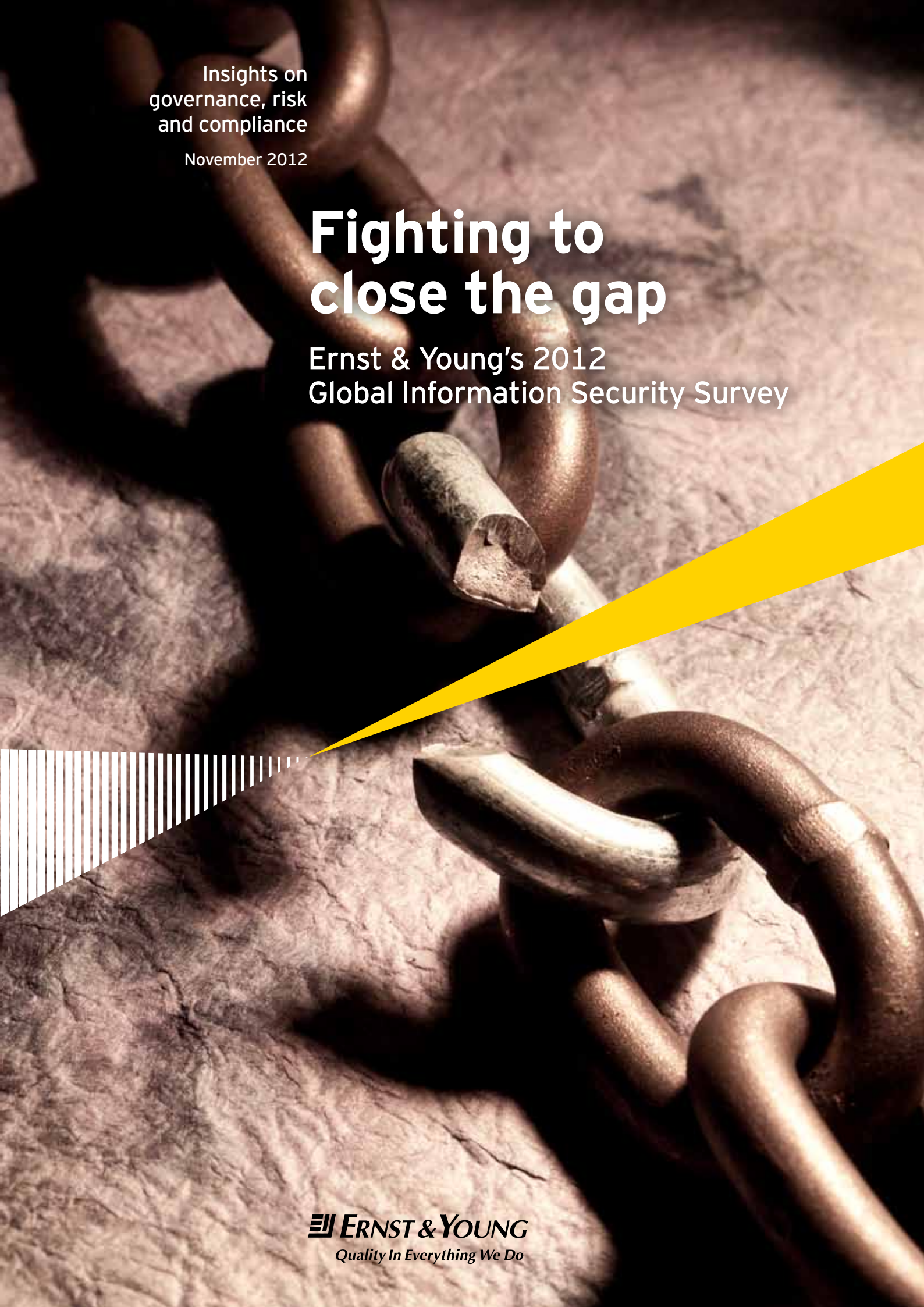


Insights on governance, risk and compliance

November 2012

Fighting to close the gap

Ernst & Young's 2012 Global Information Security Survey

Ernst & Young
Quality In Everything We Do

Contents

Welcome

Paul van Kessel
Global IT Risk and Assurance Services Leader, Ernst & Young

The Ernst & Young Global Information Security Survey is one of the longest running, most recognized and respected annual surveys of its kind. Now in its 15th year, our survey has helped our clients focus on the most critical risks, identify their strengths and weaknesses, and improve their information security.

We invited CIOs, CISOs, CFOs, CEOs and other information security executives to participate in the survey. This year, we received feedback from 1,836 participants in 64 countries and across all industry sectors.

In our 2012 report, we start by taking a look back to understand the advances organizations have made to improve their information security programs. What we have learned is that for every step forward many organizations have taken to secure their data, they are failing to keep pace with the speed and complexity of change.

As each year passes, the speed and complexity of change accelerates, creating a gap between where an organization's information security program is and where it needs to be. Eight years ago, the gap was narrow. Today, it's a chasm.

The origins of the gap are as complex as the variety of issues information security professionals face. However, based on our survey results, the issues can be organized into four distinct categories: alignment, people, process and technology. What cannot be categorized yet are the issues looming on the horizon in the form of governmental intervention and renewed regulatory pressures to address information security risk.

Short-term fixes and bolt-on solutions are not enough. Organizations fighting to narrow the gap that mobile computing, social media, cloud, cyber crime and advanced persistent threats create, need to fundamentally transform their approach to information security. This year's survey will disclose what fundamental transformation looks like and the steps organizations can take to make such a shift successful.

I would like to send a personal "thank you" to all our survey participants who took the time to share their thoughts and experiences with us. We are looking forward to further discussing the implications of the survey findings with our clients and prospects, regulators and governments, as well as analysts and universities.

Paul van Kessel

IT Risk and Assurance Services Global Leader, Ernst & Young

Questions for the C-suite

- What has your organization done to adjust information security to address the changing environment?
- Has your organization implemented the necessary information security improvements to keep up with the pace of change?
- What impact have changes to security levels had on your organization?
- Has your organization done enough?
- Are your information security objectives and measures aligned to your business strategy?

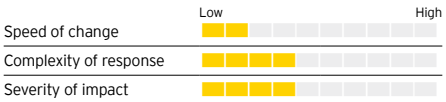
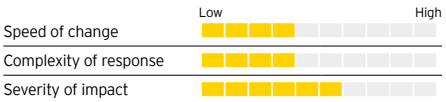
The speed of change, a widening gap

Virtualization, cloud computing, social media, mobile, the disappearing lines that once divided business and personal IT activities — the velocity of change in information security can be dizzying if we think about how quickly and how far technology has evolved in such a short period of time. The rise of emerging markets, the financial crisis and offshoring only add to the complexity of ever-evolving information security issues — and the urgency to address them.

Organizations have substantially improved information security programs to address accelerating threats. They have added new features to their information security systems, redefined strategies, installed new information security function components and added more people.

These step-by-step adjustments have undoubtedly improved information security capabilities. It just hasn't improved them enough. In fact, our survey results suggest that for as many steps as organizations are taking to enhance their information security capabilities, few are keeping up with what is going on around them. Even fewer are able to get far enough ahead to anticipate not only today's threats, but also tomorrow's.

In the pages that follow, we chart how far information security capabilities have come from 2006 until today — and how far they still need to go to close the gap between vulnerability and security.

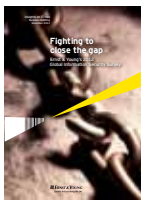
	2006	2007	2008	2009
Information security survey themes	 **Achieving success in a globalized world**	 **Achieving a balance of risk and performance**	 **Moving beyond compliance**	 **Outpacing change**
Key trends	Prior to 2006, information security was mainly seen as an important component of mitigating financial risk and meeting new compliance requirements, such as SOX 404. After 2006, the scope of information security expanded in two directions: 1. Information security needed to protect the organizations more broadly, especially in a globalized world. 2. Information security needed to have a clear return on investment, requiring an alignment of risk and performance.		In 2008, information security matured beyond compliance. Protecting brand and reputation became the primary driver in an environment of escalating threats. Identifying and managing new risks and leveraging technology to secure the business were also focal points. At the same time, the world changed dramatically: ▸ A global financial crisis and economic downturn hit many organizations hard. ▸ Emerging markets gained much more prominence. ▸ The competitive landscape changed. Confronted with these challenges, organizations focused on reshaping, restructuring and reinventing themselves to keep up with the new requirements and increasing cost pressures.	
Impact on organizations				
Recommended steps	**2006** ▸ Stay proactively involved in achieving regulatory compliance ▸ Improve risk management of third-party relationships ▸ Invest more in privacy and personal data protection **2007** ▸ Align information security with the business ▸ Face the challenges of staffing information security functions		**2008** ▸ Take a more business-centric view ▸ Keep up investments in information security despite economic pressures ▸ Invest in training and awareness programs to keep people from being the weakest link **2009** ▸ Consider co-sourcing to address a lack of resources and tighter budgets ▸ Assess the potential impact of new technology and the organization's ability to protect its assets ▸ Know the risks posed by increasing external and internal threats	

Information security survey themes

2010 | 2011 | 2012

Borderless security

Into the cloud, out of the fog



The information security gap

Key trends

With a global economy still in recovery, and in an environment of sustained cost pressures and scarce resources, two new waves of change emerged:

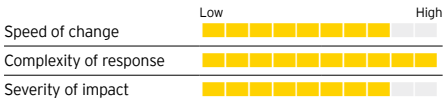
1. Organizations started to realize that with globalization, data is everywhere. Employees were increasingly sending data to business partners over the internet or carrying the data with them on mobile devices. The traditional boundaries of an organization were vanishing along with the traditional security paradigms.
2. Data processing moved into the cloud. Organizations understood the security requirements associated with IT outsourcing. Moving to the cloud required the information security function to completely rethink its approach to securing information.

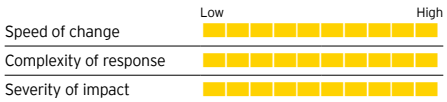
The velocity and complexity of change accelerates at a staggering pace:

- Virtualization, cloud computing, social media, mobile, and other new and emerging technologies open the door to a wave of internal and external threats.
- Emerging markets, continuing economic volatility, offshoring and increasing regulatory requirements add complexity to an already complicated information security environment.

Organizations have made great strides in improving their information security capabilities. But for as many steps as they have taken, they continue to fall behind, creating an information security gap that grows ever larger.

Impact on organizations





Recommended steps

2010

- Address the risks associated with emerging technologies
- Increase investment in data loss prevention tools
- Take an information-centric view of security that better aligns to the business

2011

- Bring information security into the boardroom
- Protect the information that matters most
- Embrace encryption as a fundamental control
- Focus on the fundamentals

2012

- Continue to make information security a board-level priority
- Develop an integrated strategy around corporate objectives, and consider the whole risk landscape
- Use data analytics to test the risk landscape and understand the data you need to protect most
- Use a three- to five-year horizon for budgeting to enable long-term planning
- Innovate, innovate, innovate
- Start working on a fundamental transformation, as described later in this report

How far do organizations still need to go?

The improvements that organizations are making

In response to the key recommendations that have been made over the years, organizations have significantly enhanced their information security programs to address changes in the risk environment.

The most significant evolution from 2006 to today may be the shift in how organizations view the security of information. Once referred to as IT security, the responsibility for protecting an organization's data used to belong solely or primarily to the IT function. No more! Today, organizations understand that data security is a strategic business imperative that requires an enterprise response under the broader information security umbrella.

Other improvements have included:

Stronger compliance to regulatory requirements

For years, external threats from worms and viruses were information security's primary driver. All that changed in 2005 when compliance became a board-level issue. Since that time, with the exception of 2008 when brand and reputation supplanted it, achieving compliance with regulations has consistently been the most important driver of information security for approximately 80% of respondents.

Stronger adherence to regulatory requirements has significantly improved how organizations manage information security risk. For example, in the financial services industry — one of the most regulated industries — banks in the US are talking about collaborating on identifying ways to address information security risks, despite competitive sensitivities. Information security is on President Barack Obama's radar, and banks are trying to improve governance around how they manage information security risk before regulators do it for them.

Better transparency

In 2008, only 18% of respondents indicated that their information security was an integrated part of the organization's business strategy; 33% suggested that their information security strategy was integrated as part of the organization's IT strategy. By 2012, these numbers have jumped to 42% and 56%, respectively.

Threats seen as unforeseeable and diverse

The dependence of civilizations on large IT-centric infrastructures has increased over the past decades. President Barack Obama recently wrote in a column, "So far, no one has managed to seriously damage or disrupt our critical infrastructure networks. But foreign governments, criminal syndicates and lone individuals are probing our financial, energy, and public safety systems every day … . Taking down vital banking systems could trigger a financial crisis." (Barack Obama, "Taking the Cyberattack Threat Seriously," *The Wall Street Journal*, 19 July 2012).

Sources of catastrophic threats are increasingly seen as unforeseeable and diverse — state-sponsored attacks, organized crime, hacktivists, natural disaster, terrorism. Especially for critical infrastructure networks, organizational resilience is a desired end state. It is a descriptive rather than prescriptive term denoting the capability of an organization to withstand disruption and achieve long-term prosperity.

The question arises whether a cyber security-driven event may trigger another catastrophic 9/11-scale event. This would automatically put the emphasis on high-impact and low occurrence types of risk — the most difficult risks to analyze and mitigate.

Developing an integrated information security strategy is critical to gaining a holistic view of the risk landscape and fully addressing those risks. Leading organizations have recognized this and are working harder to ensure that information security is embedded into both business and IT strategies.

Increasing importance of business continuity management

In 2006, business continuity was just beginning to appear on the radar for information security. In 2008, the primary responsibility for business continuity management resided with IT, where the focus was really more on disaster recovery rather than full business continuity.

By 2012, organizations ranked business continuity as the second most mature information security function within the organization. However, they still need to do more; 47% of respondents say that they expect to spend more on business continuity and disaster recovery in the next year.

Responding to new technologies

When it comes to new technologies, organizations have needed to move quickly. In 2006, smartphones were primarily used by executives and tablets didn't even exist in a consumable form. Risks related to mobile devices, social media and the cloud weren't high on anyone's agenda because they hadn't infiltrated the corporate environment.

Since then, the proliferation of mobile devices and networks, and the blurring lines between business and personal use, have forced organizations to urgently implement policies that address the risks associated with an evolving array of emerging technologies. Organizations are making policy adjustments, stepping up awareness programs, and, in the case of cloud computing, improving oversight of the contract management process for cloud services providers and boosting their encryption techniques.

Accelerating threats

Despite all the improvements organizations are making, the pace of change is picking up speed.

In 2009, 41% of respondents noticed an increase in external attacks. By 2011, that number had leapt to 72%. This year, the number of respondents indicating an increase in external threats has risen again to 77%. Examples of accelerating external threats include hacktivism, state-sponsored espionage, organized crime and terrorism.

In the same span of time, organizations have also noticed an increase in internal vulnerabilities. In this year's survey, nearly half of respondents (46%) say they have noticed an increase. Thirty-seven percent rank careless or unaware employees as the threat that has increased the most over the last 12 months. Interestingly, this number is not much smaller, relatively speaking, to the 50% of respondents in 2008 who cited organization awareness as their most significant challenge to delivering successful information security initiatives.

"The new normal for the CIO is that fast is not fast enough. The same holds true for information security."

Paul van Kessel
IT Risk and Assurance Services Global Leader, Ernst & Young

The remaining gap

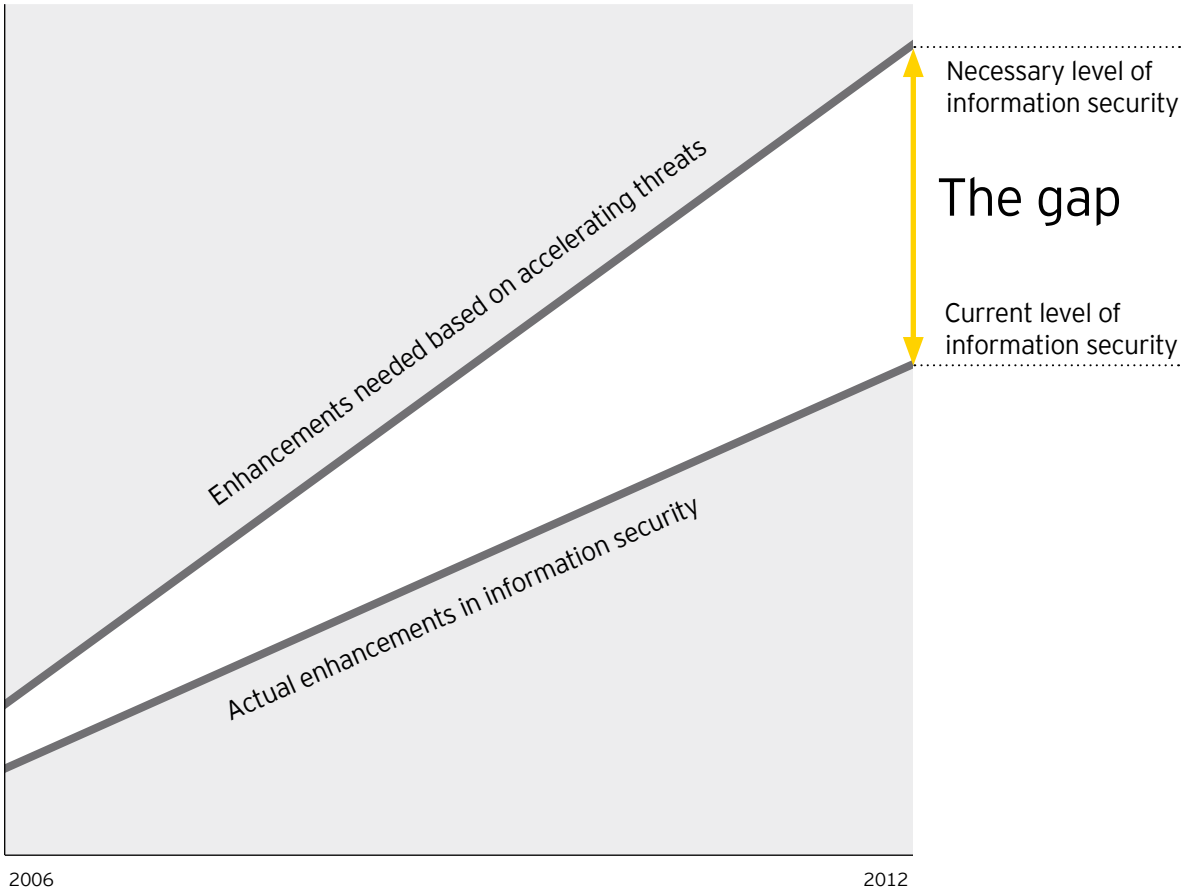
What this year's survey clearly shows is that threats are accelerating significantly faster than the enhancements organizations are making. Of more concern, in some critical areas, not only has there been little improvement, there's been stagnation or even erosion in addressing important information security initiatives.

Such issues include:

- Alignment with the business
- Sufficient resources with the right skills and training
- Processes and architecture
- New and evolving technologies

These are subjects upon which we have consistently reported and for which we have provided recommendations in previous reports.

Without appropriate and effective action, the gap between necessary information security levels and actual information security levels continues to grow. Left unattended, organizations face risks that could ultimately impact their brand or even market share.



Financial services seek to balance risk and growth in Asia-Pacific

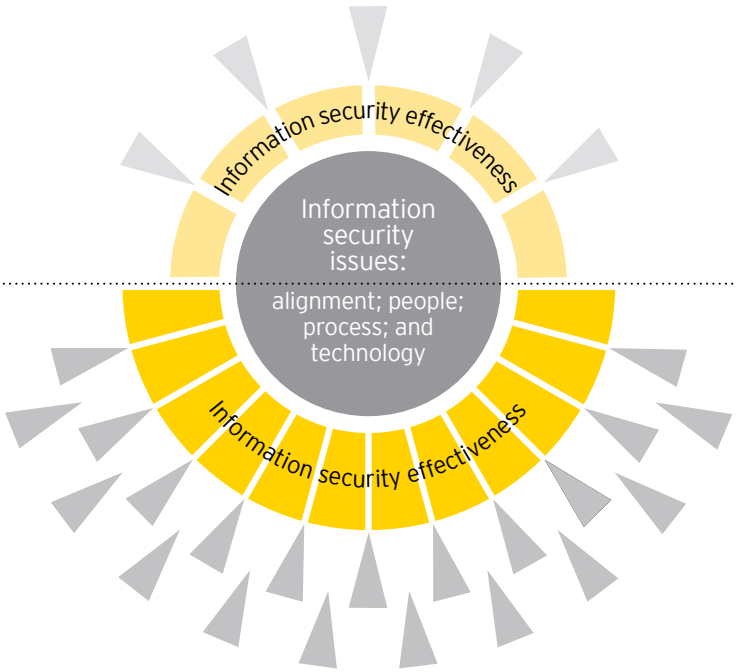
In the Asia-Pacific region, the financial services industry is genuinely interested in taking on additional, but measured, business risks. Organizations hope to either gain greater returns or expand their business footprint in Asian countries. Although critics may agree this is an admirable business strategy, organizations need to think about the compliance implications of multiple regulatory requirements in regional hubs, such as Singapore, Hong Kong and the Philippines.

Why the gap has grown

No single issue is creating the gap between where information security is now and where it needs to be. Rather, the gap is a result of a wide range of compounding issues in the areas of alignment, people, process and technology. What cannot be categorized yet are the issues looming on the horizon in the form of governmental intervention and renewed regulatory pressures to address information security risk.

Risk landscape:
2006-2011
Recognized threats impacting the organization

Risk landscape:
2012 and beyond
More, greater and new threats, impacting more quickly



Unbalanced alignment

56%

of respondents say their information security strategy is aligned to their IT strategy

42%

of respondents say that their information security strategy is aligned to their business strategy

38%

of respondents say their information security strategy is aligned to the organization's risk appetite

For years, Ernst & Young has advocated that information security needs to be more strategically positioned beyond the IT function. Information security needs to become a board-level priority and its executives need to have a seat at the boardroom table. And for a time, information security executives made great strides in achieving this level of visibility, accountability and value. But in recent years, as threats accelerate and economic volatility, emerging markets, offshoring and new technologies add complexity to the role, information security is having to compete with other board-level priorities. As a result, although information security is heading in the right direction, it may not be getting the attention it needs to keep pace with the velocity of change.

Broader alignment needed

The information security agenda continues to be IT-led rather than focused on the overall business strategy.

An effective information security strategy needs to stretch across the entire enterprise and work in tandem with many different functional areas. That's why it is so important that information security's goals are aligned not only with the overall enterprisewide business goals, but also with the various departmental and functional goals.

Admirably, the number of respondents who indicate that their information security strategy is aligned to their IT strategy has risen from 33% in 2008 to 56% in 2012. Similarly, the number of respondents suggesting that their information security strategy is aligned to their business strategy has risen from 18% in 2008 to 42% in 2012.

And yet, in 2012:

- Little more than one third (38%) align their information security strategy to their organization's risk appetite and risk tolerance.
- A little over half (54%) discuss information security topics in the boardroom on a quarterly basis or more frequently. The remaining 46% almost never – or never – discuss the topic with the top governing structure of their organization.

Governance and monitoring responsibilities

Only 5% have information security reporting to the chief risk officer — the person most responsible for managing the organization's risk profile.

Given that information security continues to be IT-led within so many organizations, it's not surprising that 63% respondents indicate that their organizations have placed the responsibility for information security with the IT function.

IT certainly understands information security and the issues that threaten it. However, having an information security strategy so completely governed by IT can also impede effective assessment, measurement and alignment with business priorities.

Some CIOs serve as a bridge between the business and enabling technology, which can help to align information security with business and IT strategies. However, blending IT expertise with a non-IT perspective, organizations can enhance overall information security effectiveness by:

- Helping to create and maintain accurate measurement that aligns with business goals
- Ensuring objective assessment around information security effectiveness
- Resolving decision-making issues, pre-empting potential conflicts of interest and helping to facilitate priority-related discussions which might otherwise be difficult if attempted in an IT-only environment

Notably, 26% of organizations have given responsibility for information security to the CEO, CFO or COO — elevating it to a C-suite topic. But only 5% have information security reporting to the chief risk officer — the person most responsible for managing the organization's risk profile.

This decision becomes critical when it comes to selecting the right tools, processes and methods to monitor threats, gauge performance and identify coverage gaps. Traditionally, IT departments do not have a formal risk landscape or assessment mechanism — something that is fundamental to the risk function. This may explain why 52% of organizations do not have a threat intelligence program currently in place.

Without a disciplined approach to researching and monitoring threat intelligence, the IT function is not only unable to proactively address current threats; it also has no way of anticipating the threats that are lurking just around the corner. This only reemphasizes the gap.

63%

of organizations have placed responsibility for information security with the IT function

26%

of organizations have given responsibility for information security to the CEO, CFO or COO

5%

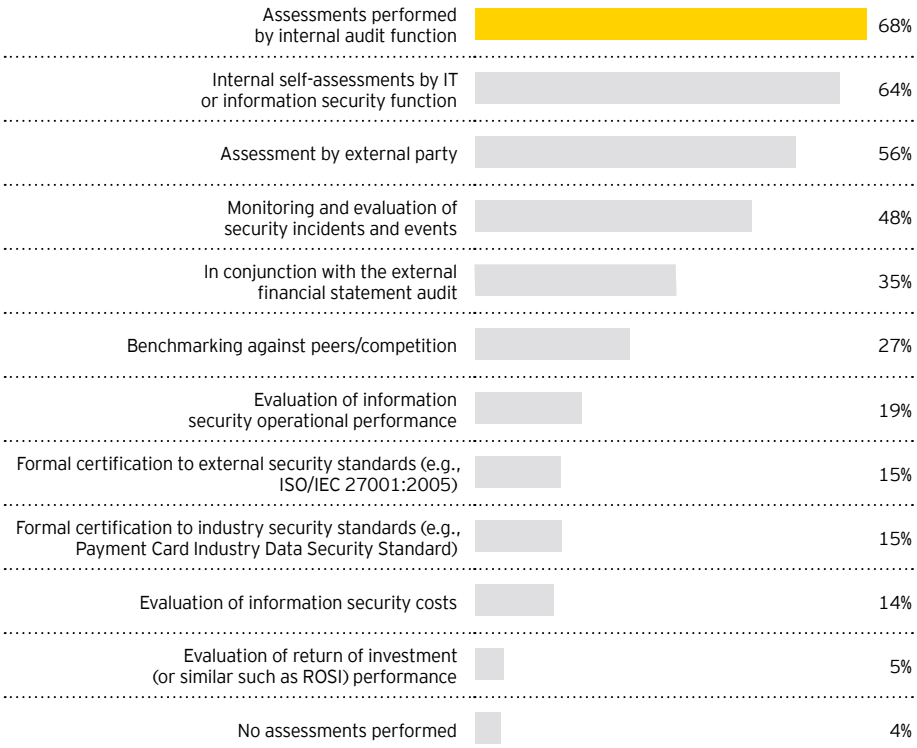
of organizations have given responsibility for information security to the chief risk officer

70%

of respondents indicate that their information security function only partially meets organizational needs and improvements are underway

Further obscuring the clarity around assessment are the multiple means used to monitor information security. As the chart below indicates, a majority of organizations use internal audit (68%) to assess the efficiency or effectiveness of information security. Slightly fewer (64%) use the IT function or information security itself to conduct internal self-assessments.

How does your organization assess the efficiency and effectiveness of information security? *Choose all that apply.*



In fact, the proliferation of threats and the widening gap between vulnerability and security requires multiple sources of assessments. Ideally, companies should use all four of the top techniques identified: assessments performed by internal audit; internal self-assessments; third-party assessments; and the monitoring and evaluation of security incidents. High-performing organizations use a combination of two or more assessment techniques to determine information security efficiency and effectiveness. Based on the high percentage of responses to the top four assessment options, many of the survey's respondents are high performers.

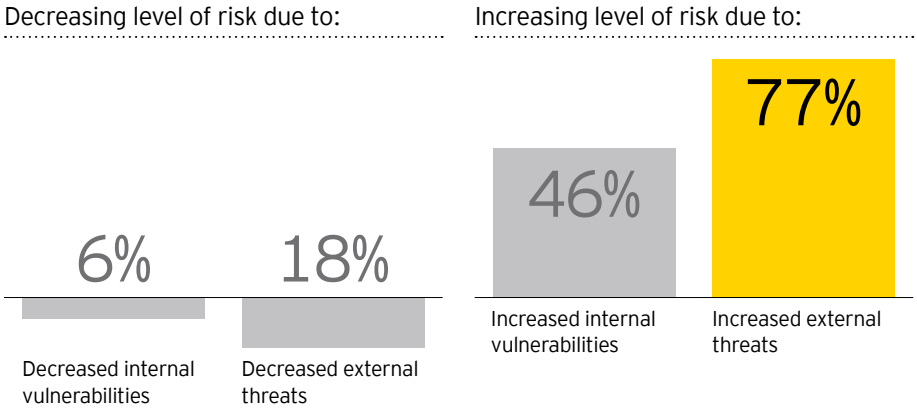
Unfortunately, strong assessment performance does not shield many information security functions from criticism of their performance overall. Only 16% of respondents say that their information security function fully meets organizational needs. Instead, 70% indicate that their information security function partially meets organizational needs and that improvements are underway.

Changing risk landscape

Physical measures can be built to prevent criminal acts. But it is often more difficult to prevent incompetence, mischief or revenge.

Organizations recognize that the risk environment is changing. Nearly 80% agree that there is an increasing level of risk from increased external threats, and nearly half agree that internal vulnerabilities are on the rise.

Change in the risk environment in the last 12 months



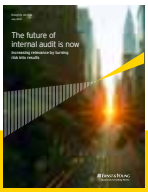
Additionally, 31% of respondents have seen increases in the number of security incidents compared to last year, while only 10% saw a corresponding decrease. Fifty-nine percent indicate that the number of incidents have stayed the same. As the frequency and nature of information security threats increase and the number of security incidents rises, so too does the potential impact of security lapses.

External threats are not the only security gap facing global organizations. Inadvertent employee data loss is also rising.

Effective management, training and awareness can stem the flow of the data loss, and physical measures can be built to prevent criminal acts. But it is often more difficult to prevent those determined to deliberately wreak havoc for reasons of mischief, revenge or greed.

"Organizations need to readjust their thinking from protecting the perimeter to protecting the data. It's all about having the right focus."

Manuel Giralt Herrero
IT Risk and Assurance Services EMEIA Leader, Ernst & Young



Information security a priority for internal audit professionals

In 2012, Ernst & Young commissioned a global survey to explore the evolving role of internal audit. Almost half of respondents (48%) indicated that information security and privacy risk were top priorities for their organizations. In fact, 14% devote between 10% and 20% of their audit time to information security risk and expect to continue doing so in the next two years.

To read our report, ***The future of internal audit is now***, please visit www.ey.com/internalaudit.

44%

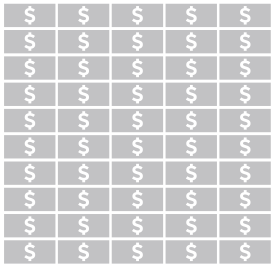
of respondents expect to keep their information security budgets the same over the next 12 months

30%

of respondents expect an information security funding increase of 5% to 15%

9%

of respondents expect to see an information security budget increase of 25% or more



32%

of respondents spend US$1 million or more on information security

More money, yes. But is it well spent?

Survey respondents rank business continuity management as their highest spending priority in the next 12 months.

As organizations around the world are seeing the rise in the threat levels, they are responding by spending more and adjusting their priorities:

- 44% of respondents will be keeping their budgets the same over the next 12 months
- 30% expect an information security funding increasing of 5% to 15%
- 9% expect to see an information security budget increase of 25% or more

In terms of budgets, size varies widely:

- 32% spend US$1 million or more on information security

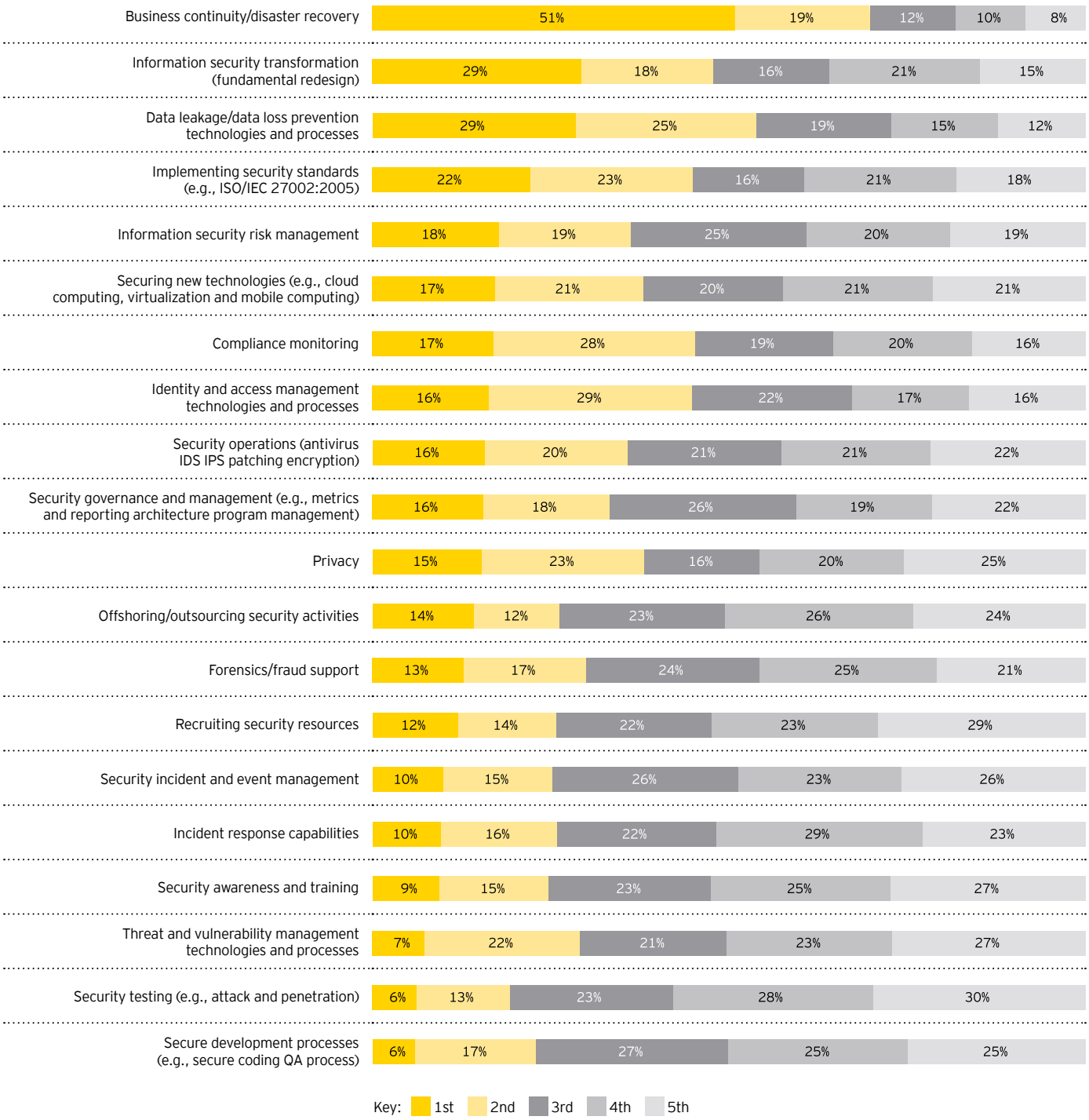
As the chart at right illustrates, the highest priority area (51% of respondents) for investment in the next 12 months is business continuity management and disaster recovery, up from 36% in 2011. This reflects our perspective, highlighted earlier in the report, that business continuity is an area in which organizations have worked hard to improve. We expect it is also, at least in part, a reaction to the disruptive and sometimes catastrophic events of the past few years – earthquakes, hurricanes, fires and tsunamis – that crippled technology, wiped out supply chains and sliced earnings.

Interestingly, the second-highest ranked spending priority for respondents was a fundamental redesign of their information security program. This underlines the fact that leading companies recognize the gap described in the first chapter of this report. These organizations understand that adding point solutions or working on incremental improvements is no longer sufficient. An information security transformation (or fundamental shift) is necessary to face today's issues.

At almost the opposite end of the spectrum, security testing was considered a high priority by only 6% of businesses. Low response rates at the bottom of the chart suggest that respondents feel that they have a level of confidence in these areas – that they are doing enough and can therefore turn their attention to the higher-priority areas.

In terms of where organizations plan to increase their investment in the coming year, it's no surprise that securing new technologies, business continuity and disaster recovery top the list. As the chart on page 19 suggests, more than half (55%) expect to spend more on securing new technologies. A slightly lower percentage (47%) are planning to spend more on their number one priority – business continuity. A little more than one quarter (26%) plan on spending more on their number two priority – information security transformation.

Which of the following information security areas are defined as "top priorities" over the coming 12 months?



A whole new paradigm

In the war over government data security, statistics indicate the bad guys are winning. And some security experts say any hope of reversing that trend will take "a whole new paradigm" in IT security.

The U.S. Government Accountability Office (GAO) reported that federal data breaches involving unauthorized disclosures of personally identifiable information increased by 19%, or about 13,000 to 15,500, from 2010 to 2011.[1] At least some of the time, victims of those breaches are being left in the dark about it for months. About 123,000 Thrift Savings Plan participants whose personal information was compromised in a July 2011 breach were not notified until May 2012.

This is not the only instance. *The Washington Business Journal* reported that the U.S. Environmental Protection Agency (EPA) waited months to notify 5,100 employees and 2,700 "other individuals" of a data security breach in March 2012 that exposed their Social Security numbers and banking information.[2]

[1] "Data breaches up 19 percent, GAO reports;" www.federaltimes.com; 31 July 2012; http://www.federaltimes.com/article/20120731/IT01/307310003/Data-breaches-up-19-percent-GAO-reports.

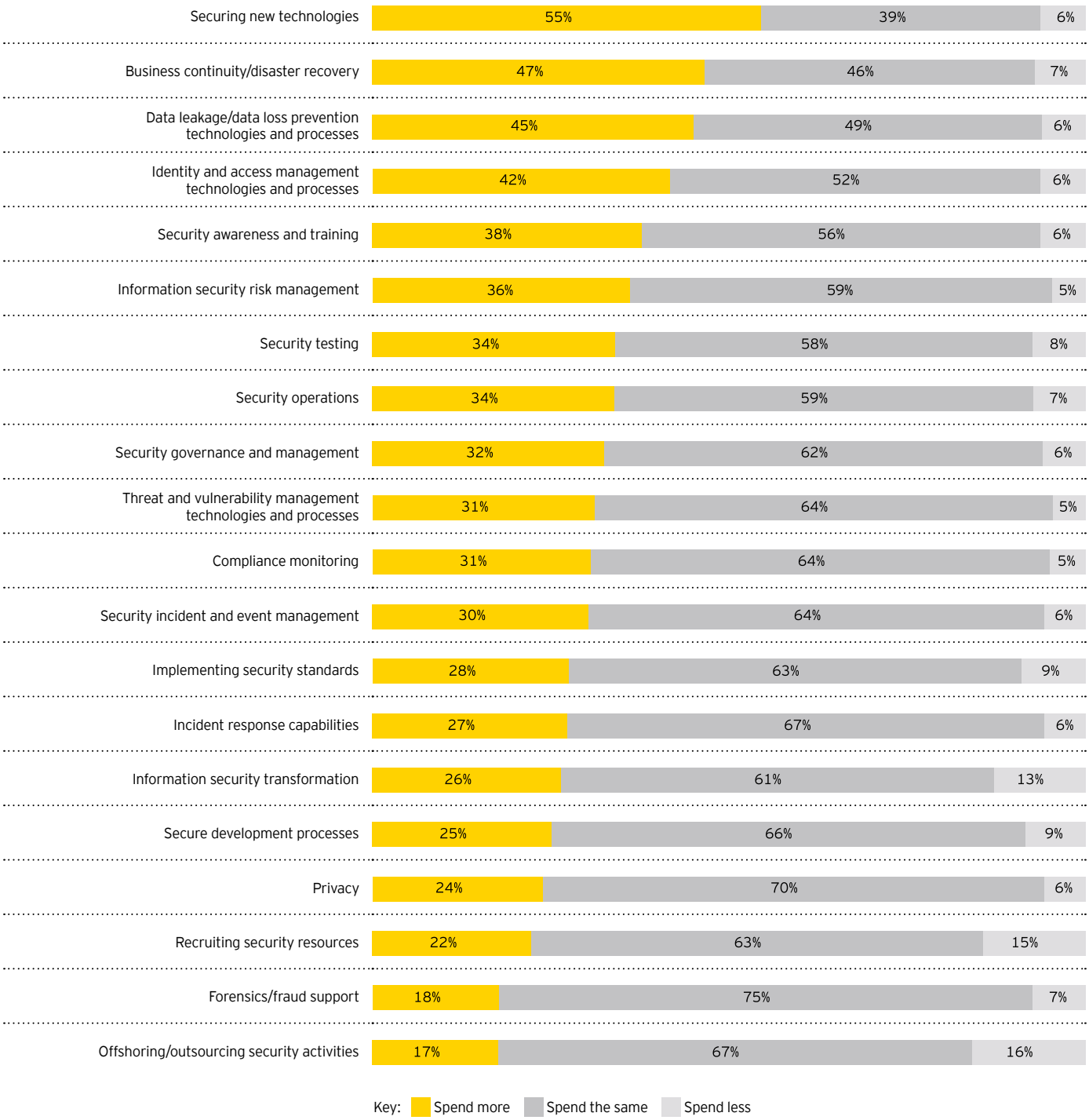
[2] Aitoro, Jill; 'EPA security breach exposes personal information of 8,000 people;" Washington Business Journal; www.bizjournals.com; 2 August 2012; http://www.bizjournals.com/washington/news/2012/08/02/epa-security-breach-exposes-personal.html.

Interesting fact

Organizations that benchmark against their competition to gauge information security effectiveness indicate higher than average financial impact. Also, significantly, nearly 25% of all respondents indicate that they do not know the financial impact.

For organizations that do no assessment of effectiveness (4% of all respondents), the percentage that does not know the impact of information security issues rises to 40%.

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



Key obstacles to information security effectiveness

62%
Budget constraints

43%
Lack of skilled resources

26%
Lack of tools

20%
Lack of executive support

Not enough resources, not the right skills

It's a familiar refrain, particularly in today's era of economic volatility and spending restraint: too much work, not enough resources. But a lack of resources only tells part of the story. Information security doesn't just need more resources; it needs people with the right skills and training to meet rapidly evolving changes in the information security landscape.

Resource constraints

Only 22% of respondents indicate that they are planning on spending more in this area in the next 12 months.

When we asked organizations which main barriers and obstacles are challenging the ability of their information security function to deliver, 43% of respondents cite a lack of skilled resources. This figure is no doubt linked to the only factor that scored above it – budget constraints. And yet, only 22% of respondents indicate that they are planning on spending more in this area in the next 12 months.

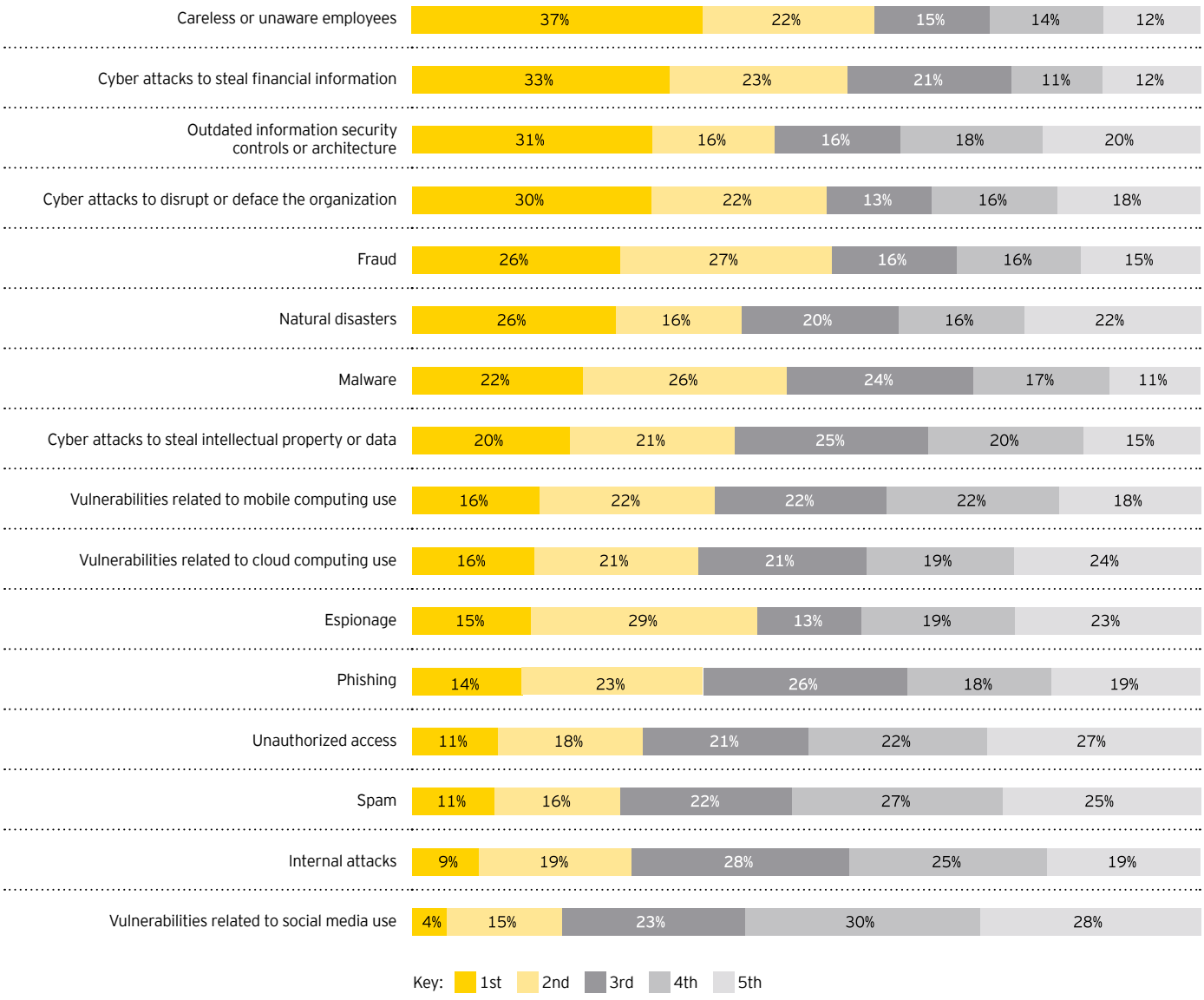
Limited security awareness training

Organizations need to train employees outside of the information security function about the role they must play in keeping the organization's information safe.

Finding the right skilled resources within information security is only one part of the equation. Given the acceleration of external threats, coupled with the proliferation of mobile devices and networks that are being used for both work and play, organizations also need to devote resources and money to train employees outside of the information security function about the role they must play in keeping the organization's information safe. As we mention earlier, 37% of respondents see the threat that has most increased their organization's risk exposure as careless or unaware employees. As well, the number of actual incidents caused by inadvertent employee data loss has risen by 25% in the last year.

Respondents indicate that they intend to spend more, but that amount will still only capture approximately 5% of the overall information security spend.

What threats and vulnerabilities have most increased your risk exposure over the last 12 months?



Data stolen from employee's car

According to eweek.com, softpedia.com and nakedsecurity.com reports, in August 2012, a group of Indiana-based doctors, the Cancer Care Group, acknowledged that backup media containing information on 55,000 patients and employees was stolen from an employee's car the month before.

Although small on the scale of data breaches reported by organizations, the stolen data included patient names, addresses, dates of birth, Social Security numbers, medical record numbers, insurance information and clinical information; as well as their employees' dates of birth, Social Security numbers and beneficiary names.

Insufficient process rigor

In 2009, we suggested that organizations needed to take an information-centric view of security to help ensure better alignment with their information flows. We further suggested that only by understanding the use of information within critical business processes could an organization, and in particular its information security function, truly begin to manage its security needs. We offered these recommendations assuming that organizations had in place, or would implement, the necessary processes – including a structured, effective framework or information security management system. In 2012, we learned that a majority of organizations still don't have a framework.

"Information security must be 'business back' rather than 'technology forward.'"

Bernie Wedge
IT Risk and Assurance Services Americas Leader, Ernst & Young LLP

No security architecture framework

A patchwork of non-integrated, complex and frequently fragile defenses creates significant gaps in security.

Surprisingly, 63% of respondents in this year's survey indicated that their organizations have no formal security architecture framework in place, nor are they necessarily planning on using one. For some organizations, skill resources, security maturity or budget may be playing a role in their decision-making. Other organizations may simply be hoping the issue will go away on its own. However, it is encouraging to see in the chart on the right that 37% use one or more framework, with The Open Group Architecture Framework being the most popular.

These overall findings could explain why 56% of organizations only conduct between 1 and 10 attack and penetration tests annually, and why 19% don't conduct any tests at all.

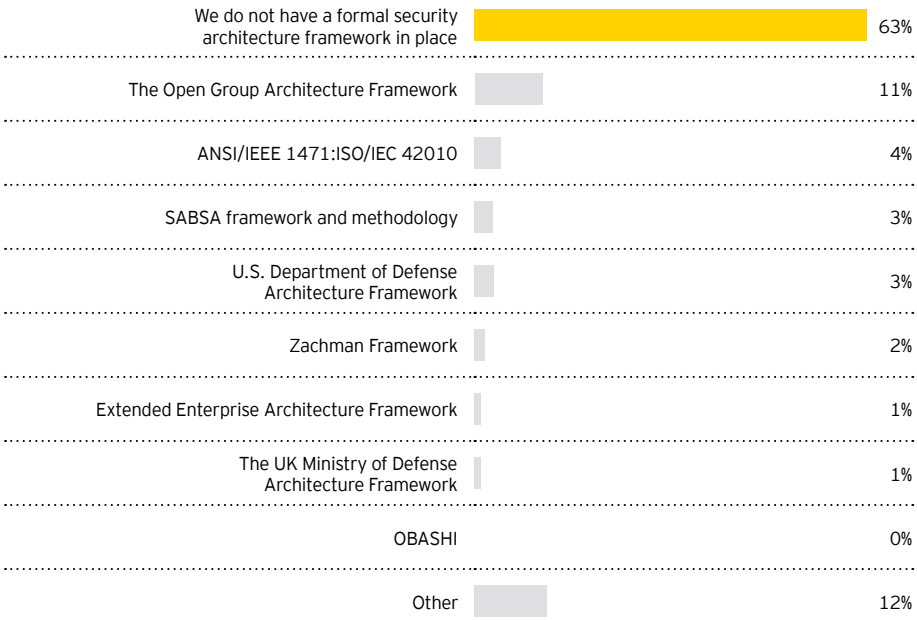
56%

of respondents only conduct between 1 and 10 attack and penetration tests annually

19%

of respondents don't conduct any attack and penetration tests at all

What formal security architecture frameworks are used (or are you planning to use) within your organization?



"Organizations need to constantly refresh their security posture to address rapidly evolving needs."

Jenny Chan
IT Risk and Assurance Services
Asia-Pacific Leader, Ernst & Young

In responding to short-term information security needs, organizations seem increasingly inclined to bolt on or stack work-around solutions. This results in a patchwork of non-integrated, complex and frequently fragile defenses, creating significant gaps in security. The work-around solution approach isn't easy to understand, use or update. Nearly a third of organizations rate their architecture as the threat or vulnerability that has increased the most over the last 12 months, largely because controls are outdated and can't easily be fixed or replaced.

Interesting fact

Sectors that have the most exposure are the ones most likely to do the most attack and penetration testing. This is especially true of banking and capital markets.

Interestingly, however, the insurance and telecommunications industries did disproportionately more testing compared to their respective exposures.

2010

30%

of respondents say they are currently using or planned to use cloud computing services

2011

44%

of respondents say they are currently using or planned to use cloud computing services

2012

59%

of respondents say they are currently using or planned to use cloud computing services

38%

of respondents say they have not take any measures to mitigate the risks of using cloud computing services

A torrent of technology

Innovation is the secret weapon that will help business keep pace with change. Businesses need to explore, implement and refine new technologies to continue growing and evolving, adapting to change particularly as threats evolve and risks grow. But the very technologies that help propel a business forward are the same ones that create new risks. New technologies open up tremendous opportunities for organizations, but the information security function needs to pay particular attention to, and manage, the associated risks.

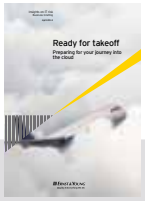
Up in the cloud

Cloud computing continues to be one of the main drivers of business model innovation and IT service delivery.

Cloud computing can enable many organizations to do much more with IT by becoming more strategy-focused and less operations-focused. Cloud-based services are nimble and adaptive, increasing the capability to read and react to changing marketplace conditions by responding to customer needs and competitors' actions.

For these reasons, cloud computing continues to be one of the main drivers of business model innovation and IT service delivery. In 2010, only 30% of organizations indicated they were currently using or planned to use cloud computing services. In 2011, that number rose to 44%. Today, 59% of organizations are in, or are headed to, the cloud. This number doesn't include the number of organizations that may be unaware of the extent of their own involvement.

Although a majority of respondents indicate they are using or will use the cloud in the next 12 months, 38% have not taken any measures to mitigate the risks. This number is down from more than 50% in 2011 as organizations recognize the risks, but a significant number of organizations remain vulnerable. The most frequently taken measures include stronger oversight on the contract management process for cloud service providers (28%) and the use of encryption techniques (28%).

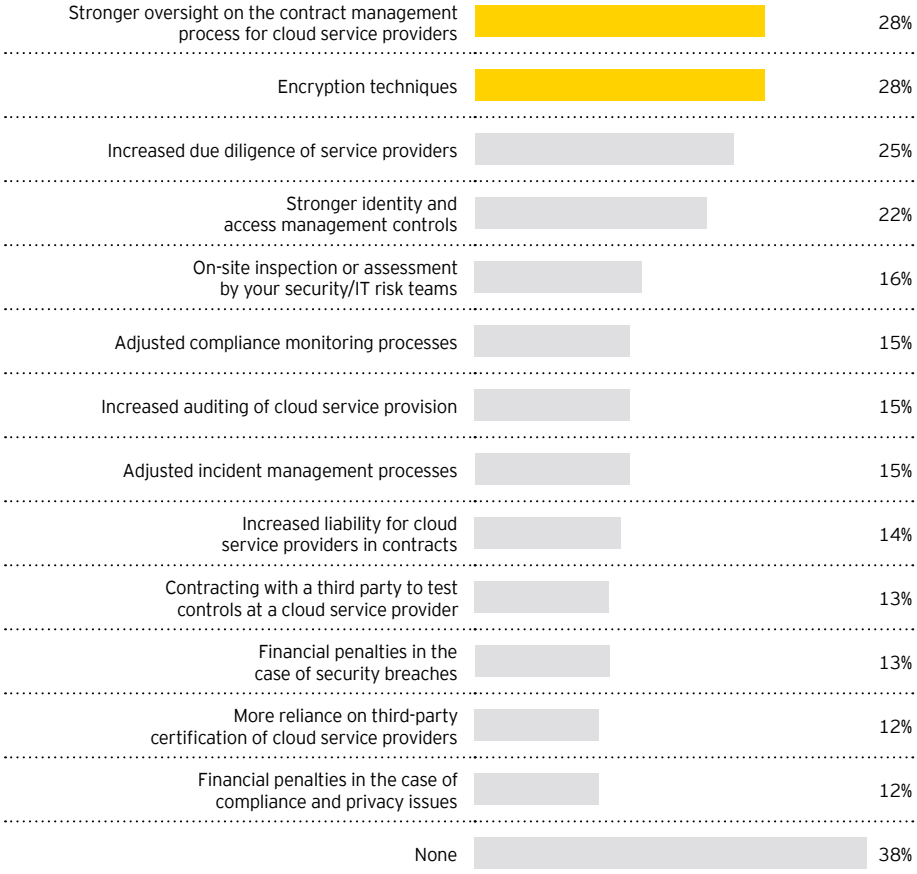


Interesting fact

More than a quarter of respondents who indicate that they do not use cloud and/or use cloud services and have no plans to do so in the next year say they rely on external assessment to gauge the effectiveness of their information security function.

Interested in learning more? Please see our publication ***Ready for takeoff: preparing for your journey into the cloud*** available at www.ey.com/informationsecurity.

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



Emerging technologies named top 10 risk for global organizations

In a recent Ernst & Young survey of 700 leading organizations, emerging technologies risk was identified as number 5 in a list of top 10 risks to be faced by businesses in the coming years.

Looking at the drivers of risk, survey respondents most frequently pointed to difficulties in developing an innovation culture. A similar number also identified the inherent uncertainty that accompanies untested technologies.

A majority of organizations surveyed indicated that they were actively managing this risk.

By far the most frequently reported mitigation strategy was to develop an organization-specific "innovation culture" to monitor new technologies and review products, services and internal processes continuously.

For more details relating to emerging technologies risk, please read our report, ***Turn risks and opportunities into results***, available at www.ey.com/top10challenges.

Social media in business

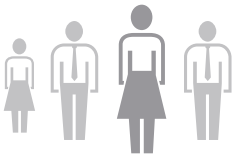
Social media can quickly build an organization's brand, and just as quickly crush it.

Once taboo within the four walls of many organizations, social media is now considered a key component of product development, feedback and customer interaction and engagement. Social media has reinvented the relationship among organizations, customers, employees, suppliers and regulators. And it has shortened processes that used to take days or weeks down to just a few hours or minutes.

But in addition to the many opportunities that social media generates, there are also many new challenges. In a 24/7, anytime, anywhere world, social media – and everyone who has internet access – can quickly build an organization's brand, and just as quickly crush it. Challenges include data security, privacy concerns, regulatory and compliance requirements, issues over employees' use of work time and business tools to engage in social media.

As noted in the chart opposite, our survey shows that 38% of organizations do not have a coordinated approach to address social media usage within or by their organization. The result is an increase in overall risk and limited capability to fully exploit social media channels in the future.

How does your organization address social media?

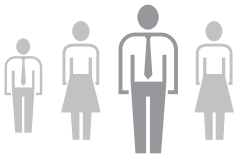


43%

We have a coordinated approach led by a department other than the information security department

38%

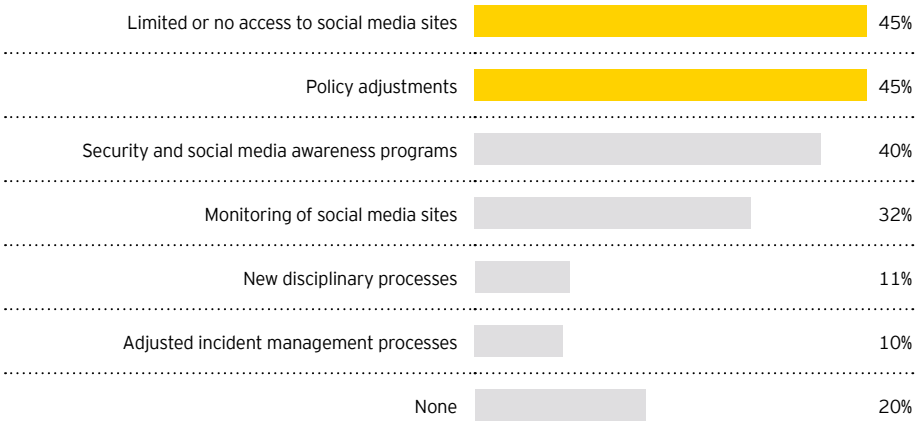
We do not have a coordinated approach to address social media



19%

We have a coordinated approach led by the information security department

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



For those organizations that do have a formal approach for using social media, the chart above shows that the most frequently implemented risk mitigation measures include: limited or no access to social media sites (45%), policy adjustments (45%) and awareness programs (40%).

Interesting fact

Almost universally, most respondents say policy adjustments are their preferred way of mitigating concerns around social media, regardless of how they measure the effectiveness of their information security function.

However, most of the respondents who indicate that they perform no assessment of their information security function's effectiveness, also indicate that to mitigate social media-related concerns, they simply prohibit or limit employees' access to social media sites.

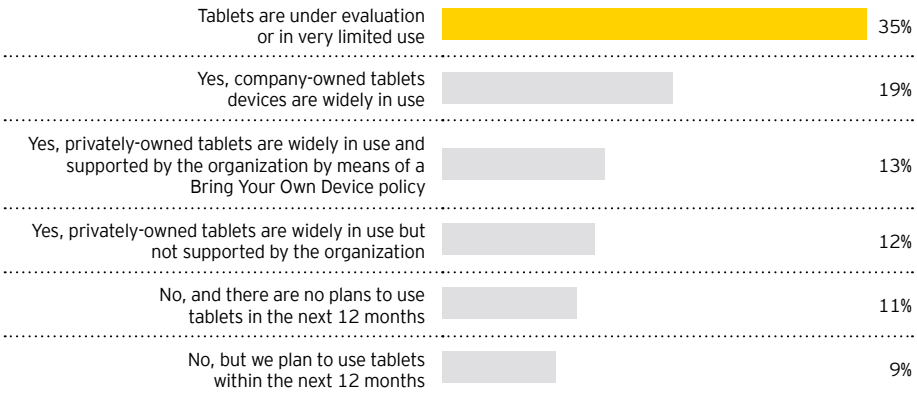
Interested in learning more? Please see our publication, ***Protecting and strengthening your brand***, related to social media available at www.ey.com/informationsecurity.

Making the most of mobile

As the mobility of today's workforce continues to grow, the phrase "out of the office" becomes less relevant.

According to a recent Cisco forecast, by 2016 there will be 10 billion internet-enabled mobile devices — nearly 1.5 for every man, woman and child on the planet. Once meant solely for telephone calls, mobile devices today are a vital communications tool and knowledge source for both business and personal activities. They enable connectivity to the internet and cloud on a 24/7 basis.

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

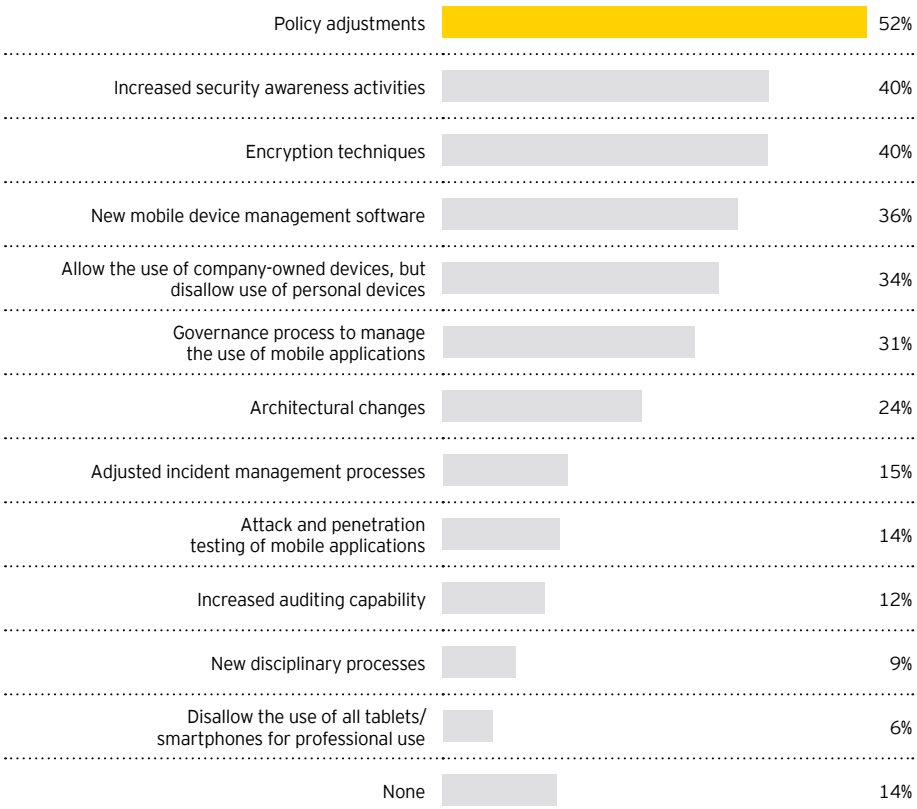


Technology advancement and the associated business benefits have vastly increased adoption rates of mobile technology. According to our survey, and illustrated in the chart above, tablet computer use for business has more than doubled since last year. From 20% in 2011, 44% of organizations now allow the use of company or privately-owned tablets within their organization — 19% indicate that company-owned tablets are widely in use; 13% support the use of privately-owned tablets through a "bring your own device" policy; and 12% allow the private use of tablets, but do not support them.

As the mobility of today's workforce continues to grow, the phrase "out of the office" becomes less relevant. And the dramatic increase in the flow of information in and out of the organization becomes more difficult to control.

As the chart on the next page highlights, 52% of respondents have implemented policy adjustments; 40% have invested in awareness programs. But organizations recognize the need to do more. They are beginning to educate themselves about the capabilities and design of the mobile device security software products that are available in the market; however, the adoption of security techniques and software in the fast-moving mobile computing market is still low. For instance, encryption techniques are used by fewer than half (40%) of the organizations.

Which of the following controls have you implemented to mitigate the new or increased risks related to the use of mobile computing including tablets and smartphones?



Mobile technologies: opportunities vs. threats

Opportunities:

- Increased productivity
- Choice of technologies
- Reduced capital expenses
- Promotes a more creative environment
- Keep employees happy and motivated

Threats:

- Theft/loss/data leakage
- Malware infection
- Unauthorized access
- Legal considerations
- Privacy concerns
- Increase in administrative overheads
- Work/play balance
- Enterprise ready/system integration

BYOD — bring your own device

As sales of mobile and smartphones outpace those for PCs, and organizations race to figure out how to configure their response to help their employees blend their work devices with their personal devices, they must consider in detail the data and information security issues.

Employees are buying phones and data plans anyway. Supporting device enablement in the workplace helps not only to lower employee costs, but also removes some of the overhead formerly associated with massive company-sponsored mobile phone purchases. This integration of personal devices with company access can help lower collective costs, and increase employee productivity, morale and creativity.

However, with opportunity also comes risk. Increasing BYOD activities mean that employees are able to upgrade their tablet or smartphone themselves — without the involvement of IT. This can impact both the functionality and security of any corporate or otherwise authorized apps that may be installed on the device. This is why mobile device management becomes so critically important. Organizations should consider the following activities when supporting BYOD.

1. **Decide who actually "owns" the device.** Once decided, an organization can then better set policies around its limits. For example, the organization could install an app that allows it to turn off cameras and applications, or block social media sites through which data can leak. This allows the employees to choose whether they want the organization to help pay for the device and its use in exchange for potential loss in freedom, including limits that protect the organization's data security.
2. **Secure the corporate network.** To prevent data loss caused by authorized access by unsupported devices, consider having a parallel "guest" network that is separate from your main network. This allows employees to use their personal device to get access to the web directly, perhaps even through a work-only email account. Also, consider using third-party services or their own coding to create "sandboxes" in those devices where company data and company-issued applications reside and are walled off from interaction with personal data, applications or online services.
3. **Maintain basic data security.** Organizations need to make sure that the data stored on the device is protected from any hacking, outsider access and from viruses.

Data spills

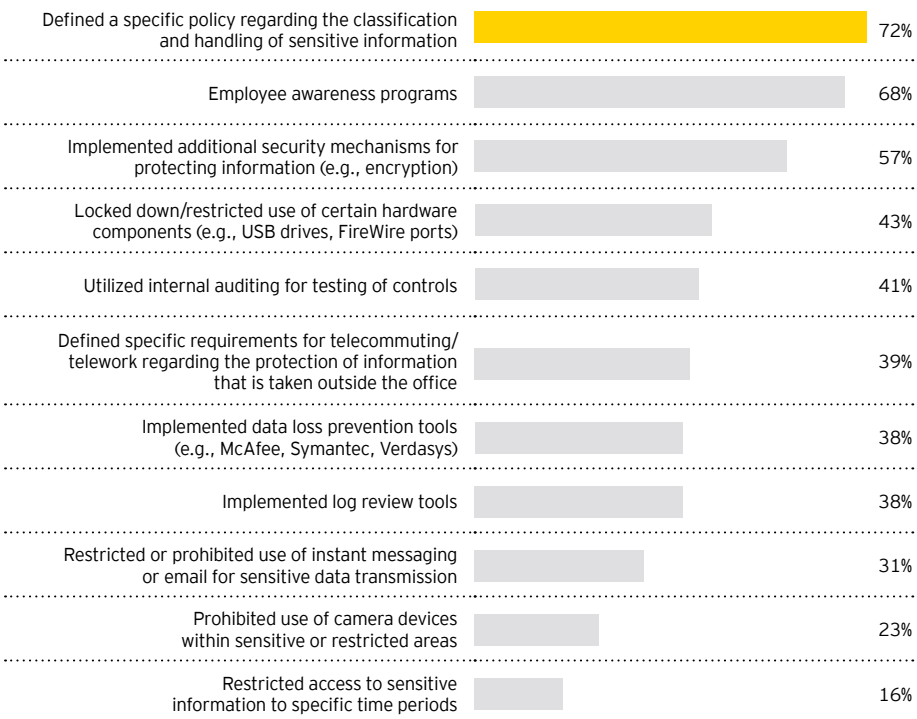
Increasingly sophisticated malware is providing a conduit for sensitive information to be released unknowingly outside the organization.

The global digitization of products, services and processes have a profound impact on organizations. The availability of huge amounts of data creates fantastic opportunities to extract insight and value. Organizations that master the discipline of big data management can reap significant rewards and separate themselves from their competitors.

However, for all the benefits, organizations also need to be aware of the challenges. Over the last five years, organizations have experienced a rise in the volume of intentional and unintentional data leakage. Increasingly, sophisticated malware is providing a conduit for sensitive information to be released unknowingly outside the organization.

As the chart below demonstrates, this year's survey suggests that most organizations have defined a policy regarding information classification (72%). As well, many organizations (68%) have executed awareness programs. The adoption of DLP (data loss prevention) technology, however, remains relatively low (38%).

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



"Organizations need to implement flexible, adaptable defences that remain resilient, even when data breaches occur – and they will occur."

Haruyoshi Yokokawa
IT Risk and Assurance Services Japan Leader, Ernst & Young

Looming gaps

Although we've identified some of the current gaps, there are still more on the horizon in the form of government intervention and new regulatory pressures.

Businesses may have been looking — more or less effectively — at the risk landscape, and evaluating threat intelligence, but they are not the only ones to be concerned. Governments and regulators have also observed the increasing risks to information security. And they are beginning to do something about it. If organizations don't take action of their own, the combined consequence of current issues (described above) and future issues (described below) will only widen the gap.

Critical infrastructure providers

Governments are likely to start producing directives — backed up by regulators — to any organization it considers economically critical, to ensure it does not fall victim to an information security threat.

Although individual businesses worry about their own performance, governments want reassurance that organizations providing key services that support the continued well-being of society can continue to operate with the minimum of disruption, whatever the circumstances.

Energy companies, telecoms, water suppliers, food producers and distributors, healthcare and financial services companies will all be expected to implement robust measures to safeguard against an information security incident that could interrupt or damage operations.

Interesting fact

In response to gridlock in the US Congress over the Cybersecurity Act of 2012, Senator John D. Rockefeller IV is challenging 500 of the US' largest companies to play a leading role in reforming information security laws.

Lobbying by the US Chamber of Commerce and other anti-security parties scuttled the approval of legislation that both the Commanding General of Cyber Command and the Chairman of the Joint Chiefs of Staff both felt were absolutely vital given the severity of the cyber threat America faced.

Through a series of questions in a letter to Exxon Mobil, Wal-Mart Stores, General Electric, AT&T, Apple, Citigroup, UnitedHealth Group and others, Senator Rockefeller asked these corporate leaders to differentiate themselves by working together to develop action-oriented solutions to combat the increasing information security threats the US faces.

With the Cybersecurity Act of 2012, Senator Rockefeller and other supporters seek to protect critical infrastructure such as power plants, pipelines, utilities, hospitals, transportation networks and telecommunications that Americans define as essential for their everyday lives.

Interesting fact

Many organizations are still having difficulty finding security breaches and properly logging them to meet required regulatory disclosures.

When large data breaches or outages are made public, they receive extensive media coverage, demonstrating that breaches are of societal importance. But ENISA, the European Union's cyber security agency, warned in a recent report[3] that even though reliable internet and electronic communications are now central to the economy, many incidents remain undetected or unreported.

"Cyber incidents are most commonly kept secret when discovered, leaving customers and policy-makers in the dark about frequency, impact and root causes," say the report's authors.

Their report identifies gaps in the regulatory framework around incident reporting, and calls for an improvement in sharing across the EU. There is "still little exchange of information between national authorities" about lessons learned and leading practices, despite the cross-border nature of the threat.

[3] Dr. Marnix Dekker, Christoffer Karsberg, Barbara Daskala,"Cyber Incident Reporting in the EU: An overview of security articles in EU legislation," European Network and Information Security Agency, August 2012.

Governments don't just have the protection of its citizens to consider. It also has its reputation as an effective government to bear in mind, and the protection of GDP.

Beyond the critical infrastructure organizations, other top 100 or top 500 businesses of all industries are coming under scrutiny. Economic growth is high on government agendas. Organizations that do the most to support that growth, and drive GDP through productivity and employment, will also need to deliver highly effective information security programs.

Governments are likely to start producing directives — backed by regulators — to any organization it considers economically critical, to ensure it does not fall victim to an information security threat. These directives will likely require businesses to share their knowledge of threats and the measures they have implemented to mitigate against or manage them.

Ideally, businesses would come together of their own volition to share experiences and establish common frameworks and solutions. It has worked for other issues and it may be the best choice organizations have to stem the flow of impending regulation.

A fundamental transformation

Organizations are working hard to keep up with the pace of technology, and the increasing number of information security threats, with varying levels of success. Those that can minimize the gap between what their information security functions are doing now and what they need to do will secure competitive advantage.

Organizations need to take four key steps to fundamentally shift how their information security functions operate:

1. **Link the information security strategy to the business strategy**, and the overall desired results for the business.
2. **Start with a blank sheet when considering new technologies and redesigning the architecture, to better define what needs to be done.** This presents an opportunity to break down barriers and remove existing biases that may hamper fundamental change.
3. **Execute the transformation** by creating an environment that will enable the organization to successfully and sustainably change the way information security is delivered.
4. **When considering new technologies, conduct a deep dive into the opportunities and the risks they present.** Social media, big data, cloud and mobile are here to stay, but organizations must prepare for their use.

1

Linking to the business strategy

As we have already seen from our findings in this year's survey, it is vital that organizations align their information security strategy with their business strategy and objectives. But would that vary depending on the organization's business objectives? What does the information security strategy need to do? What actions and tactics need to be on the organization's information security agenda?

In today's economic environment, organizations are typically focusing their efforts on achieving one or more of the following results: growth, innovation, optimization and protection. As organizations take steps to deliver these results, information security has a key role to play.

Growth

Organizations are seeking to expand their businesses into new markets, and attract new customers with new products, all with the aim of generating **revenue**. Effective information security can protect the whole business, safeguard revenue and free up resources to increase revenue opportunities.

Innovation

Organizations are using new technology to interact directly with customers in new ways. The data that is generated needs to be secure, with privacy a critical issue. In the light of today's threats, effective information security will enable an organization to **demonstrate leadership** in the matter of keeping their customers, and their organizations, safe.

Optimization

Information security structures and methods cost money, but businesses are not always spending the money they have wisely. Organizations can **reduce costs** across the business with well-structured and well-managed information security.

Protection

Information security needs good governance and transparency to provide stakeholders with **confidence**. Strong and effective monitoring and testing need to be a key component throughout the information security framework.

It is also important to develop the strategy and framework, and identifying the activities that need to be done.

Redesigning the architecture and demonstrating how information security can deliver business results

2

The best place to start is with a blank sheet so that in the initial stages the overall design is free of bias, legacy issues and other distorting factors.

Instead of looking at the existing landscape and how they can rework it, information security functions should undertake a fundamental redesign. They will need to allow for innovation and the need to constantly leverage new and emerging technologies, to help organizations achieve the results that promote protection and progress. When the results that information security should be delivering ("what" information security can do) are defined, the next step is how to get there.

Identify the real risks

As a starting point, organizations need to develop a brand new information security strategy. This strategy should start with the inclusion of technologies and issues such as cloud, social media, big data, mobile computing, globalization and borderless, rather than simply adding these topics as "bolt ons" to an existing strategy. The focus should also be on identifying the current risks (the "real risks"), which will be different from what the organization has faced in the past. This identification process is not a simple carryforward of the known risks from previous years; risk identification today requires a fresh perspective starting with a recognition of what is most important today.

Organizations should begin with looking at their risk appetite and how that translates to information risks. There should be a clear picture of what the most important data, applications and other IT assets are and where they reside, which may not be easy to answer in the case of cloud computing. The next step is to assess the threat landscape and determine the points of exposure.

2

Protect what matters most

With the real risks in mind, the next step is to develop an enterprisewide information security framework. Historically, frameworks were often static, but in today's environment they need flexibility: organizations need to be able to adapt, change and respond rapidly and effectively. An information security framework should be focused on the fundamentals and the emerging threats. It should also assume that breaches will occur and therefore planning and protecting is just as important as detecting and responding (two components that are easily overlooked).

The framework should cover information security governance (including who is responsible for what), the link between the business drivers and the information security measures, the information security monitoring (the dashboards, the compliance processes, the key control indicators) and how to respond when incidents are detected.

Embed in the business

Information security is everyone's responsibility and not just a task for management or the information security department. Therefore, any information security framework needs to be embedded in the business. All employees, functions, business projects and related elements have a role to play. However, embedding information security in the business is not an easy task. A number of fundamental decisions have to be made, such as:

- What needs to be done in the day-to-day business and what should be the responsibility of an information security function?
- What should be done manually and what should or can be incorporated via technology?
- What should be done in-house and what should or can be outsourced?

Sustain your security program

One of the most critical questions of risk management in general is: how can we make sure that our risk management framework is continuously up and running as intended? The same applies to an information security framework that is embedded throughout the organization. Organizations can have a presence in multiple countries, have large numbers of employees and manage huge number of IT assets. How can they make sure that all information security measures are effective, day in, day out?

As a result, "sustain your information security program" is a key component of the fundamental shift. Your compliance measures, self-assessments, continuous learning and improvement measures, and how you follow up on incidents, will keep your information security framework effective. In doing so, it will allow the organization to answer questions concerning whether the organization is continuously applying the information security measures as designed. And more importantly, it will solidify whether the framework is up-to-date by determining which emerging risks could trigger changes in the information security framework and the response required while the issues are small.

What organizations need to do to deliver information security that supports the business

Identify the real risks:

- Develop a security strategy focused on business drivers and protecting high-value data
- Define the organization's overall risk appetite and how information risk fits
- Identify the most important information and applications, where they reside and who has/needs access
- Assess the threat landscape and develop predictive models highlighting your real exposures

Protect what matters most:

- Assume breaches will occur — improve processes that plan, protect, detect and respond
- Balance fundamentals with emerging threat management
- Establish and rationalize access control models for applications and information

Sustain your security program:

- Get governance right — make security a board level priority
- Allow good security to drive compliance, not vice versa
- Measure leading indicators to catch problems while they are still small
- Accept manageable risks that improve performance

Embed in the business:

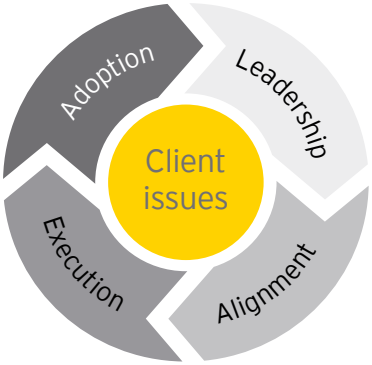
- Make security everyone's responsibility
- Align all aspects of security (information, privacy, physical and business continuity) with the business
- Spend wisely in controls and technology — invest more in people and processes
- Selectively consider outsourcing operational security program areas

3

Executing the transformation successfully and sustainably

Fundamental transformation isn't just about implementing a program and walking away. To make the changes stick, organizations need to:

- Make leaders accountable for delivering results and visibility throughout the life of the program.
- Align the entire organization in the transformation approach – from planning and delivery of the program to the sustained adoption of the performance objectives.
- Continually predict, monitor and manage risk throughout the execution of the program.
- Fully adopt new solutions before closing a program so that the old ways don't creep back in.



Leadership

- Involve leaders and other key decision-makers in defining future state
- Establish benefits-realization process, accountabilities and dashboards
- Link external analysis and alerts to the program approach
- Create a multilayered case for change

Alignment

- Define and involve the entire organization in understanding and owning the future state
- Drive results early and often to accelerate the move to future state
- Perform active listening to identify issues and implement continuous improvement
- Provide dedicated specialist skills to support various stakeholders across the enterprise

Execution

- Provide more extensive support in the execution phases to enable successful delivery
- Implement careful design of technology and process foundations to bring stability and adaptability
- Use data to model program delivery risks and continually improve approaches and plans

Adoption

- Build long-term relationships with stakeholders to sustainably adopt program solutions
- Leverage social media to facilitate interaction and increase the level of influence of the program early and often
- Identify adoption techniques
- Communicate wins and be transparent with challenges and fixes

A deep dive into the new technologies

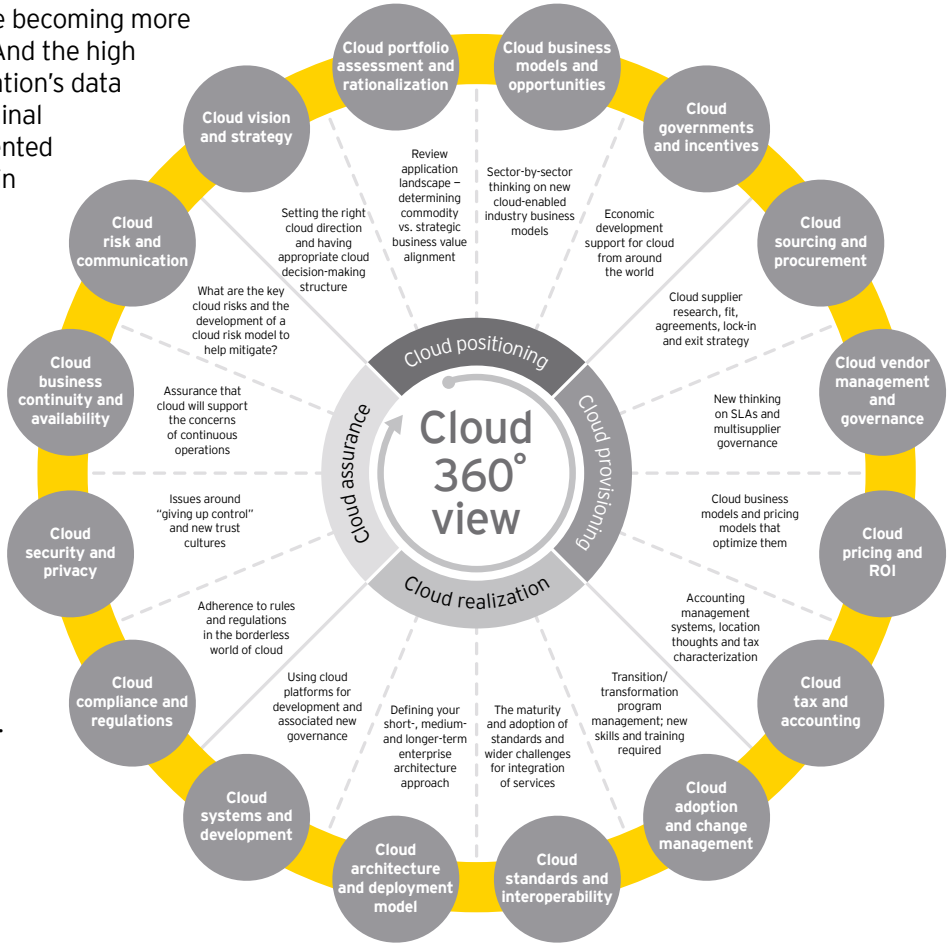
4

Despite their risks, new technologies are here to stay. Organizations need to use them to their advantage to extend their reach and energize profitable growth. Any information security framework needs to constantly assess the role of new technologies and how to maximize their potential for the organization while keeping them safe.

Virtualization, mobilization and cloud technology have increased the threat of serious attacks by increasing the number of entry points to an organization's business. Hacktivism and state-sponsored espionage are becoming more sophisticated and persistent. And the high rewards for selling an organization's data are feeding the growth of criminal organizations at an unprecedented rate. These attacks can result in significant financial loss and brand damage.

What is surprising, considering the truly sinister nature of these crimes, is that these attacks often occur without the business being aware of it.

Short-term, incremental changes and temporary solutions are not enough. Organizations need to take a 360° look at each of the new technologies to identify and offset the associated risks.



A 360° view of cloud computing

Across all aspects of the cloud, assurance is a core consideration, and in our view there are four key components to delivering cloud assurance:

1. **Cloud risk and communication:** identifying the key cloud risks and the development of a cloud risk model to help mitigate
2. **Cloud business continuity and availability:** gaining assurance that the cloud will support the concerns of continuous operations
3. **Cloud security and privacy:** addressing issues around "giving up control" and a new trust culture
4. **Cloud compliance and regulations:** ensuring adherence to rules and regulations in the borderless world of cloud

For more details relating to cloud, please read our report: ***Cloud computing issues and impacts***, available at www.ey.com/informationsecurity.

Make the shift, close the gap

From 2006 until today, our survey findings suggest that the disparity between accelerating threats and organizations' responses is not narrowing. In fact, it is growing at an exponential rate, expanding the information security gap from a sliver to a chasm.

Effective information security transformation does not require complex technology solutions. It requires leadership and the commitment, capacity and willingness to act. Not 12, 24 or 36 months from now, but today. Any delay and many organizations may fall too far behind to catch up.

Ernst & Young believes that by following the four key steps discussed on the previous pages:

1. Link the information security strategy to the business strategy
2. Redesign the architecture
3. Execute the transformation successfully and sustainably
4. Deep dive into the opportunities and risks of new technology

organizations can fundamentally shift how their information security functions operate and be better able to close the ever-widening IT risk gap.

What some leading organizations are doing

- Moving from protecting the security perimeter to protecting their data with the understanding that some attackers will inevitably penetrate perimeter defenses.
- Creating dynamic capabilities to manage information security so that they can react quickly in a rapidly evolving environment.
- Actively involving senior business leaders across functions in making security trade-offs.
- Creating information security strategies and processes based on a much higher degree of transparency into critical assets, attackers, security capabilities, business risks and options for defense.

Survey methodology

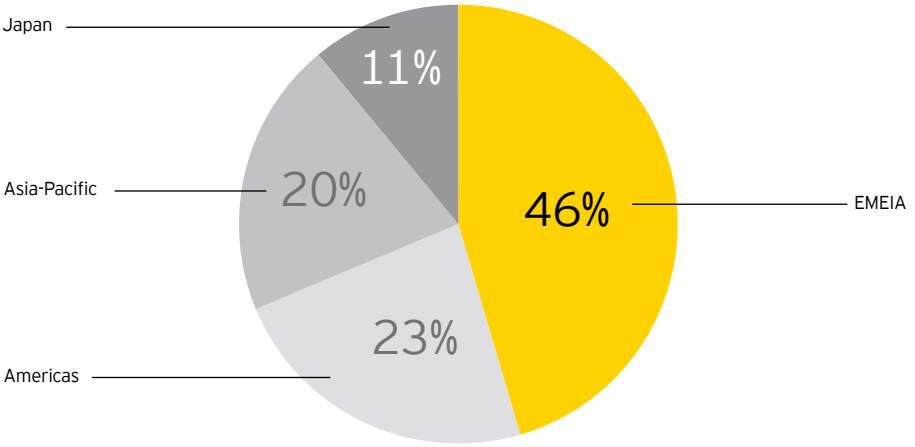
Ernst & Young's Global Information Security Survey was conducted between May 2012 and July 2012. We had 1,836 respondents across all major industries and in 64 countries participated.

For our survey, we invited CIOs, CISOs, CFOs, CEOs and other information security executives to participate. We distribute a questionnaire 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.

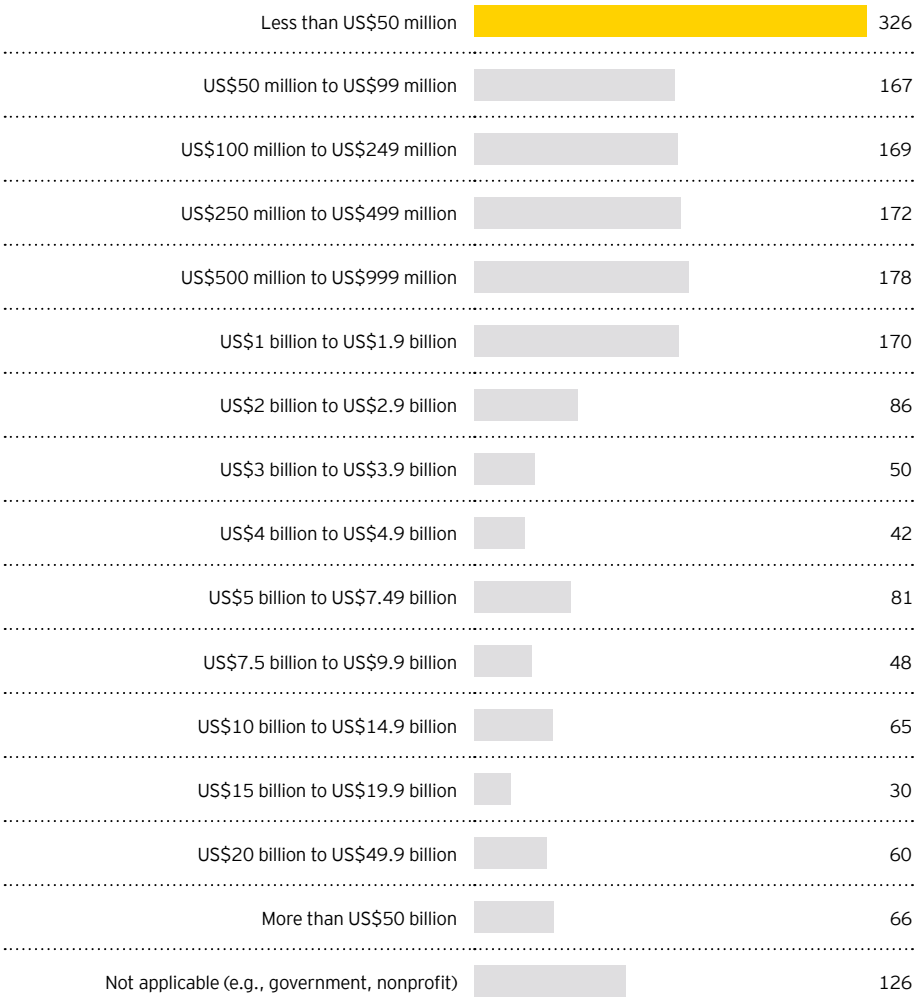
If you wish to participate in Ernst & Young's 2013 Global Information Security Survey, please contact your local Ernst & Young office, or visit www.ey.com/US/en/Home/Home-ContactUs and complete a simple request form.

Respondents by area (1,836 respondents from 64 countries)

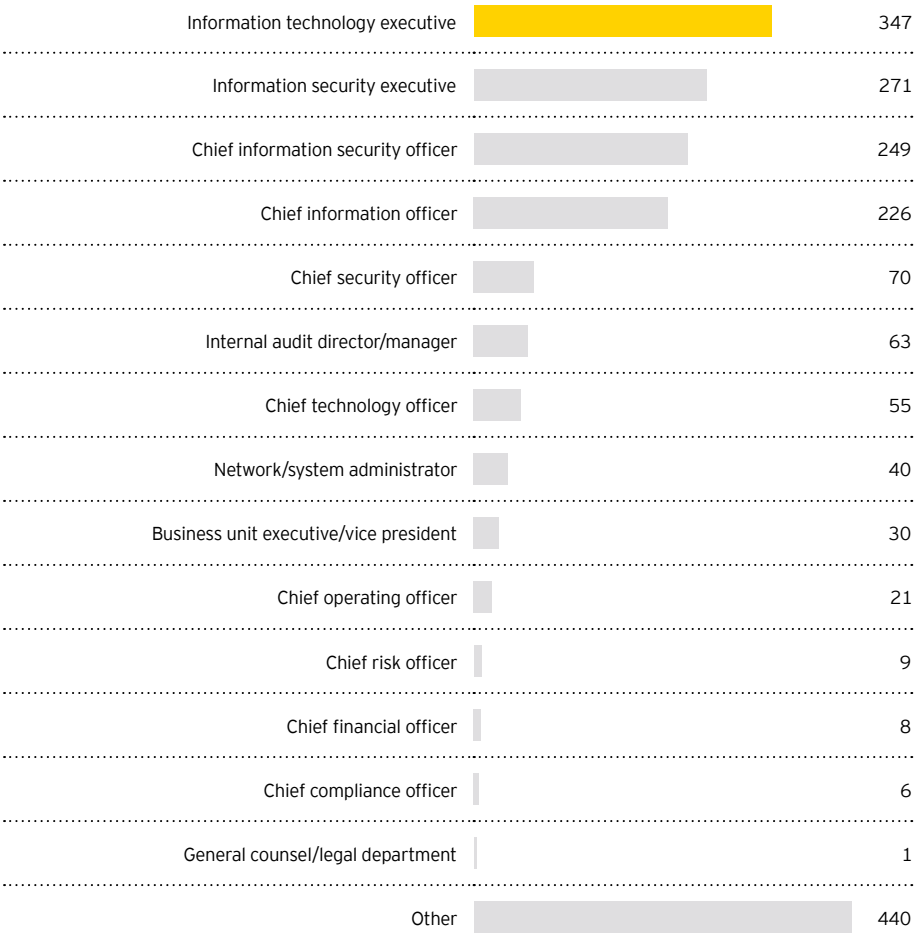


Respondents by industry (1,836 respondents from 64 countries)

Respondents by total annual company revenue



Respondents by position

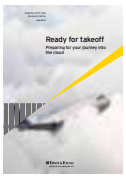


Other thought leadership resources

Ernst & Young regularly publishes thought leadership on a wide range of IT and information security topics, including our ongoing *Insights on governance, risk and compliance* series, focused on IT risk and its related challenges and opportunities. These timely perspectives are designed to help clients offer timely and valuable insights that address issues of importance for C-suite executives.

To access the reports listed below, please use the QR code provided, or visit www.ey.com/informationsecurity.

Protecting and strengthening your brand: social media governance and strategy
For many organizations, long-term success depends on the success of a number of individual critical transformation programs. Businesses – focused on responding to today's market turmoil – need to execute numerous change programs and projects in parallel, while at the same time keep the business functioning. Many organizations struggle with "doing the right things" and "doing things right." As a result, many get poor returns from their investment in projects or programs.

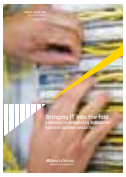


Ready for takeoff: preparing for your journey into the cloud
Many organizations are looking to cloud computing to increase the effectiveness of IT initiatives, reduce cost of in-house operations, increase operational flexibility and generate a competitive advantage. Through an effective strategy, cloud computing can enable many companies to do much more with IT by becoming strategy-focused and not operations-focused. Cloud-based services are nimble and adaptive, increasing capability to read and react to changing marketplace conditions by responding to customer needs and competitors' actions.

Privacy trends 2012
As quickly as governments are taking steps to regulate privacy, industry groups are exploring opportunities for self-regulation to limit an increase in government intervention. Ultimately, however, it is the organizations themselves that need to take action. To achieve greater accountability, many organizations will have to rethink their approach to privacy.

Mobile device security
Huge technological advances in mobile devices have extended the virtual boundaries of the enterprise, blurring the lines between home and office by providing constant access to email, enabling new mobile business applications and allowing the access to, and storing of, sensitive company data. We explore the risks related to today's most popular mobile device platforms and technologies, along with methods by which an organization may assess its exposure to and attempt to mitigate to risks.

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. This report describes the issues and impacts of all aspects of cloud computing.



Bringing IT into the fold: lessons in enhancing industrial control system security
Power and utility companies, as well as other enterprises with industrial operations such as oil and gas and many manufacturing companies, are facing increasing risk of cyber attacks as they converge their real-time operational technology environments with their enterprise IT environments.

A path to making privacy count
Is the personal information you collect from your customers safe from prying eyes? As IT departments everywhere grapple with the technology evolution and how it impacts legacy systems and new integrations alike, privacy needs to be a vital consideration. Effectively managing privacy-related risks can safeguard against costly breaches that can harm reputations and shareholder value. It can also provide opportunities to improve business performance and achieve competitive advantage.

Ernst & Young's approach to IT risk

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 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 create a multidisciplinary team bespoke to every client's specific requirement. Using consistent methodologies that have been tried and tested in the field, our team draws on Ernst & Young's global reach, our broad sector experience and deep subject-matter knowledge to help you win the battle against ever-changing IT risks.

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

Contacts

Global	Telephone	Email
Paul van Kessel	+31 88 40 71271	paul.van.kessel@nl.ey.com
Randall J Miller	+1 312 879 3536	randall.miller@ey.com

Area	Telephone	Email
Americas		
Michael L Herrinton	+1 703 747 0935	michael.herrinton@ey.com
Bernard R Wedge	+1 404 817 5120	bernard.wedge@ey.com
EMEIA		
Jonathan Blackmore	+44 20 795 11616	jblackmore@uk.ey.com
Manuel Giralt Herrero	+34 91 572 7479	manuel.giraltherrero@es.ey.com
Asia-Pacific		
Jenny S Chan	+86 21 2228 2602	jenny.s.chan@cn.ey.com
Rob Perry	+61 3 9288 8639	rob.perry@au.ey.com
Japan		
Yoshihiro Azuma	+81 3 3503 1100	azuma-yshhr@shinnihon.or.jp
Haruyoshi Yokokawa	+81 3 3503 2846	yokokawa-hrysh@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 167,000 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 25,000 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. AU1311
www.ey.com/giss2012

ED 0114.
1207-1373188 CLE