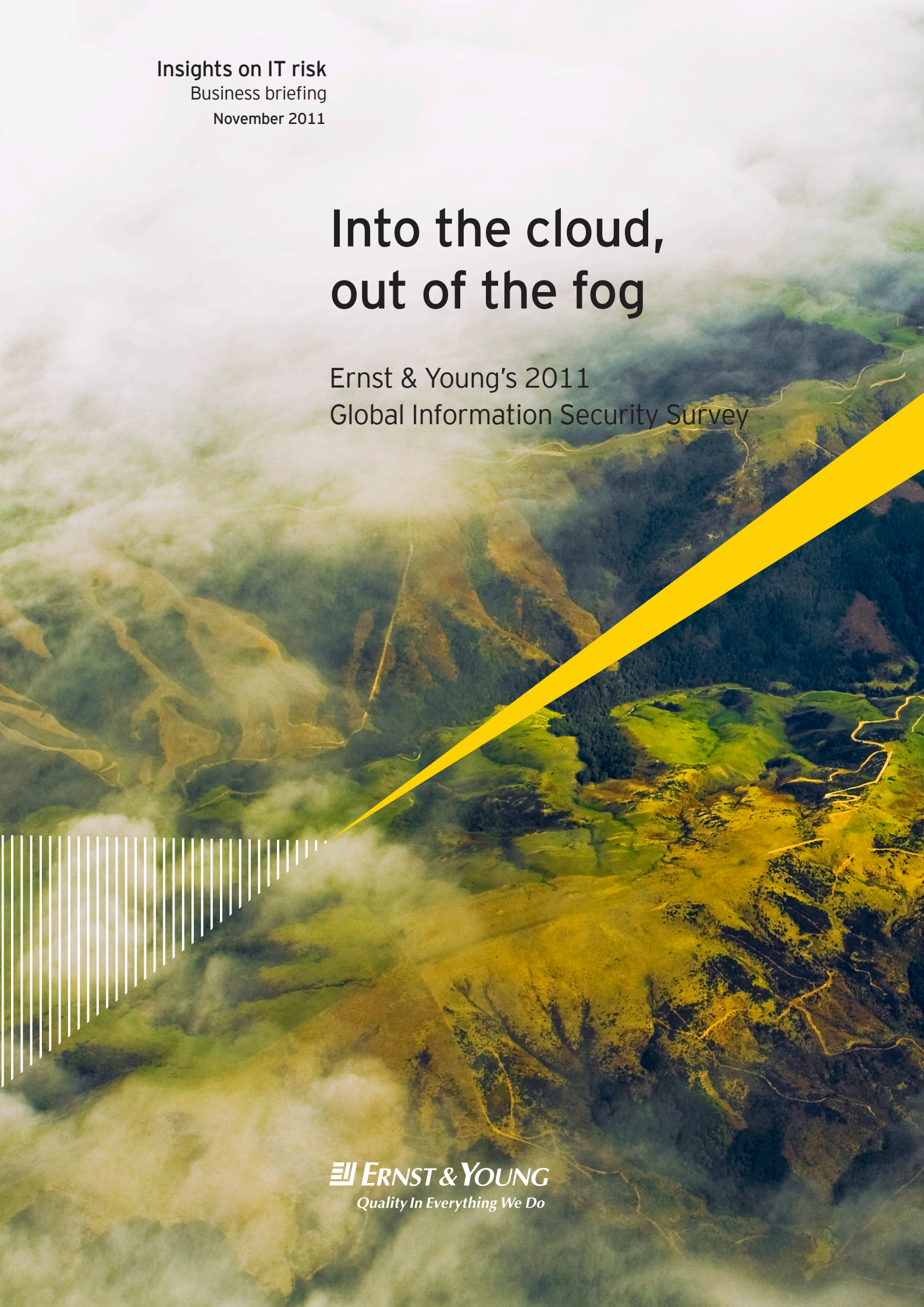
Insights on IT risk
Business briefing
November 2011

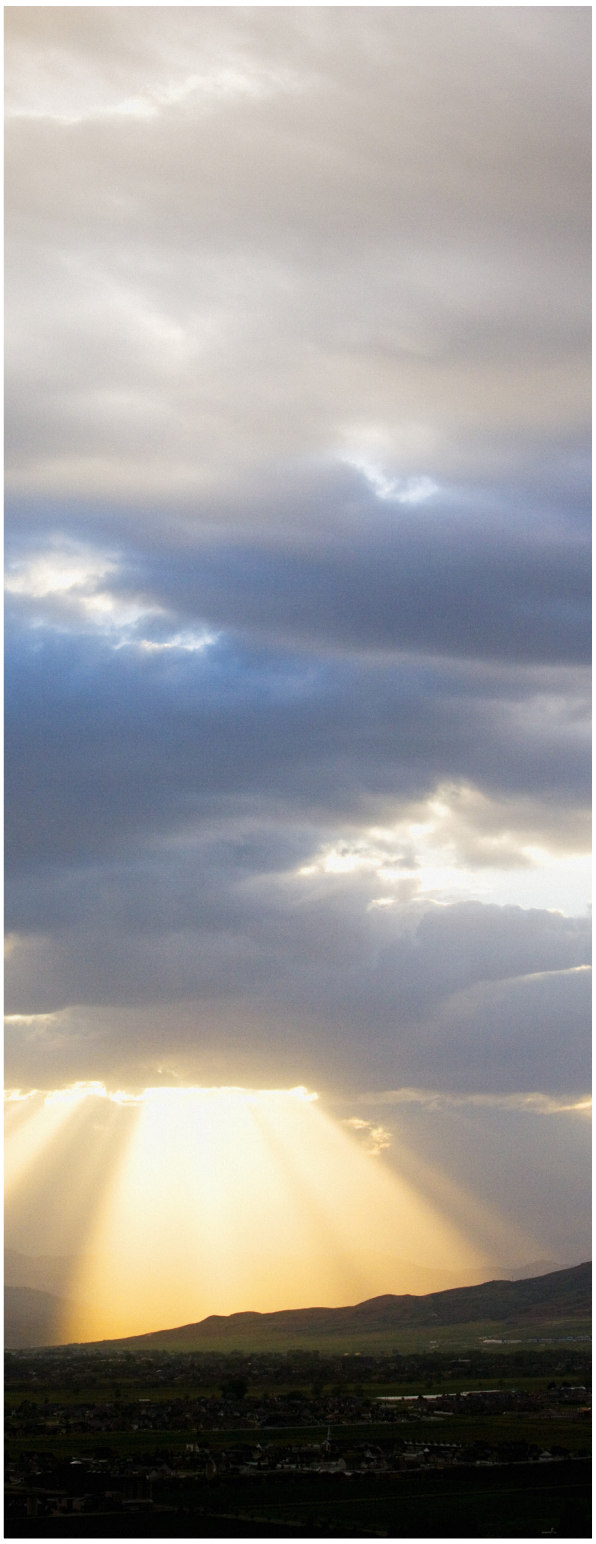
Into the cloud, out of the fog

Ernst & Young's 2011 Global Information Security Survey



ERNST & YOUNG
Quality In Everything We Do

Contents



Welcome

The Ernst & Young Global Information Security Survey is one of the longest running, most recognized and respected annual surveys of its kind. For 14 years our survey has helped our clients focus on the most critical risks, identify their strengths and weaknesses, and improve their information security.

Our survey is not just another online poll that anyone can access. We invite CIOs, CISOs, CFOs, CEOs and other information security executives to participate. This year, we received feedback from nearly 1,700 participants in 52 countries and across all industry sectors. The increased level of participation in our 2011 survey demonstrates that information security is still one of the most important issues facing organizations today.

The environment is one of unprecedented change, with many new business paradigms supported by new technologies. We see more and more traditional and non-traditional businesses moving not only information but also entire business models into the "cloud" – extending the virtual business with increased use of mobile computing, social media and shared computing infrastructures and services.

But these new technologies do not come without risks – this survey report should serve as a wake-up call for those organizations that have yet to recognize and address the associated risks.

Many of our survey participants revealed that their information security budgets are increasing. However, they also revealed a growing gap between their business needs and what information security is doing for their organizations. It is clear that there is still much more that can be done to protect information and manage information risk. We suggest that it is time to get back to basics and define a clear information security strategy and improvement agenda to help information security out of the fog.

I would like to extend my warmest thanks to all of our survey participants for accepting our invitation to openly discuss and share their views with us on information security.

We would welcome the opportunity to speak with you personally about your specific information security risks and challenges, and we believe that such discussions would help in addressing your needs, enabling you and your organization to see more value and certainty from information security and your investment in this area.

Paul van Kessel
Global Leader
IT Risk and Assurance Services

Moving into the cloud

More and more businesses are moving into a virtual world, supported by new technologies and driven by a need to reduce costs. It is a fascinating journey into the "cloud" that these organizations have undertaken — one that we expect many more organizations will follow.

In this new virtual world, the delivery of appropriate information security has been dramatically altered and has emerged as a "license to operate" for many organizations. We have identified three distinct trends that together have had and will continue to have a significant impact on the role and importance of information security.

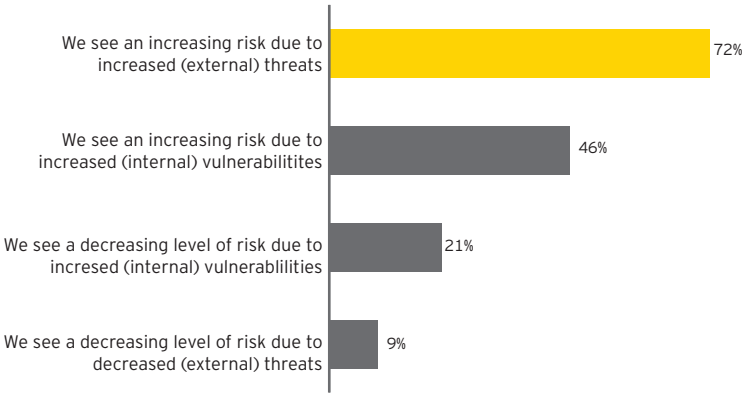
First, a company's physical boundaries are disappearing as more of its data is transmitted over the internet. Employees, customers, suppliers and other stakeholders are able to access this data "wherever and whenever" they wish, and the widespread adoption of mobile devices is accelerating this trend. In last year's survey we already noted this development, referencing the "borderless" environment; however, it continues to be a key area of concern for organizations today.

We also have watched the pace of change continue to accelerate and have witnessed technology transform entire industries — from automotive to publishing to retail. The theme here is the move from "physical" to "digital." Digitization is having a profound effect on businesses models, with traditional bricks-and-mortar industries being dominated or completely replaced by models that are essentially just based on software. Books have been transformed into e-books, CDs have been transformed into MP3s and cars are largely managed by software today, providing consumers with immediate delivery of products and enhanced value.

Last but not least, companies are moving from the more traditional outsourcing contracts to cloud service providers. In fact, our survey revealed that 61% of respondents are currently using, evaluating or planning to use cloud computing-based services within the next 12 months. This is a significant increase of 16 percentage points over the 45% that was reported in 2010. As organizations realize the benefits of bringing their business into the cloud and confidence in the cloud business model continues to rise, they will move more critical capabilities and sometimes their entire IT infrastructure and applications platform into the cloud — thereby forever altering their business model and their IT functions. By moving into the cloud, organizations now have the potential to greatly reduce or even eliminate their IT operations.

As organizations "digitize," move into the cloud and become "borderless," the risk landscape changes as well. Participants in our survey recognize this trend: 72% of respondents see an increasing level of risk due to increased external threats. At the same time, however, only about a third of respondents have updated their information security strategy in the past 12 months to respond to these enhanced threats. In addition, 46% of organizations have also identified increased threats within their own organizations.

In what way has the risk environment in which you operate changed in the last 12 months?



Shown: percentage of respondents

72% of respondents see an increasing level of risk due to increased external threats.

Cyber crime statistics

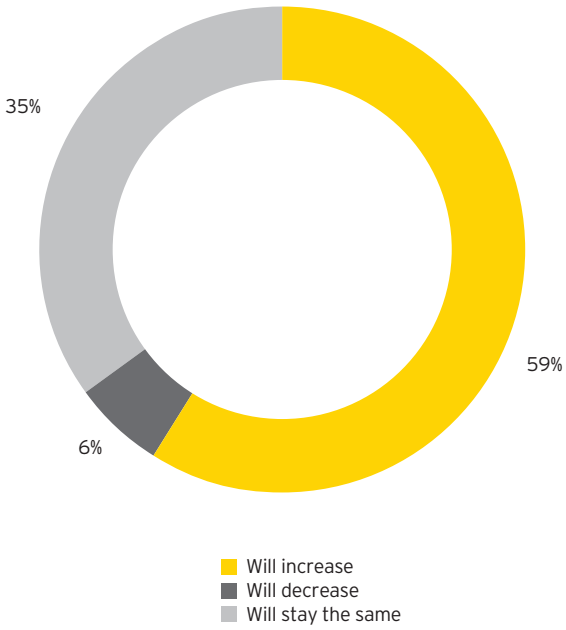
The 2001 Computer Security Institute/FBI Computer Crime and Security Survey noted that financial losses caused by cyber crimes amounted to more than $37 million for the nearly 200 companies that participated in the survey. And now in 2011, FBI reports have indicated that more than 350,000 complaints of cyber crimes were received this year alone. This statement should be judged in the context that most the cyber crimes remain unreported. According to the most recent reports of uscollegeresearch.org, about 73% of US and 65% of global internet users have been victimized by cyber criminals through June 2011.

Coming out of the fog

Information security is a critical component and key enabler for making the transition to the cloud a successful one. It is encouraging that 59% of respondents plan to increase their information security budgets in the coming 12 months. However, indications suggest that the money might not be spent as wisely as it should be. Only 51% of respondents stated that they have a documented information security strategy. The previous mentioned trends – borderless, IT services in the cloud and the digitization of the business – come with challenges that require a well thought-out strategy and carefully considered response. Ad hoc solutions may have been helpful in the past but are not sustainable in the future. It is important to recognize that increasing investment alone will not provide any guarantees of protection if there is no focus on doing the right things.

A pragmatic and proactive response rather than a reactive one is required. Information security needs to be more visible in the boardroom with a clearly defined strategy that will support the business in the cloud and elsewhere. Our survey shows that most companies have a long way to go to make this a reality, with only 12% of respondents presenting information security topics at each board meeting and fewer than half (49%) of our survey respondents stating that their information security function is meeting the needs of the organization. External perception and reputation of an organization's information security stance is also key – unless organizations get information security right, why should their customers trust them with their information and ultimately their business?

In absolute terms, which of the following describes your organization's total planned information security budget in the coming 12 months?

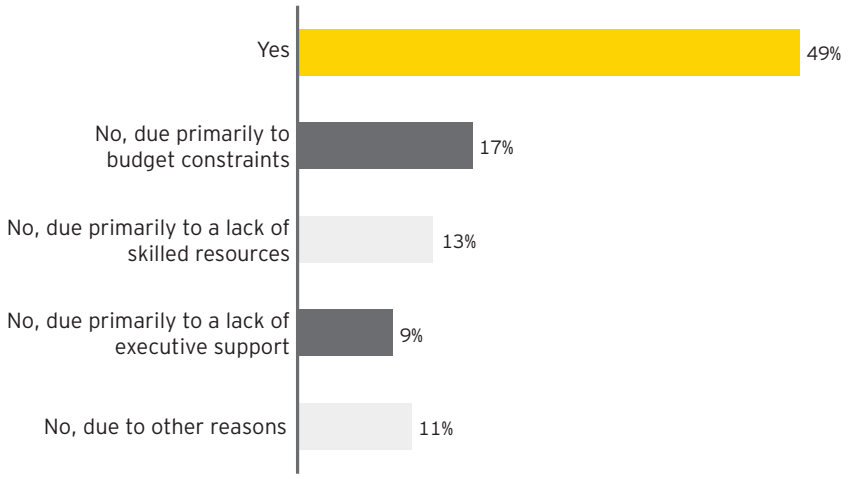


Shown: percentage of respondents

Until information security becomes an integral aspect of service and product delivery and part of management's day-to-day thinking, it will not be viewed as a strategic enabler to enhance business performance.

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

Do you believe the information security function is meeting the needs of your organization?



Shown: percentage of respondents

While 49% of respondents stated that their information security function is meeting the needs of the organization, 51% said otherwise.

Our perspective

- Bring information security into the boardroom, making it more visible with a clearly defined strategy that will protect the business while also adding more value through tighter alignment with business needs.
- Make information security an integral part of service and product delivery and everyone's day-to-day thinking.
- Focus information security on protecting what matters most, such as customer information and intellectual property. If information security is not adequate and not an enhancement to your brand, why should customers trust you as a business?

Keeping track of mobile computing

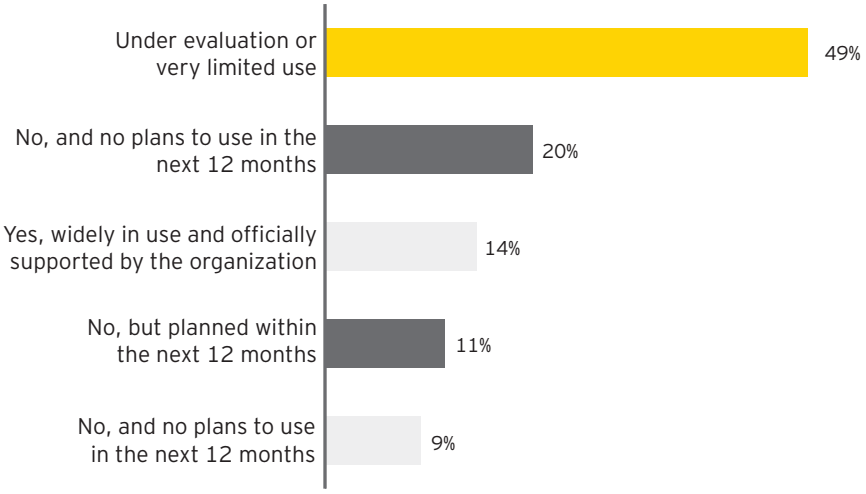
Tablets on the rise

Over the past two decades, we have witnessed significant technological advances in mobile devices, from the personal data assistants (PDAs) of the late 1990s and early 2000s to the ubiquitous and multifunctional smartphones and tablets of today. These advances have extended the virtual boundaries of the enterprise, blurring the lines between home, office, coworker and competitors. Constant access to email and corporate applications enables new mobile business applications and allows access to, and storage of, sensitive company data as well as private personal data. In other words, more access equals more productivity, but also more risk.

Mobile technologies are converging as the functionality overlap between laptops, smartphones and tablets continues to increase. In addition, the pace of the adoption by organizations is unprecedented. Organizations therefore need to integrate quickly, compressing the time needed to identify potential risks and develop effective strategies and implement measures to address those risks.

The rapid adoption of tablet computing is evidenced by the results of our survey. Only 20% of respondents do not have plans to permit the use of tablet computers; the vast majority of respondents (80%) are either planning to (11%), evaluating (46%) or widely using tablet computing (23%, of which 9% did not support use; 14% supported use). On the other hand, our survey shows that the adoption of tablets and smartphones ranked second-highest on the list of technology challenges perceived as most significant, with more than half of respondents listing it as a difficult or very difficult challenge.

Does your organization currently permit the use of tablet computers for business use?



Shown: percentage of respondents

Bring your own device

An increasing number of companies are offering support for employee-owned devices instead of providing devices with a preconfigured system. With this shift in ownership, organizations relinquish some control around limiting support to a single consistent software build because they have no legal right to force employees to adapt to company software. Additionally, it opens up the possibility of employees knowingly or unknowingly making changes in the mobile device that lessens the security of the device. For instance, users could install a remote administration server that may be another interface for an attacker to target, or they could compromise the underlying operating system integrity through processes such as "jailbreaking."

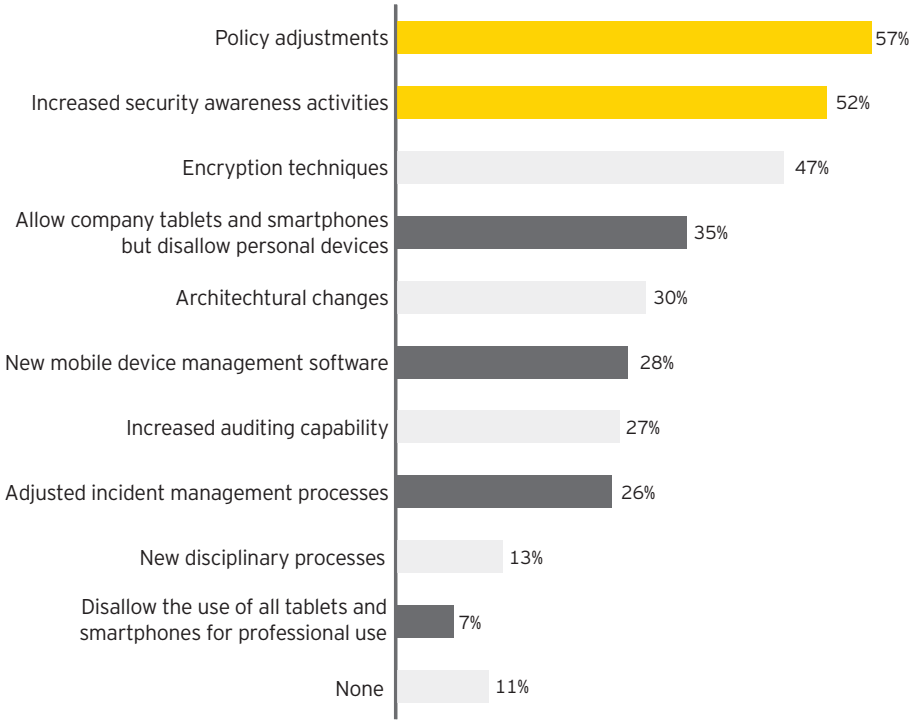
Policy as key control

Our survey shows that policy adjustments and awareness programs were chosen as the top two measures organizations are using to help address risks posed by this new technology. While establishing governance in security is a recognized approach to securing any technology, we believe this is even more effective considering the evolving nature of both mobile devices and the security software products they employ. User awareness of the risks of mobile devices will also help limit the instances of employee misuse and inform users of the policies around acceptable use.

In parallel with efforts toward updating policies and user awareness, we see that companies recognize the need to do more. In fact, the above approaches are far from being watertight measures to mitigate the risks. Therefore, they are beginning to educate themselves about the capabilities and design of the mobile device security software products that are available in the market. The adoption of security techniques and software, however, in the fast-moving mobile computing market is still low. For instance, encryption techniques are used by fewer than half (47%) of the organizations.

57% of respondents have made policy adjustments to mitigate the risks related to mobile computing risks.

Which of the following controls have you implemented to mitigate the new or increased risks related to the use of mobile computing (e.g., tablet computers)?



Shown: percentage of respondents

Our perspective

- Establish governance and guidance for the use of both mobile devices and their associated security software products.
- Use encryption as a fundamental control. Because fewer than half of the respondents are using it, organizations should consider embracing encryption.
- Perform attack and penetration testing on mobile apps before deployment to help reduce the organization's risk of exposure.

Seeing through the cloud

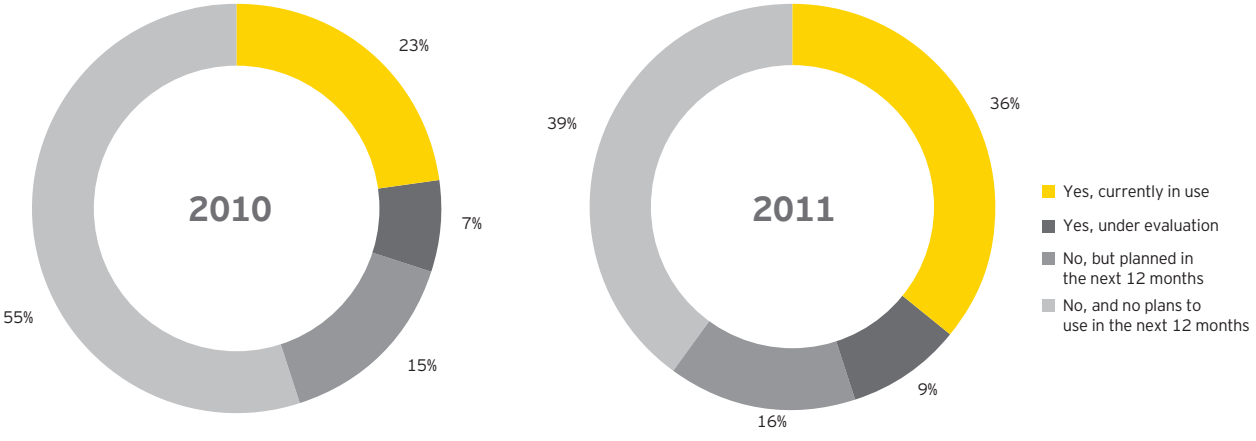
61% of respondents are currently using, evaluating or planning to use cloud computing-based services within the next year.

Looking beyond the benefits of cloud computing

As cloud computing is evolving, so are the buyers of cloud services. Savvy business professionals have recognized the speed and efficiencies that embracing cloud technology can bring. Organizations not interested in being in the business of IT have acknowledged the tremendous value of being able to focus on their core business competencies and remaining only a user of IT services. Traditional IT models demanded we erect mammoth infrastructures and complex application architectures just to run our most basic business processes. Cloud computing has given birth to a new breed of business user: a sophisticated consumer who can choose which services to consume and combine them as easily as ordering from a menu.

Despite the compelling story for cloud adoption, many organizations are still unclear of the implications of the cloud and are increasing their efforts to better understand the impact and the risks. Out of 16 information security areas, respondents named cloud computing as their top funding priority for the coming 12 months, and it ranked second among all other categories in the areas most likely to receive more – rather than less – funding than the previous year. In exchange for highly configurable, rapidly deployed, externally managed applications, organizations are making trade-offs – whether they realize it or not. Governing bodies, such as audit and compliance, view these trade-offs as being dangerous due to the lack of expertise or experience by some of the individuals making such risky decisions. Whether we realize it or not, our appetite for external cloud services has increased our dependency on third parties and dimmed our view into the inner workings of core business applications. And as organizations become increasingly locked in to their cloud provider, they also face compliance risks, contracting and legal risks, and integration risks. Moving to the cloud is not just another change program; it is nothing less than a complete transition of business processes, including the risks associated with it.

Does your organization currently use cloud computing-based services?



Shown: percentage of respondents (GISS 2010 and GISS 2011)

Category	Key risks and challenges
Compliance and privacy	Cloud computing is often "borderless," but compliance is not. For cloud users it is often not clear where data resides, which creates challenges for legal compliance or privacy. For instance, a cloud provider may be subject to privacy laws such as Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI/DSS) the US Patriot Act and EU Data Privacy Act.
Information security and data integrity	Processing data with a cloud service provider followed by communication over the internet, as opposed to keeping it entirely within a company network, increases data and information vulnerability. Key risks include unauthorized modification of systems or data and unauthorized deletion of data. The cloud therefore brings new challenges when it comes to application security, identity and access management, authentication, encryption and data classification.
Contract and legal	Contractual risks stem primarily from the types of contracts that companies enter into with cloud service providers. Those contracts should include the service level agreements (SLAs) and key performance indicators (KPIs) that are used to agree and evaluate performance. Managing these complex vendor relationships requires experience and deeply specialized skills. In many cases, the complexity makes it hard to see where risk is assumed and by whom.
Governance and risk management and assurance	When embarking on the journey into the cloud, organizations will want to ensure that it fits well within their overall business goals in terms of both the benefits and the risks. Organizations therefore need a governance model and a cloud strategy, including a cloud risk management approach. Standards, leading practices and guidance for cloud users and cloud service providers are under development with several independent bodies. However, there is no agreed-upon baseline available.
Reliability and continuity of operations	Continuity of the business is critical. Therefore, it is important to understand a cloud provider's geographical coverage and how this may affect cloud users. In addition, cloud users are depending on their cloud service providers' business continuity program and disaster recovery capabilities. The cloud user is also dependent on a cloud service provider's capabilities regarding operations and support processes, such as incident management and service desk.
Integration and Interoperability	The integration of systems in the cloud is a significant undertaking. Systems need to be able to talk to one another between the cloud user and the cloud service provider. In some cases, cloud users negotiate transition services to make this happen, including full-range testing. To provide for ongoing interoperability, technology changes and systems upgrades, including testing, must also be addressed and managed.

Why organizations need to understand their external cloud provider

The majority of our respondents (80%) using cloud computing are using Software as a Service (SaaS)-based services. However, to further complicate things, although many people believe that they are purchasing SaaS, it may be from a cloud provider who is using Platform as a Service (PaaS) capabilities from another cloud provider who purchased its infrastructure from an Infrastructure as a Service (IaaS) provider who rents space in a shared data center. In simple terms, it is similar to a car from a manufacturer that outsourced its engine production to a company which, in turn, outsourced its steel foundry to another supplier. The lines between vendors are blurring, and in a world where data flows freely from vendor to vendor, trust becomes a precious commodity. Therefore, it is critical to develop trusted relationships with cloud service providers to be comfortable that the processes they leverage to manage businesses and data can be trusted and relied upon.

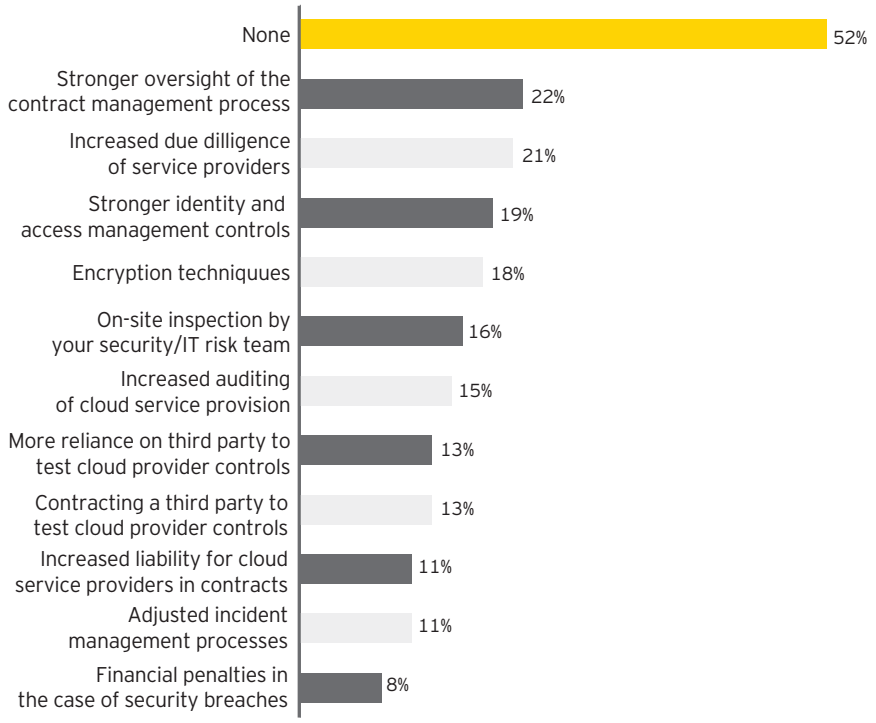
Seeing through the cloud (continued)

Where is the guidance?

Despite the evolution of cloud computing and the ability of service providers to implement high-value, easy-to-use solutions, organizations struggle with the integration of external cloud computing into their business. In 2011, 48% of respondents listed the implementation of cloud computing as a difficult or very difficult challenge, and just over half have not implemented any controls to mitigate the risks associated with cloud computing. Organizations, uncertain about their control options, select and implement only a subset of those available, sometimes none at all. The most frequently taken measure is stronger oversight on the contract management process with cloud providers, but even this is only done by 20% of respondents, indicating a high and possibly misguided level of trust.

In the absence of clear guidance, many organizations seem to be making ill-informed decisions, either moving to the cloud prematurely without appropriately considering the associated risk, or avoiding it altogether. The survey results indicate that although many organizations have moved to the cloud, many have done so reluctantly, evidenced by 80% of respondents who are challenged to deliver information security initiatives for new technologies such as cloud computing and virtualization.

Which of the following controls have you implemented to mitigate the new or increased risks related to the use of cloud computing?



Shown: percentage of respondents

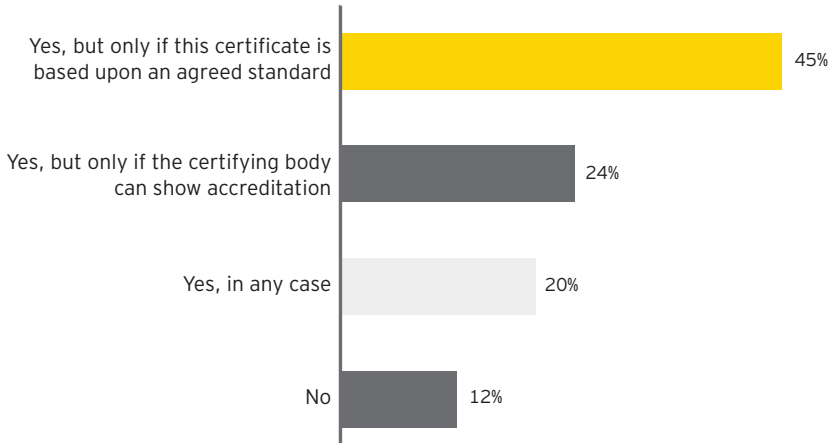
Building trust in the cloud

Most respondents agree that they rely heavily on trust, when in fact what is required are trust and validation, verification and certification. Almost 90% are in favor of external certification, with nearly half (45%) saying this should be based only on an agreed-upon standard. The market need for independent verification and certification is recognized by several independent bodies. In fact, great strides forward have been made recently regarding insightful guidance on cloud certification.

Many organizations have begun the governance process, addressing many of the perceived challenges through service attestation registries and consistent audit frameworks like those used in the financial services industry. Much progress toward a consistent trust model has been achieved (e.g., by the Cloud Security Alliance), and we expect that many respondents will find increased comfort with providers who participate in the trust community.

The cloud industry needs to evolve. Currently, the appeal of extensibility, customization and low cost is driving decisions to use cloud services. However, real risks exist, and the use of cloud-based services should be weighed in the context of the benefits they deliver. As the cloud industry evolves, so too must the ability to trust. This will be accomplished through the development of regulated trust standards. Currently, there are alliances working toward this goal, both private and federal. Organizations must continue to leverage the guidance of these organizations, aligning with industry practices to encourage standardization across service providers. It is not enough to rely on external entities to address all of the risks associated with cloud computing. These risks can represent a significant change to the way an organization operates and must be managed by formal enterprise and IT risk management procedures.

Would external certification of cloud service providers increase your trust in cloud computing? (Choose one)



Shown: percentage of respondents

Almost 90% of respondents believe that external certification would increase their trust in cloud computing.

Our perspective

- Choose verification above trust.
- Understand who owns the risks before entering a cloud agreement.
- Plan for continuity and select providers that are transparent about resiliency build backups and test recoverability.
- Proceed in using the standard security processes and techniques that have worked effectively on other technologies in the past.
- Align your business and information security strategy, and continuously assess risks to comply with regulations and industry standards.

Connecting through social media

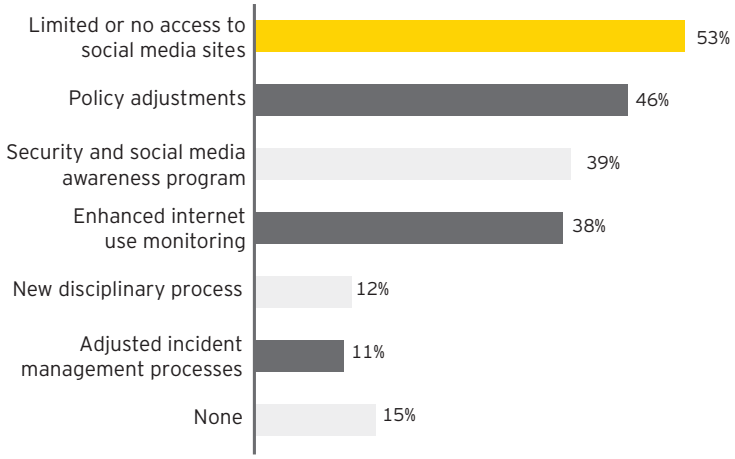
53% of respondents have implemented limited or no access to social media sites as a control to mitigate risks related to social media.

Staring social media risks in the face

More than 1 billion people, about 15% of the world's population, are registered users of the world's most-popular social and business networking sites. If the registered users of the world's largest social networking site were a country, it would be the third largest behind China and India. The popularity and massive growth of social media is attributed to its profound benefits: social media enables individuals to stay connected to one another like never before, which allows organizations to transform the way they connect with customers, develop brand loyalty and sell more effectively. Social media enables organizations to engage with customers on a real-time basis and solicit direct feedback, which then helps them to continuously improve their market offerings and positioning.

The increasing adoption of social media affects the IT risk landscape. In reality, "virtual friends" aren't always who they seem to be in the world of social media. Social media risks include the introduction of malicious software lurking within social networks, hacked accounts that are used to solicit information, and the release of confidential or negative company information or personal data.

Which of the following controls have you implemented to mitigate the new or increased risks related to the use of social media?



Shown: percentage of respondents

Our survey reveals that a significant portion of participants recognize the risks: nearly 40% of respondents rated social media-related issues as either challenging or significantly challenging. Most respondents (72%) claimed that external malicious attacks were their top risk. These attacks may be fueled by information obtained through the use of social media that was used to send targeted phishing messages to targeted individuals.

To help address potential risks posed by social media, organizations seem to be adopting a hard-line response. Just over half (53%) have responded by blocking access to sites rather than embracing the change and adopting enterprise-wide measures. Although this response may be effective in some situations, the increased ease of access by means of (privately owned) mobile devices enables individuals to get direct access to social media during office hours. Therefore, blocking or limiting access to social media sites will never be completely effective.

Nearly 40% of respondents rated social media-related risks issues as challenging.

Our perspective

- Reconsider (if applicable) using hard-and-fast "no access/no use" policies for social media sites. This response, while perhaps addressing external threats to internal hardware and software, does not completely address the widespread global personal adoption of social media usage and indirect integration into business use via other channels such as mobile devices. Organizations may consider monitoring their employees' usage of these sites, without restricting access.
- Embrace the full advantages of social media. The lack of an integrated information security policy for both access to and use of social media is preventing companies from keeping pace with competitors and may be creating a sense of mistrust with employees.
- Consider testing and using technical solutions that also enforce the security stance outlined within your social media policy.
- Perform your own reconnaissance to better understand what potential attackers can find on social media.

Plugging the data leaks

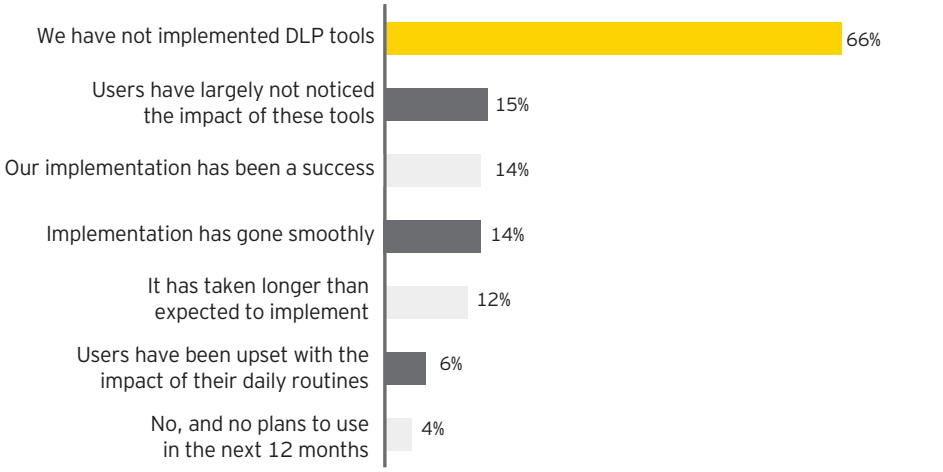
66% of respondents have not implemented data loss prevention (DLP) tools.

The importance of data loss prevention

Knowledge is power, and information derived from data is any organization's most valuable asset. A number of high-profile data leakage events have recently brought this issue into the public eye. With new borderless operating environments and the increasing adoption of the cloud, the risk of data loss is growing rapidly. The increased amount of data that is carried around through the use of mobile devices heightens the risk that unauthorized parties can gain access to sensitive data. But data loss is not only limited to the risk of physical loss of devices such as tablet computers, mobile phones or laptops. Many incidents are also due to accidental disclosure through electronic transmissions. In most cases, employees are not even aware of the risks associated with sending sensitive data through unencrypted emails, instant messages, webmail and file transfer tools. The embedding of technological user friendliness and access to data has become so intertwined that it has become relatively easy to engage in the unintentional spreading of confidential data.

Holes through which data can leave — already large due to expanding technologies and platforms — are made larger by the use of decentralized systems and work collaboration tools, making it even more difficult for organizations to track and control information within the business. Another complicating factor in efforts to help control data is the availability of increasingly inexpensive storage devices. Many gigabytes of data can literally "walk" out the door on an employee's keychain or in a smartphone, or they can be intercepted when sent through low- and no-cost cloud service and storage providers.

Regarding DLP tools implementation, how would you describe that deployment?



Shown: percentage of respondents

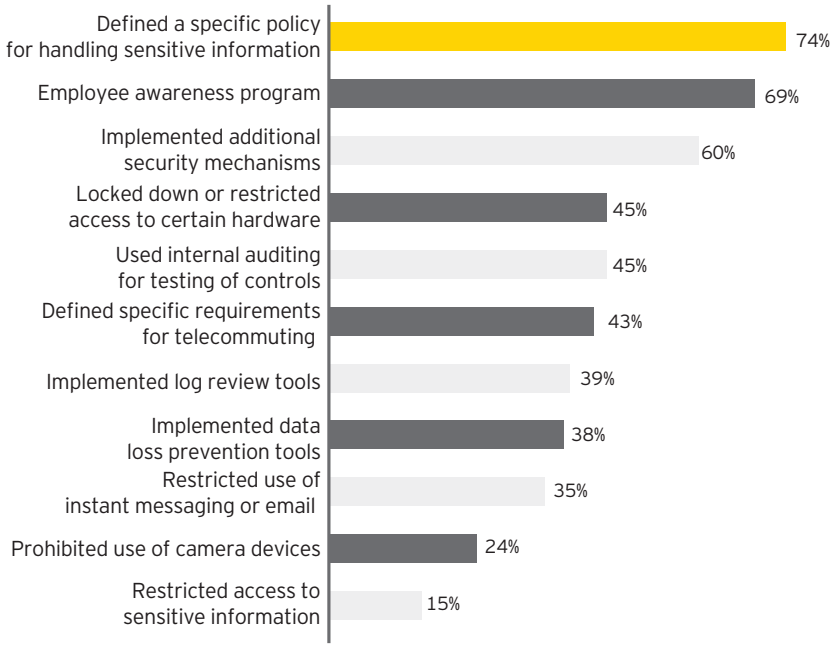
DLP technologies and processes are, however, widely recognized as one of the top management priorities, ranking second on the list of areas most likely to receive additional funding. More than half of companies plan to spend more on DLP-related efforts than they did last year.

In terms of actions taken to control the data leakage of sensitive information, 74% of organizations have defined a specific policy regarding the classification and handling of such data. Nearly 70% have run employee awareness programs, and almost two-thirds have implemented additional security mechanisms such as encryption for protecting information.

Logging and monitoring approaches include network intrusion detection and network segmentation — the two most popular measures implemented to prevent, detect or react to external attacks. In addition, 75% of organizations will perform an external network attack and penetration assessment over the next year, and 73% plan to run an external network vulnerability scan.

74% of respondents have defined a policy for the classification and handling of sensitive data as a control for data leakage risk.

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



Shown: percentage of respondents

Plugging the data leaks (continued)

Our perspective

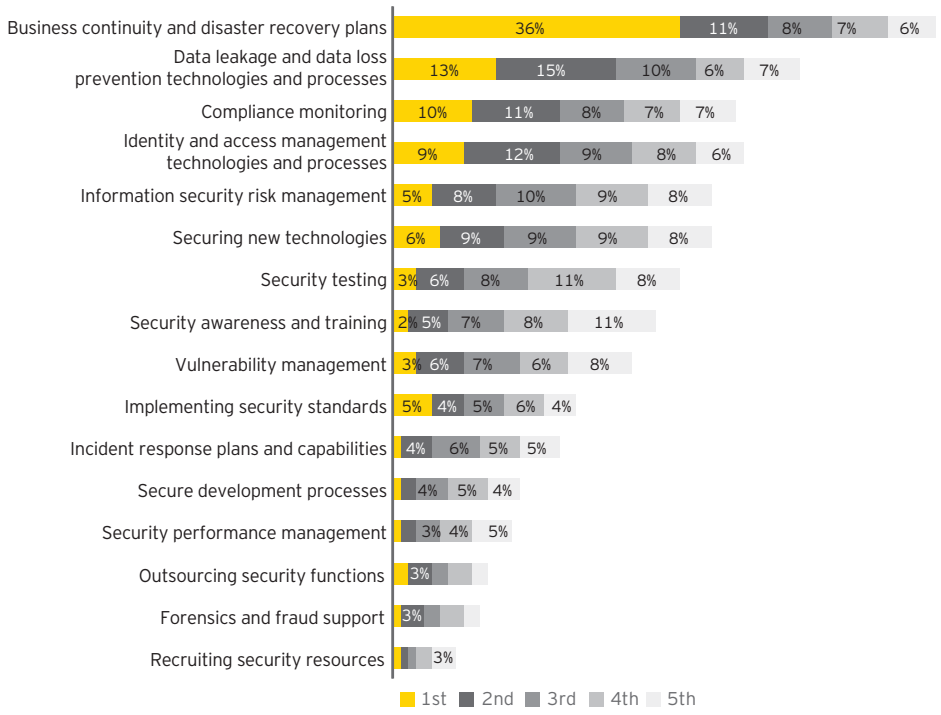
- Assess, understand and appreciate the many potential risks and areas of data loss, specifically documenting and ranking the risks relating to the data loss channels that exist within the organization.
- Identify, assess and classify sensitive data across the enterprise so that DLP controls can be focused to provide protection for the organization's most sensitive data.
- Take a holistic view of data loss prevention by identifying key DLP controls and measuring their effectiveness. All key controls that support the data loss prevention program, such as asset management and physical security controls, should be understood to provide accurate reporting of data loss risks and controls.
- Cover data in motion, data at rest and data in use within the organization's DLP controls.
- Implement incident investigation, enlist a strong team to carry out the program and seek the support of key stakeholders throughout the business to create a successful DLP program.
- Pay special attention to third parties with access to sensitive company data.
- Understand what data is sent to third parties, how it is sent and if the transmission mechanisms are secure. Organizations have a responsibility to perform due diligence to validate that third-party data stewards have reasonable safeguards in place for protecting sensitive company data.

Preparing for the worst

The need for a business continuity plan

Unexpected and catastrophic occurrences, including natural disasters and terrorist attacks can cause tragic losses on both personal and business levels. As organizations grow in size and complexity within the borderless world, the impact of non-availability of key resources has magnified. Big disasters, as well as smaller disruptions, have prompted leading executives not merely to hope for the best but also to prepare for the worst by investing in effective business continuity management (BCM). Information security measures play a key role in this. Our survey results reflect this trend: most respondents are making business continuity and disaster recovery a top funding priority for the coming year, with 36% of respondents identifying it as their top funding priority, three times as many respondents as those who indicated that the second-ranked area (data leakage and data loss prevention efforts) was their top priority.

Which of the following information security areas will receive the most funding over the coming 12 months?



Shown: percentage of respondents

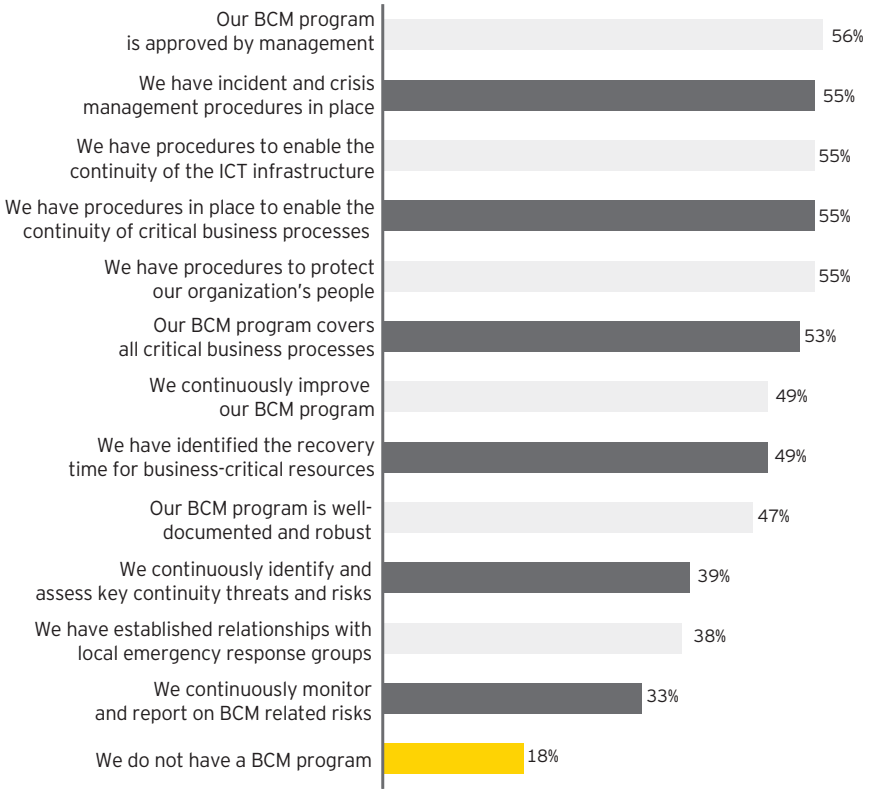
Black Swan events

Black Swan events evolve from one or a combination of factors, including unintended human error, negligence, malicious actions or acts of nature. Regardless of their causes, they are alike in that they occur unpredictably or unexpectedly, develop rapidly, are catastrophic in scale, present hazards beyond immediate financial risks, jeopardize lives, involve significant asset damage, and require significant resources to resolve. (N.N. Taleb, *The Black Swan*, Second Edition, Penguin, 2010.)

At the same time, some organizations are still not prepared: 18% indicated they have no BCM program in place, and only 56% indicated that management had approved BCM activities. Even when it is performed, BCM planning lacks maturity across many organizations, which runs the risk that it will not work when it is most needed. Despite business continuity being the top funding priority, many respondents report only partial BCM, with a sizable minority (45%) of organizations having no procedures to respond to crisis events, no procedures to protect staff or no plans that cover all critical business processes. In addition, given the criticality of information and communications technology (ICT) infrastructure to organizations, it is notable that 45% indicated that they lack procedures to help ensure it will continue working through a disaster. It is evident that many organizations still have a long way to go before they can be confident that they have actually planned for a worst-case scenario.

From a strategy, governance and control perspective, while 67% test their continuity plans regularly, only 52% of organizations have "appropriate resources to sustain" their BCM capability. In addition, just over a third of organizations (36%) have embraced technology as a mechanism for communicating during incidents or use tools to manage BCM data (28%).

Which of the following statements apply to your organization's business continuity management strategy and program?

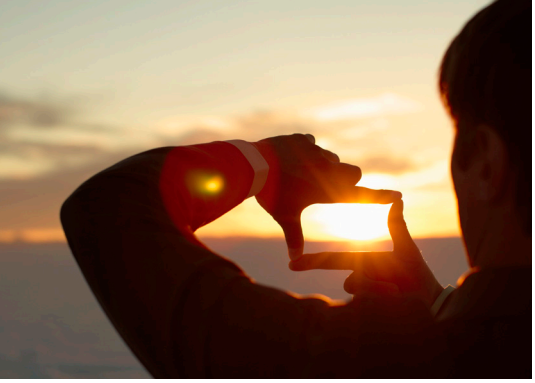


Shown: percentage of respondents

For the second consecutive year, respondents have indicated that business continuity is their top funding priority.

Our perspective

- Prepare for and secure business continuity plans that anticipate high-impact, low-frequency events, and determine which are integrated into a broader risk management framework that focuses on protecting the organization from catastrophic loss.
- Assess whether the business continuity plan has the right level of maturity in light of the emerging trends and new technologies.
- Test the organization's business continuity plan frequently to help validate your business resiliency in practice. The more complex the scenarios that are tested, the better the coverage of the test.
- Solicit the support of the board and the audit committee for their business continuity programs.

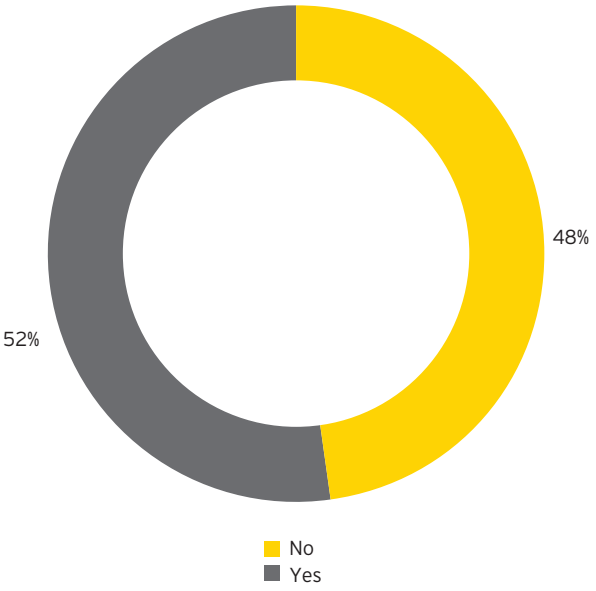


Looking into the future

Focusing on the fundamentals

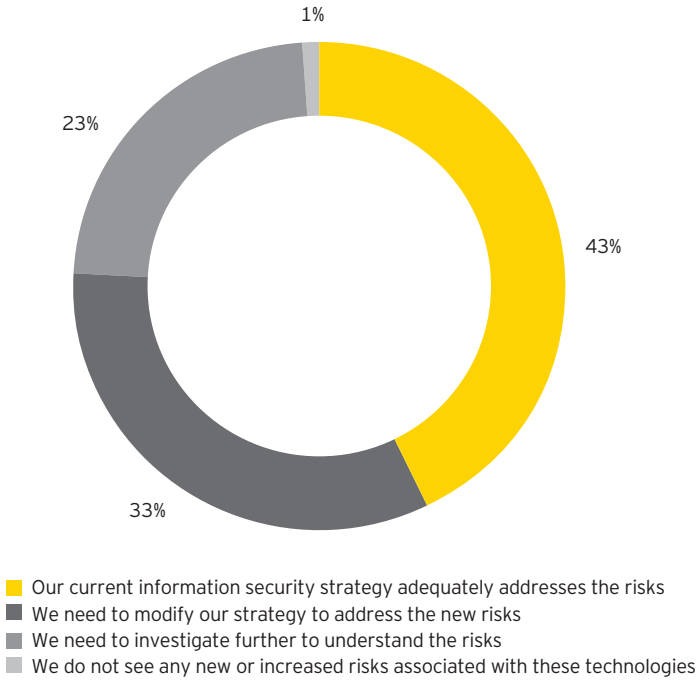
The results from this year's survey indicate that the risk landscape is changing at an accelerated pace. Confronted with diminishing borders, cloud services and business models in the cloud, companies are asking themselves how to respond to new and emerging risks and whether their strategy needs to be revisited. Surprisingly, only 53% of respondents have a documented security strategy, and 47% indicated that their current strategy adequately addresses the risks. Additionally, the majority of participants (56%) indicated they need to modify their strategy (33%) or need to investigate further to understand the new risks (23%). Having a clearly articulated and up-to-date strategic plan shows company leadership and stakeholders that the organization has a vision and clear agenda for delivering and improving security. This will take information security out of the fog and into the clear. It will build the necessary level of trust, which is an absolute prerequisite for doing business in today's virtual world.

Does your organization have a documented information security strategy for the next one to three years?



Shown: percentage of respondents

Which of the following statements best describes your organization's information security strategy in relation to today's threat landscape?



Shown: percentage of respondents

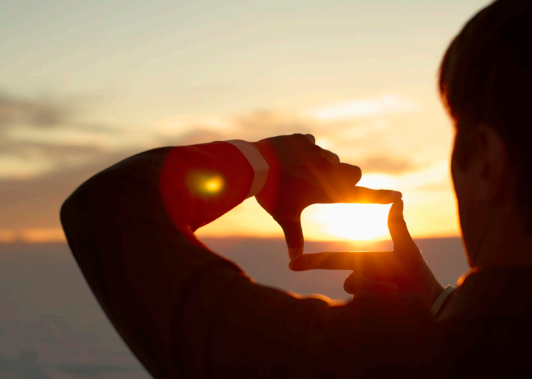
56% of respondents indicated that their current information security strategy needs to be modified or needs further investigation.

Point solutions have ceased to work

This year's results show that almost one-third of respondents (31%) indicated that their organization has recently purchased information security solutions that are perceived as having failed or under-delivered. Organizations would be better served by not always acquiring the latest tools, but instead focusing on the fundamentals. They remain a critical first line of defense – patching vulnerabilities, strengthening system configurations and properly configuring software. Such "back to basics" programs aren't quite as exciting as a multimillion-dollar software purchase or a versatile new security appliance, but they are proven to be effective.

New emerging risks: Web-blackmail

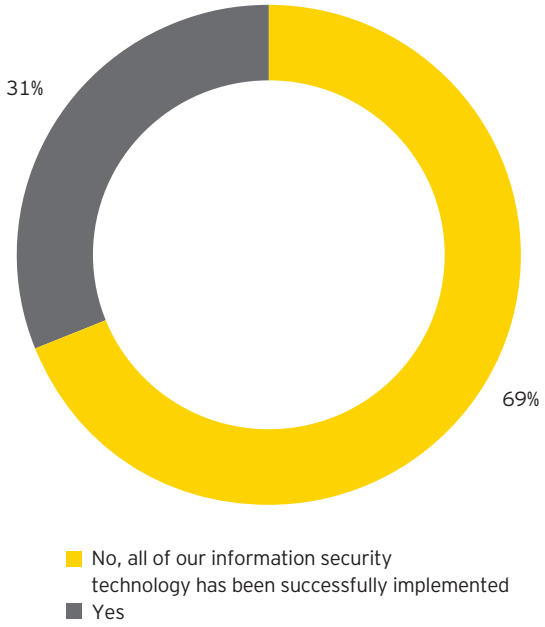
The owner of a prospering internet site experienced a Denial of Service (DoS) attack, in which the site was down for one hour. The lack of ongoing trade caused him damage and prompted worried customers to email him and ask what the problem was. Another email arrived from a "concerned" security company. The company detected that his site was shut down for one hour, but it offered a solution for his vulnerability. For a not-so-small, one-time-fee, the company guaranteed that the site would not undergo another DoS attack. It also mentioned that if he did not pay, tomorrow the site would go down for two hours, the next day for four hours, with the price for "fixing" the problem increasing each time.



Looking into the future (continued)

31% of respondents indicated that their organization has recently purchased information security solutions that are perceived as having failed or under-delivered.

Has your organization purchased software and/or hardware to support information security initiatives in the past 18 months that is perceived as having failed or under-delivered?

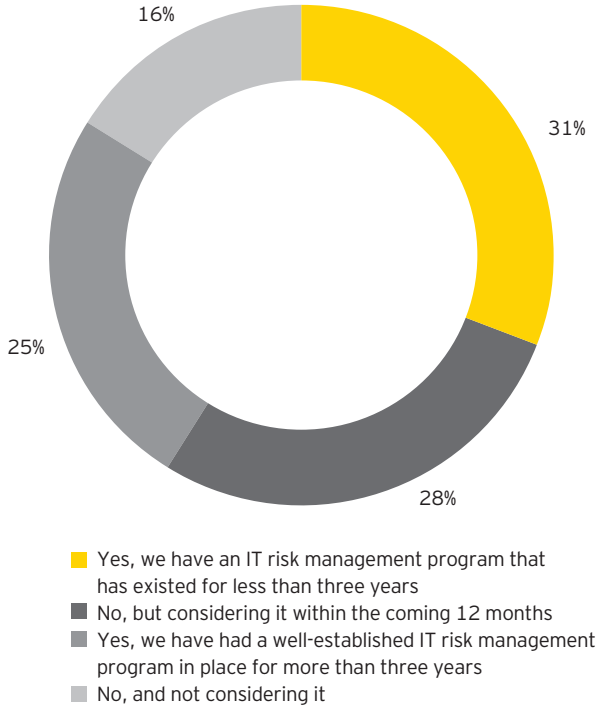


Shown: percentage of respondents

The emergence of IT risk management as a structured approach

In order to effectively manage IT risks in general, organizations need to gain a broad and comprehensive view of the entire IT risk landscape. This holistic perspective will provide companies with a starting point to help identify and manage current IT risks and challenges, as well as those that may evolve over time. This will enable the organization to focus on the risks that matter most — rather than focusing on point solutions. When we look at our survey results, 84% of respondents indicated that they have an IT risk management program in place or are considering it within the next 12 months.

Do you have a formalized IT risk management program in place at your organization?



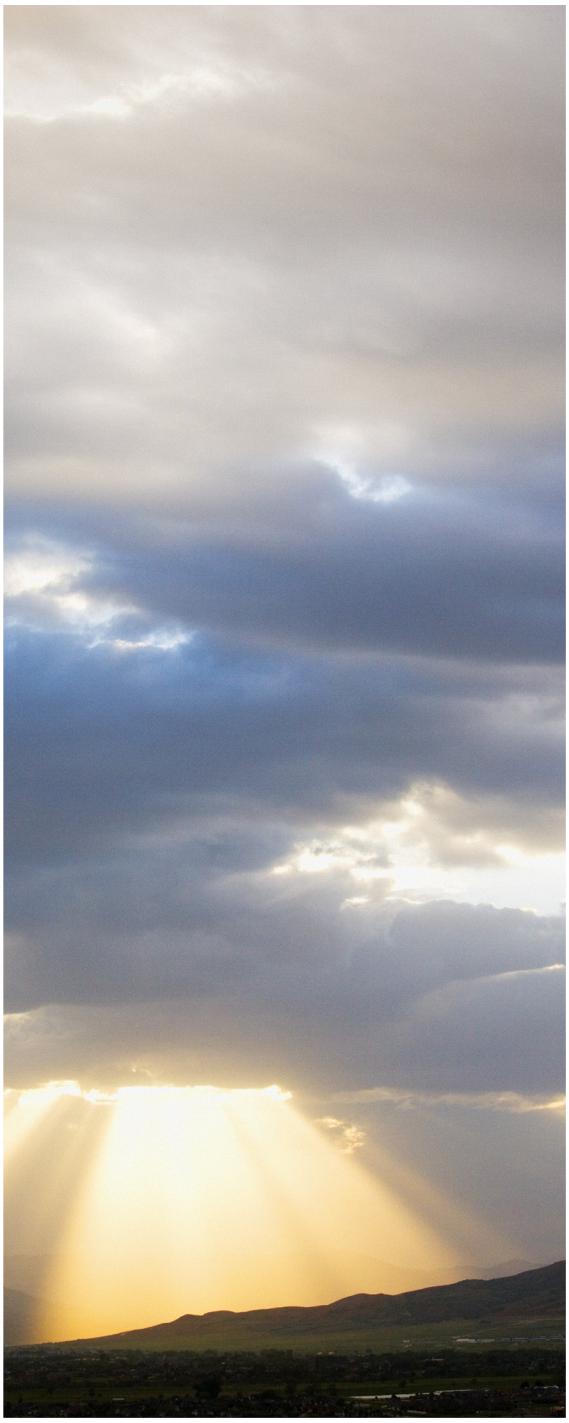
Shown: percentage of respondents

84% of respondents indicated that they have an IT risk management program in place or are considering it within the coming year.

Our perspective

- Revisit your information security strategy to conform to the current risk landscape.
- Instead of acquiring the latest tools, focus on the fundamentals.
- Implement a structured, pragmatic approach to managing IT risk to make sure it focuses on the risks that matter. We see an IT risk management or governance risk and compliance (GRC) approach as a key future investment for many organizations.
- Address the entire IT risk universe in your IT risk or GRC program, which is broader than just information security.

Summary of survey findings



Data is everywhere: at work, at home and at play. It's in our computers, our televisions, our phones, our cars and our appliances. Some of the world's biggest companies have for decades relied on data to help conduct their business. But lately, not only do many of the world's largest companies use data, it is their whole business.

Through mobile computing, the use of cloud-based services and the feverish increase in the use of social media, that ever-present data is increasingly at risk. Our 2011 Global Information Security Survey shows that, despite economic pressures, many respondents recognize the need to safeguard and secure data. In fact, survey respondents indicate their information security budgets are increasing.

However, the survey also shows that the recognition of the challenges posed by new technologies does not always translate into appropriate actions to address that risk. The survey revealed a growing gap between business needs and the capabilities of the corresponding information security efforts. It is clear that now is the time for that gap to be filled with an effective strategic information security plan that focuses less on short-term fixes and more on a holistic approach integrated with long-range strategic corporate goals.

Summary

- 72% of respondents see an increasing level of risk due to increased external threats.
- 49% of respondents stated that their information security function is meeting the needs of the organization.

Mobile computing

- 80% of respondents are either planning, evaluating or actually using tablet computers.
- 57% of respondents have made policy adjustments to mitigate the risks related to mobile computing.

Cloud computing

- 61% of respondents are currently using, evaluating or planning to use cloud computing-based services within the next year.
- Almost 90% of respondents believe that external certification would increase their trust in cloud computing.

Social media

- Nearly 40% of respondents rated social media-related risks issues as challenging.
- 53% of respondents have implemented limited or no access to social media sites as a control to mitigate risks related to social media.

Data loss prevention

- 66% of respondents have not implemented data loss prevention tools.
- 74% of respondents have defined a policy for the classification and handling of sensitive data as a control for data leakage risk.

Business continuity management

- For the second consecutive year, respondents have indicated that business continuity is their top funding priority.

IT risk management

- 56% of respondents indicated that their current information security strategy needs to be modified or needs further investigation.
- 31% of respondents indicated that their organization has recently purchased information security solutions that are perceived as having failed or under-delivered.
- 84% of respondents indicated that they have an IT risk management program in place or are considering one within the coming 12 months.

Survey approach

Ernst & Young's 2011 Global Information Security Survey was developed with the help of our assurance and advisory clients.

This year's survey was conducted between June 2011 and August 2011. Nearly 1,700 organizations across all major industries and in 52 countries participated.

Methodology

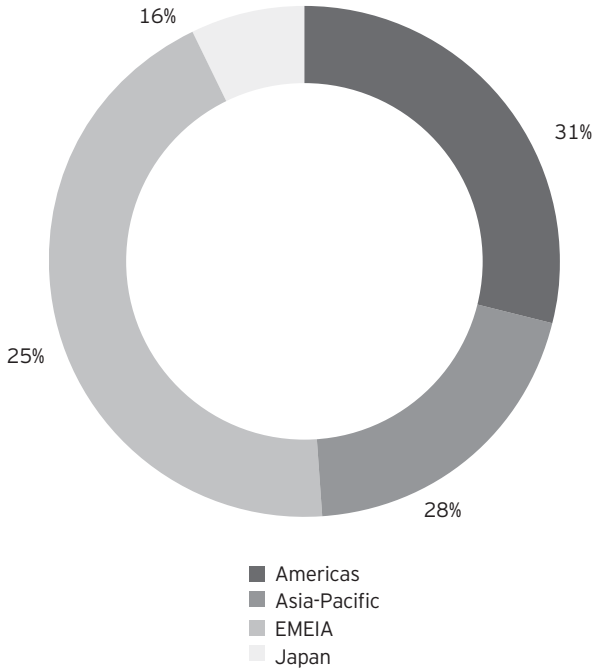
Our survey is not just another online poll that anyone can access. We invited CIOs, CISOs and other information security professionals and executives to participate.

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. When this was not possible, the questionnaire was conducted online.

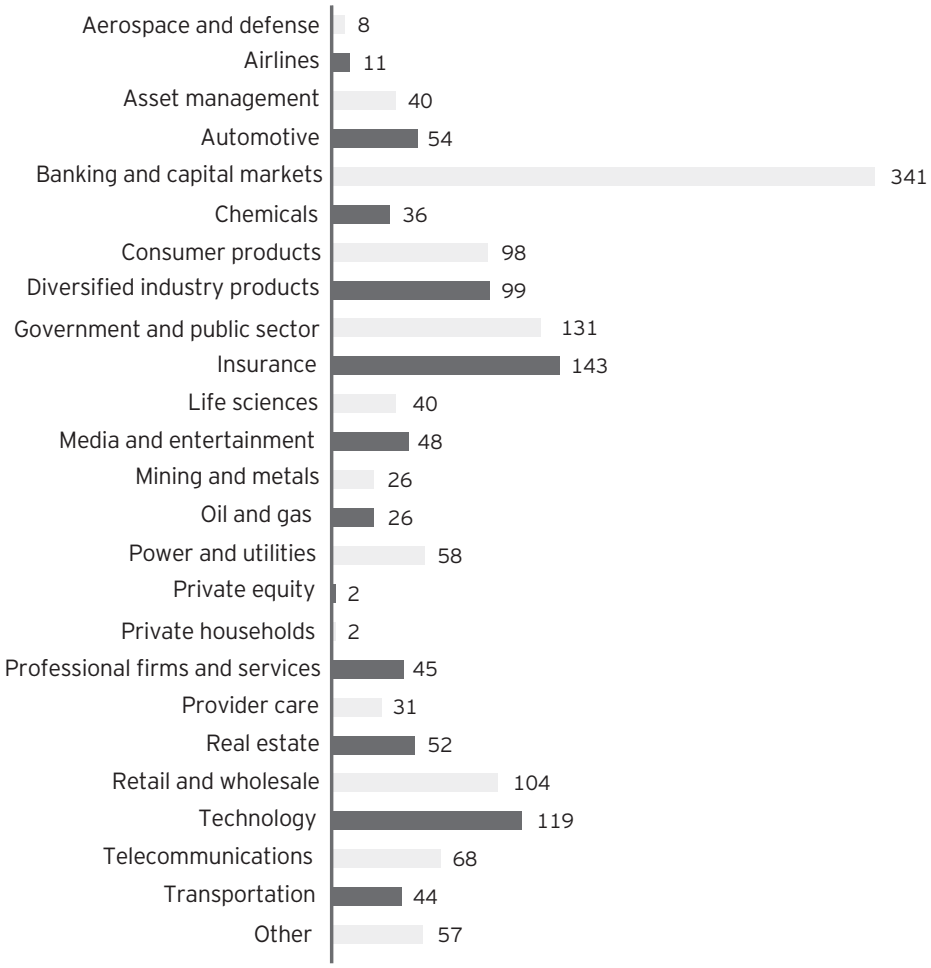
If you wish to participate in Ernst & Young's 2012 Global Information Security Survey, contact your local Ernst & Young office, or visit www.ey.com and complete a simple request form.

Survey participants by region



Shown: percentage of respondents

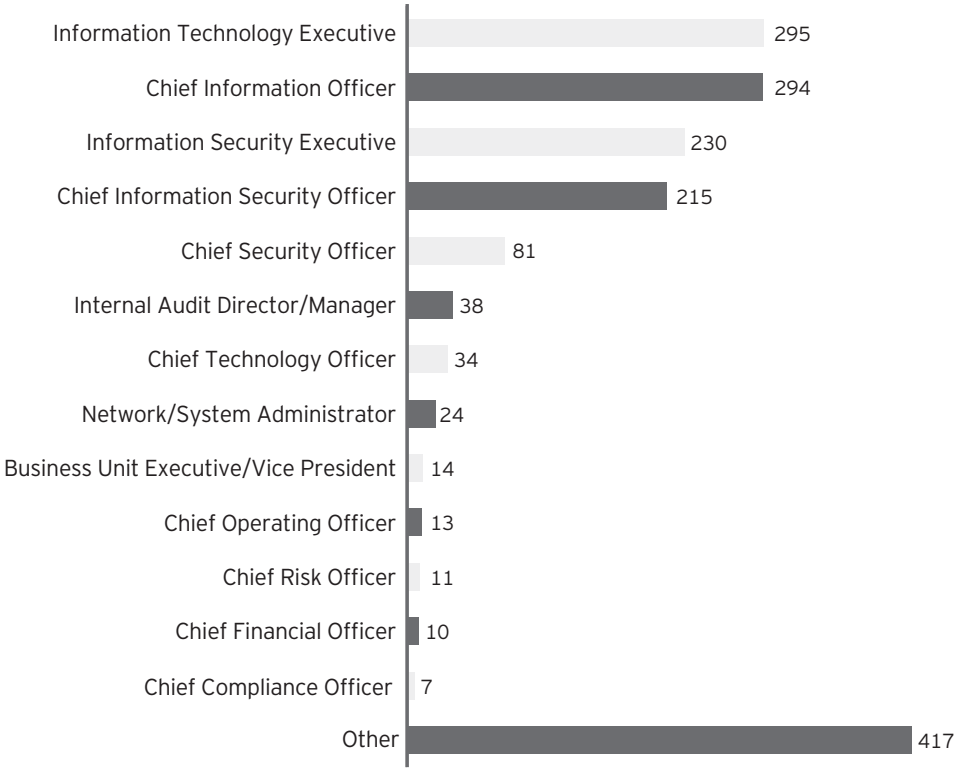
Survey participants by industry



Shown: number of respondents

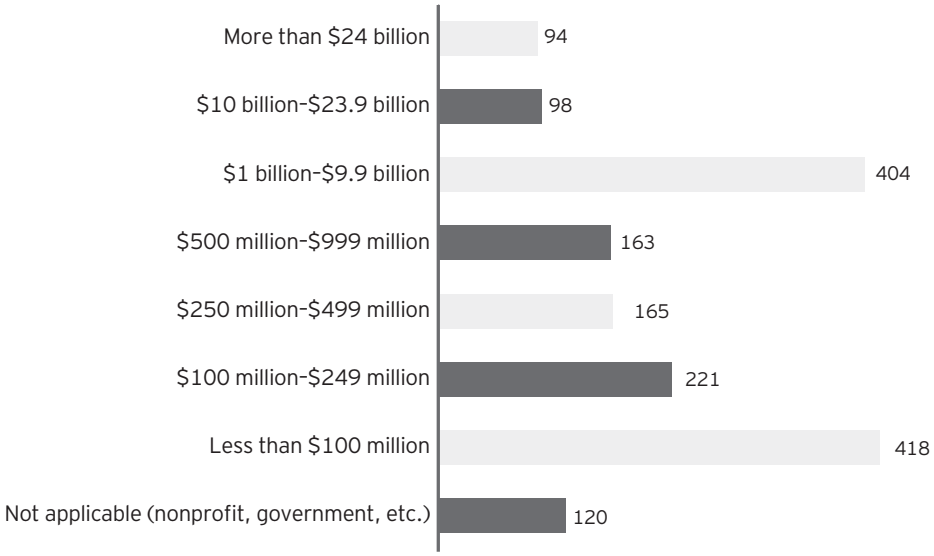
Survey approach (continued)

Survey participants by title



Shown: number of respondents

Survey participants by annual revenue (US$)

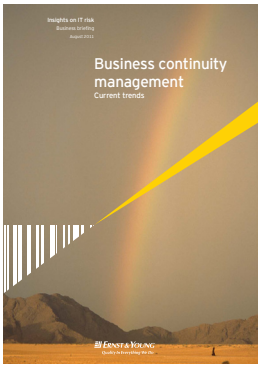


Shown: number of respondents

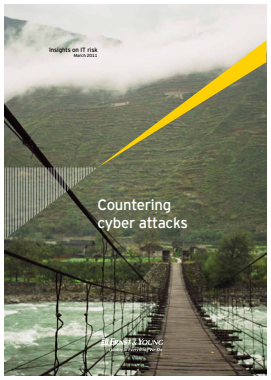
Related insights

Thought leadership at ey.com/informationsecurity

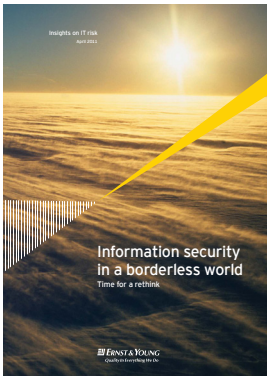
Business continuity management
While disasters and the resulting non-availability of resources – data, raw materials, personnel, finished products – can be devastating, only about half of companies have taken steps to address these potential disruptions. This report outlines the need to develop, maintain and sustain effective business continuity management programs.



Countering cyber attacks
Given the continuous and persistent threat posed by new waves of attack channels and malicious entities, leading companies recognize the need to instill a new mind-set and approach toward the organization's security strategy. This report describes how companies should examine their current security strategy, controls and maturity of controls to determine their gaps and weaknesses.



Information security in a borderless world
Traditional security models that focus primarily on keeping the bad guys out no longer work. It's time to radically rethink how organizations can keep their most valuable assets safe. This report describes how effective information security can help our clients transform their information security strategy and build trust in a borderless world.

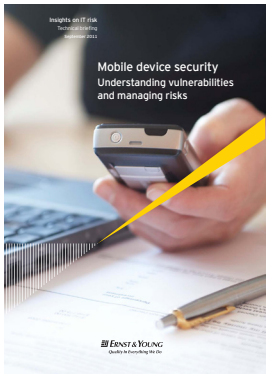


Cloud computing: issues and impacts
Cloud computing is a fundamental shift in IT that alters the technology industry power structure, enhances business agility and improves everyone's access to computing, storage and communications power. This report describes the issues and impacts of all aspects of cloud computing.

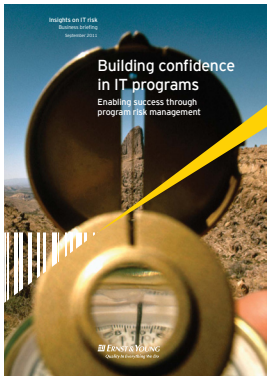
The evolving IT risk landscape
Security risks posed by mobile computing, cloud computing, virtualization, social media and online payments are a critical issue for investors, regulators, shareholders and executives. A strategic IT risk management program helps address IT risks consistent with strategic corporate objectives and helps set risk culture by providing management with a holistic, enterprise-wide perspective.

Data loss prevention: keeping your sensitive data out of the public domain
Advances in technology and how users apply that technology have increased the risk of data leakage. The blurry line between work and personal use of – and access to – data can result in unintentional leaks, as well as malicious ones. This paper explores how leading companies can identify and address holes in their information security strategy.

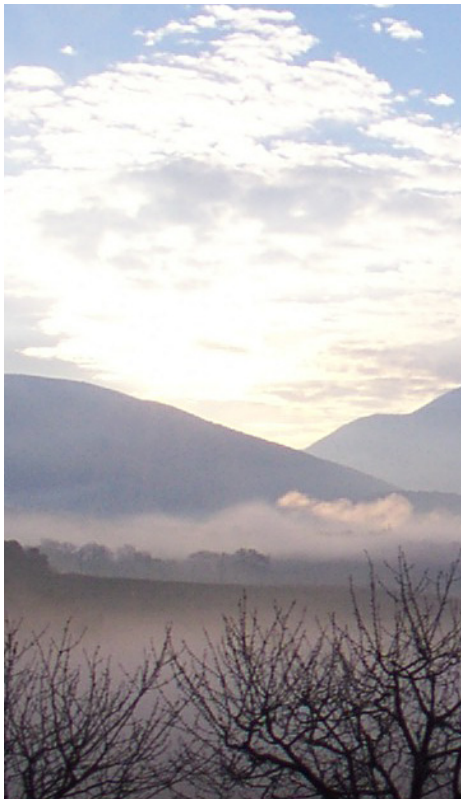
Mobile device security
Over the past two decades, we have witnessed significant technology advances in mobile devices, from the personal data assistants (PDAs) of the late 1990s and early 2000s to the ubiquitous and multifunctional smartphones of today. New mobile technologies come with new risks that are specific to the various device platforms and technologies. These risks may be mitigated through technical device controls, third-party software, and organizational policy. These components all contribute to an enterprise-wide mobility management program that will ultimately serve as a guide in the rapidly evolving mobile environment.



Building confidence in IT programs
Despite an increase in investment, organizations continue to fail to deliver on large IT programs. However, approximately two out of three programs go over budget, are completed too late or do not deliver the expected benefits. Engaging independent Program Risk Management (PRM) assistance is ultimately about building and sustaining confidence in the IT program and having the right information at the right time to make well-informed decisions throughout the program lifecycle.



About Ernst & Young



At Ernst & Young, our Advisory 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 to customers and respond to them more quickly which can significantly enhance both the effectiveness and efficiency of operations. But as organizations move into the cloud and leverage new technologies, the risks also increase.

Our 6,000 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.

Beyond IT, our other 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 on the next page.

Contacts

Global	Telephone	Email
Norman Lonergan Advisory Services Leader	+44 20 7980 0596	norman.lonergan@uk.ey.com
Paul van Kessel IT Risk and Assurance Services Leader	+31 88 40 71271	paul.van.kessel@nl.ey.com
Advisory Services		
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 Leader	+61 2 9248 4923	doug.simpson@au.ey.com
Naoki Matsumura Japan Leader	+81 3 3503 1100	matsumura-nk@shinnihon.or.jp
IT Risk and Assurance Services		
Bernie Wedge Americas Leader	+1 404 817 5120	bernard.wedge@ey.com
Manuel Giralt Herrero Europe, Middle East, India and Africa Leader	+34 915727479	manuel.giraltherrero@es.ey.com
Troy Kelly Asia-Pacific Leader	+852 2629 3238	troy.kelly@hk.ey.com
Giovanni Stagno Japan Leader	+81 3 3506 2411	stagno-gvnn@shinnihon.or.jp

Ernst & Young

Assurance | Tax | Transactions | Advisory

About Ernst & Young
Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 152,000 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.

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. For more information about our organization, please visit www.ey.com.

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.

EYG no. AU0981

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.

www.ey.com/informationsecurity