

**33% of respondents indicated that social networking is a considerable challenge to effectively delivering information security initiatives**

---

### Social media

The workforce is changing; there is a new generation of workers that have never known a world without the internet, without social media and without sophisticated personal technology to access information 24 hours a day. They will spend countless time texting, chatting and browsing Facebook, LinkedIn, blogs, wikis and other social networking and social media websites. They have a new set of expectations regarding technology and their ability to connect to networks and communities, both inside and outside the business environment.

For most organizations, this means that in order to attract and retain the best and brightest people, they must find ways of providing the social networking and collaboration tools that these individuals have increasingly come to expect. To address this issue, many organizations are implementing infrastructure and applications that support social media usage inside the enterprise (known as Enterprise 2.0). Such social tools provide the new generation of employees with increased opportunities for professional collaboration and personal interaction but within the protected and secure environment of the business intranet. In addition, businesses are looking for new ways to make their people aware of the risks, policies and acceptable behaviors related to the use of such tools both internally and in the public environment.

### Identifying social media risks

Our survey results show that social networking is not high on the list of challenges for most of our participants (see page 4); only 33% of respondents indicated that social networking is a considerable challenge to effectively delivering information security initiatives. We believe this to be an indication that although most companies recognize the fact that there are risks and information security issues related to social media and Web 2.0, only a few have thoroughly examined the issue and developed an approach that will balance the business opportunity with the risk exposure.

The fact that only 10% of respondents indicated the examination of new and emerging IT trends as a critically important function is further evidence that few organizations have assessed the impact of social networking. The question we would like to ask is if the information security function is not evaluating the risks associated with new technologies and IT trends, such as social media, then which function within the organization is?

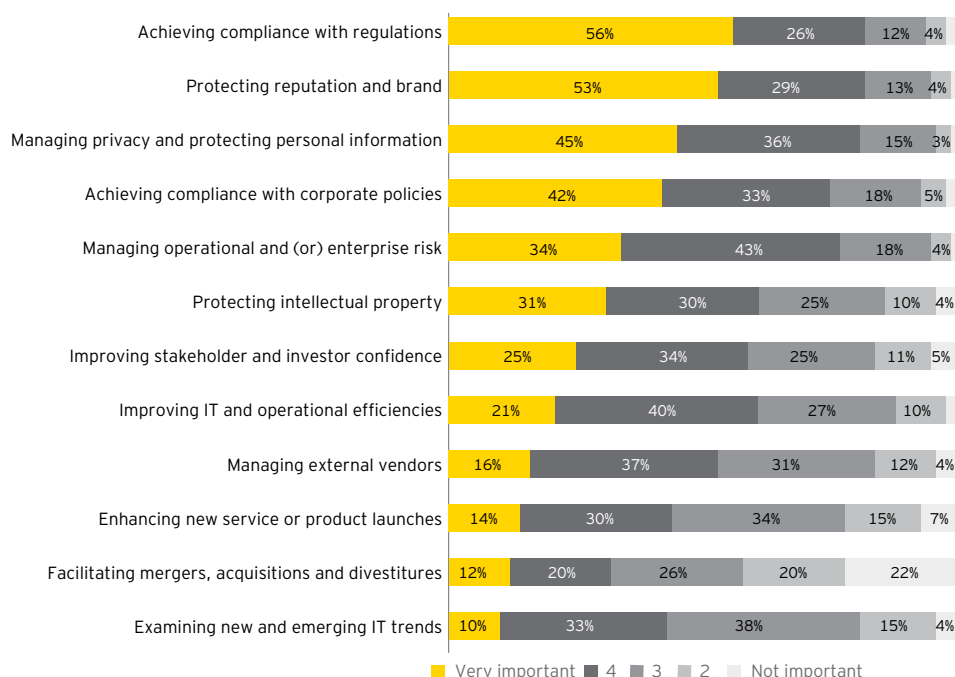
### Enterprise 2.0 defined

Enterprise 2.0 is the use of social media software inside the enterprise, enabling users to connect and collaborate in ways that mimic natural human social behaviors. It includes social and networked modifications to the corporate intranets and software platforms used by companies for internal communication.



As the use of social networking and Web 2.0 sites continues to increase and become part of the standard work environment, the behaviors related to sharing personal information are often being transferred to sensitive business information, where they are not appropriate. If no action is taken, this will likely lead to an increase in the disclosure of business information or protected privacy-related data, either intentionally or accidentally through the use of social media.

**How important is information security in supporting the following activities in your organization?**



Shown: percentage of respondents

As a result, survey participants' activities of primary focus – achieving compliance with regulations (56%), protecting reputation and brand (53%), and managing privacy and protecting personal information (45%) – could become increasingly difficult to achieve without an effective process in place to evaluate the risks associated with new and emerging IT trends. This is particularly true for those technologies that will make their way into the organization, whether intended or not.

**Only 10% of respondents indicated that examining new and emerging IT trends was a very important activity for the information security function to perform**

## Web connections (continued)

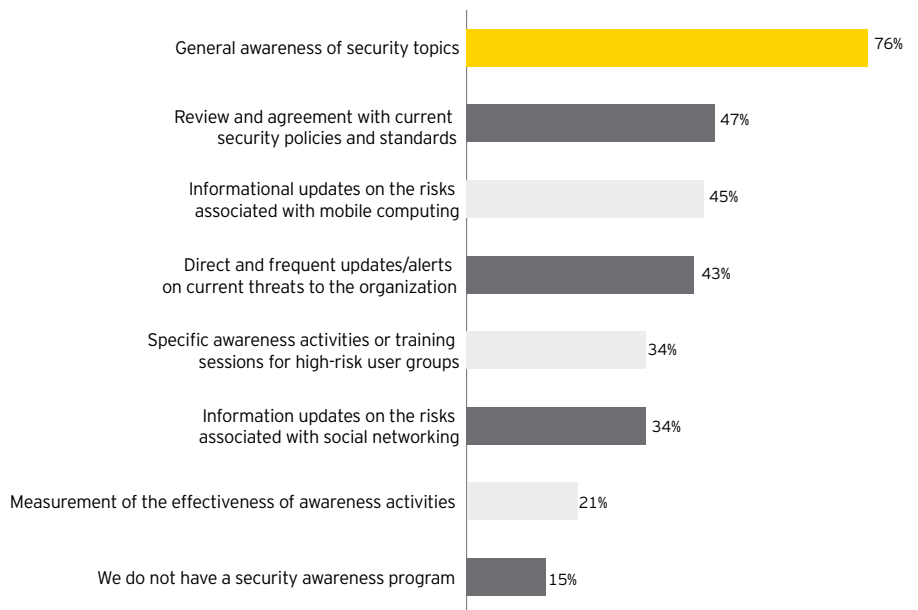
**34% of respondents include information updates on the risks associated with social networking**

### Securing social behavior

Understanding that this issue is primarily a behavior issue, organizations must profile their technology users, update and align security policies, and increase awareness communications in an attempt to successfully change behavior.

It is encouraging that only 15% of our survey participants indicated that they do not have a security awareness program in place and that 42% plan on spending more over the next year on security awareness and training (see page 6). However, just 34% of respondents currently include information updates on the risks associated with social networking.

What elements are currently covered in your organization's security awareness program?



Shown: percentage of respondents

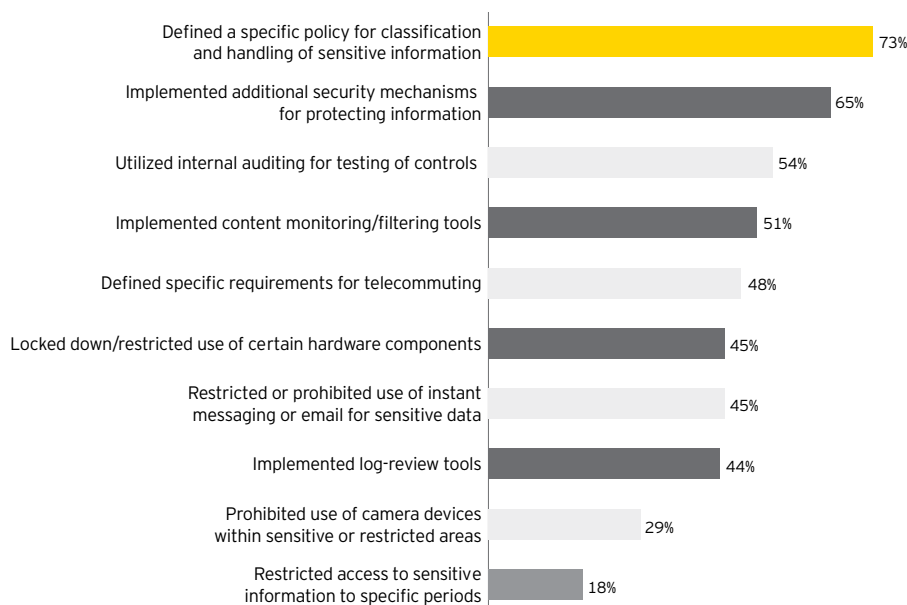
The simplest way to reduce the risks associated with social networking and Web 2.0 is to restrict or limit the use of such tools in the work environment. It is doubtful that such an approach can be successful – since it does not prevent the sharing of sensitive information from personal devices or home computers; it could also drive additional unwanted behaviors, such as connecting personal laptops to the business network. Another downside to such an approach is that the organizations that do not offer or restrict the use of these tools may be unable to attract and retain the best and brightest from the new generation of workers.



In an attempt to control data leakage of sensitive information, 45% of respondents indicated that they restrict or prohibit the use of instant messaging or email for sensitive data.

Which of the following actions has your organization taken to control data leakage of sensitive information?

**45% of respondents indicated that they restrict or prohibit the use of instant messaging or email for sensitive data**



Shown: percentage of respondents

## Our perspective

Today's social networking and collaboration tools are transforming the way in which business is conducted. People not only can share information and collaborate around the world at astonishing speed and efficiency – but they demand it. While the potential benefits and opportunities associated with the social trend are exciting, there are also new risks and information security issues that must be addressed.

The social media trend cannot be ignored by organizations that want to attract and retain the brightest talent of the new generation. Organizations must provide the online communities and social collaboration tools that the new workforce while protecting sensitive business information in a way that aligns enterprise requirements with personal responsibility. Specifically, organizations must raise security awareness and personal responsibility to levels previously not achieved.

To create a secure and successful business environment, organizations must involve their people; a technology-savvy workforce will find a way around controls, unless they fully understand the danger of the risks involved. By informing every member of the organization on the risks and issues related to social media, information security becomes an expanded function that all employees are fully aware of and have a responsibility to perform.



# Summary

Our 2010 Global Information Security Survey shows that companies and information security leaders are facing a changing business environment, where traditional enterprise boundaries are quickly evaporating, an environment driven by an increase in workforce mobility, greater adoption of cloud computing services, and a growing use of social media and collaboration tools within the enterprise.

Organizations are struggling to manage these trends – while needing to adopt them to get the most benefits and cost savings, where possible – but they need to understand and mitigate the potential risks and security impact to the organization.

By leveraging the information in this survey and taking action on the suggested steps for improvement, organizations can better manage the risks associated with an increasingly borderless environment.

## Survey findings

### Borderless security

- ▶ 60% of respondents perceived an increase in the level of risk they face due to the use of social networking, cloud computing and personal mobile devices in the enterprise.
- ▶ 46% of respondents indicated that their annual investment in information security is increasing.
- ▶ 30% of respondents indicated that they have an IT risk management program in place that addresses the increasing risks related to the use of new technologies.

### Mobile computing

- ▶ 51% of respondents indicated that increased workforce mobility is a considerable challenge to effectively delivering their information security initiatives.
- ▶ 64% of respondents indicated that data (e.g., disclosure of sensitive data) was one of their top five areas of IT risk.
- ▶ 50% of respondents plan to spend more on data leakage/data loss prevention technologies and processes over the next year.

### Cloud computing

- ▶ 45% of respondents are currently using, evaluating or are planning to use cloud computing services within the next 12 months.
- ▶ 77% of respondents who use cloud services indicated that they are using Software as a Service as the main cloud service model.
- ▶ 39% of respondents cited the loss of visibility of company data as an increasing risk.

### Social media

- ▶ 32% of respondents indicated that social networking is a considerable challenge to effectively delivering information security initiatives.
- ▶ 10% of respondents indicated that examining new and emerging IT trends was a very important activity for the information security function to perform.
- ▶ 34% include information updates on the risks associated with social networking.
- ▶ 45% of respondents indicated that they restrict or prohibit the use of instant messaging or email for sensitive data.



## Our perspective

### Borderless security

- ▶ Establish a detailed IT risk management program that identifies and addresses the risks associated with new and emerging technologies
- ▶ Undertake a risk assessment exercise to identify potential exposure and put in place appropriate risk based responses
- ▶ Take an information-centric view of security, which is better aligned with the organization's business and information flows

### Mobile computing

- ▶ Increase the investment in data leakage prevention technologies, encryption, and identity and access management services – focusing on the people who use the technology
- ▶ Gain an understanding of the risks created by the use of new technologies – including technologies adopted personally by employees that may be used for business purposes
- ▶ Information security policies should be reviewed and adjusted appropriately to establish the acceptable use and any specific restrictions related to mobile computing devices
- ▶ Increase security awareness training activities for the mobile workforce
- ▶ Push enterprise security out to end-point devices to protect critical business information and provide better alignment with the organization's risk profile

### Cloud computing

- ▶ Assess the legal, organizational and technological risks as well as the security issues related to placing information into the public cloud
- ▶ Develop a company strategy, a governance model and an operational approach to cloud computing use, including the information security function to help define policies and guidelines
- ▶ Set standards and minimum requirements to enable your organization to adopt cloud computing in as secure a manner as possible

### Social media

- ▶ Provide the online communities and social collaboration tools that the new workforce expects, but do so with a view that aligns enterprise requirements with personal responsibility to protect sensitive business information
- ▶ Raise security awareness and personal responsibility to levels that have not been achieved before
- ▶ Inform every member of the organization on the risks and issues related to social media

# Survey approach

Ernst & Young's 2010 Global Information Security Survey was developed with the help of our assurance and advisory clients.

This year's survey was conducted between June 2010 and August 2010. Nearly 1,600 organizations across all major industries and in 56 countries participated.

## Methodology

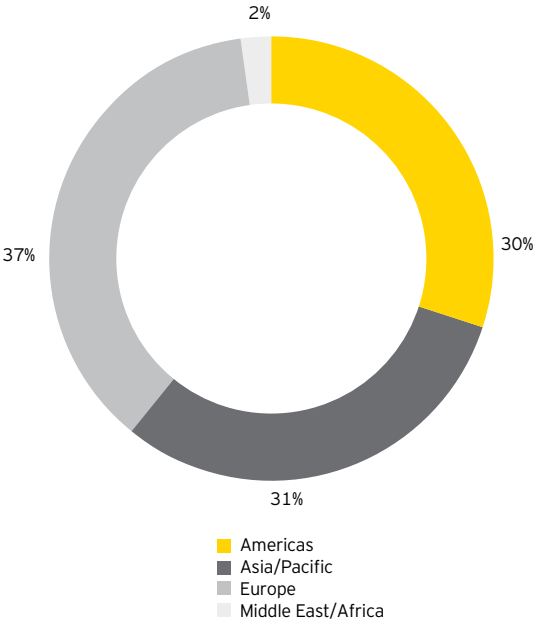
The questionnaire was distributed to designated Ernst & Young professionals in each country practice, along with instructions for consistent administration of the survey process.

The majority of the survey responses were collected during face-to-face interviews with individuals responsible for information security at the participating organizations. When this was not possible, the questionnaire was administered electronically via the internet.

If you wish to participate in Ernst & Young's 2011 Global Information Security Survey, you can do so by contacting your local Ernst & Young office, or visiting [www.ey.com](http://www.ey.com) and completing a brief request form.

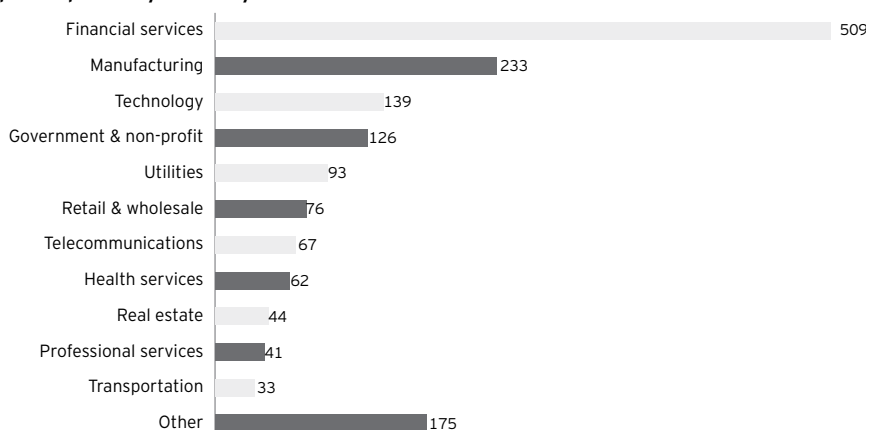
## Profile of 2010 survey participants

Survey participants by region

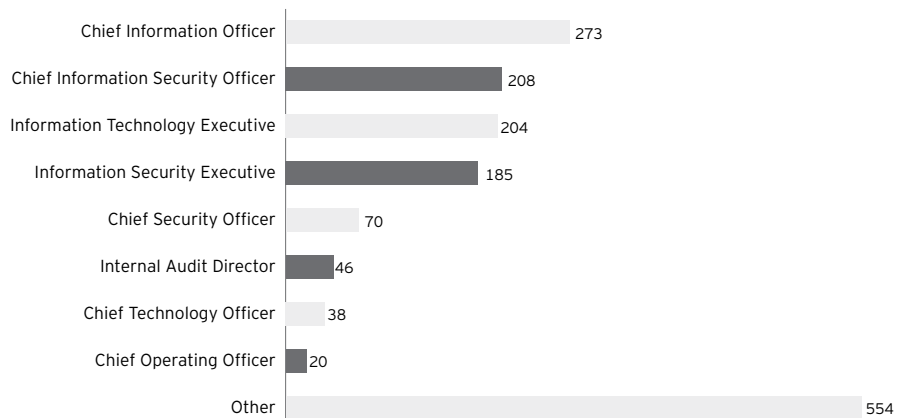




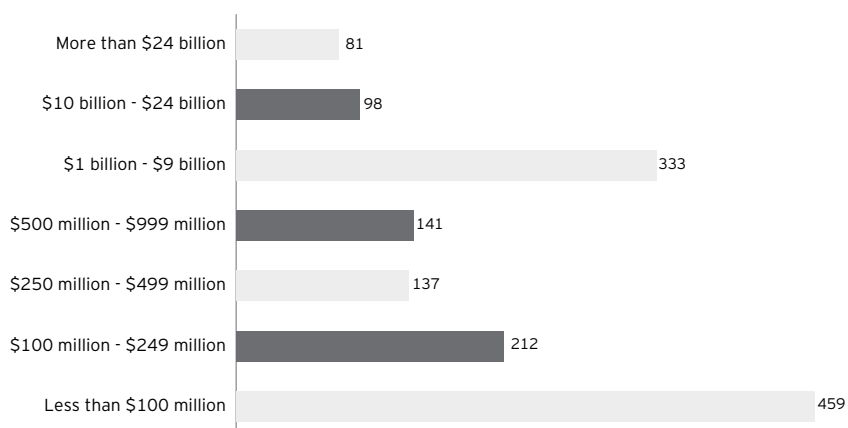
### Survey participants by industry



### Survey participants by title



### Survey participants by annual revenue (US\$)



# About Ernst & Young

At Ernst & Young, our services focus on our individual clients' specific business needs and issues, because we recognize that every need and issue is unique to that business.

IT is a critical enabler for organizations to compete in today's global business environment. IT provides the opportunity to get closer and respond faster to customers, and can significantly enhance both the effectiveness and efficiency of operations. But as opportunities through technology increase, so do the risks.

Our 6,500 IT risk and assurance professionals draw on extensive personal experience to give you fresh perspectives and open, objective advice – wherever you are in the world.

We view IT as both a business and a business enabler. IT is critical in helping businesses continuously improve their performance and sustain that improvement in a rapidly changing business environment.

Our business advisory professionals bring the experience of working with major organizations to help you deliver measurable and sustainable improvement in how your business performs.

We assemble multidisciplinary teams, use a consistent methodology, proven approaches and tools, and draw on the full breadth of Ernst & Young's global reach, capabilities and experience. We then work to give you the benefit of our broad sector experience, our deep subject matter knowledge and the latest insights from our work worldwide. That's how Ernst & Young makes a difference.

For more information on how we can make a difference in your organization, contact your local Ernst & Young professional or any of the people listed in the table below.

## Contacts

Global	Telephone	Email
Norman Lonergan (Advisory Services Leader)	+44 20 7980 0596	norman.lonergan@uk.ey.com
<b>Advisory Services</b>		
Robert Patton (Americas Leader)	+1 404 817 5579	robert.patton@ey.com
Andrew Embury (Europe, Middle East, India and Africa Leader)	+44 20 7951 1802	aembury@uk.ey.com
Doug Simpson (Asia Pacific)	+61 2 9248 4923	doug.simpson@au.ey.com
Isao Onda (Japan Leader)	+81 4 3238 7011	onda-s@shinnihon.or.jp
<b>IT Risk and Assurance Services</b>		
Bernie Wedge (Americas Leader)	+1 404 817 5120	bernard.wedge@ey.com
Paul van Kessel (Europe, Middle East, India and Africa Leader)	+31 88 40 71271	paul.van.kessel@nl.ey.com
Troy Kelly (Asia Pacific Leader)	+81 2 2629 3238	troy.kelly@hk.ey.com
Masahiko Tsukahara (Japan Leader)	+81 3 3503 2900	tsukahara-mshk@shinnihon.or.jp



#### **About Ernst & Young**

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 141,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

For more information, please visit [www.ey.com](http://www.ey.com).

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients.

#### **About Ernst & Young's Advisory Services**

The relationship between risk and performance improvement is an increasingly complex and central business challenge, with business performance directly connected to the recognition and effective management of risk. Whether your focus is on business transformation or sustaining achievement, having the right advisors on your side can make all the difference. Our 20,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and superior client experience. We use proven, integrated methodologies to help you achieve your strategic priorities and make improvements that are sustainable for the longer term. We understand that to achieve your potential as an organization you require services that respond to your specific issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where the strategy is delivering the value your business needs. It's how Ernst & Young makes a difference.

© 2010 EYGM Limited.  
All Rights Reserved.

EYG no. AU0663



In line with Ernst & Young's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

[www.ey.com](http://www.ey.com)