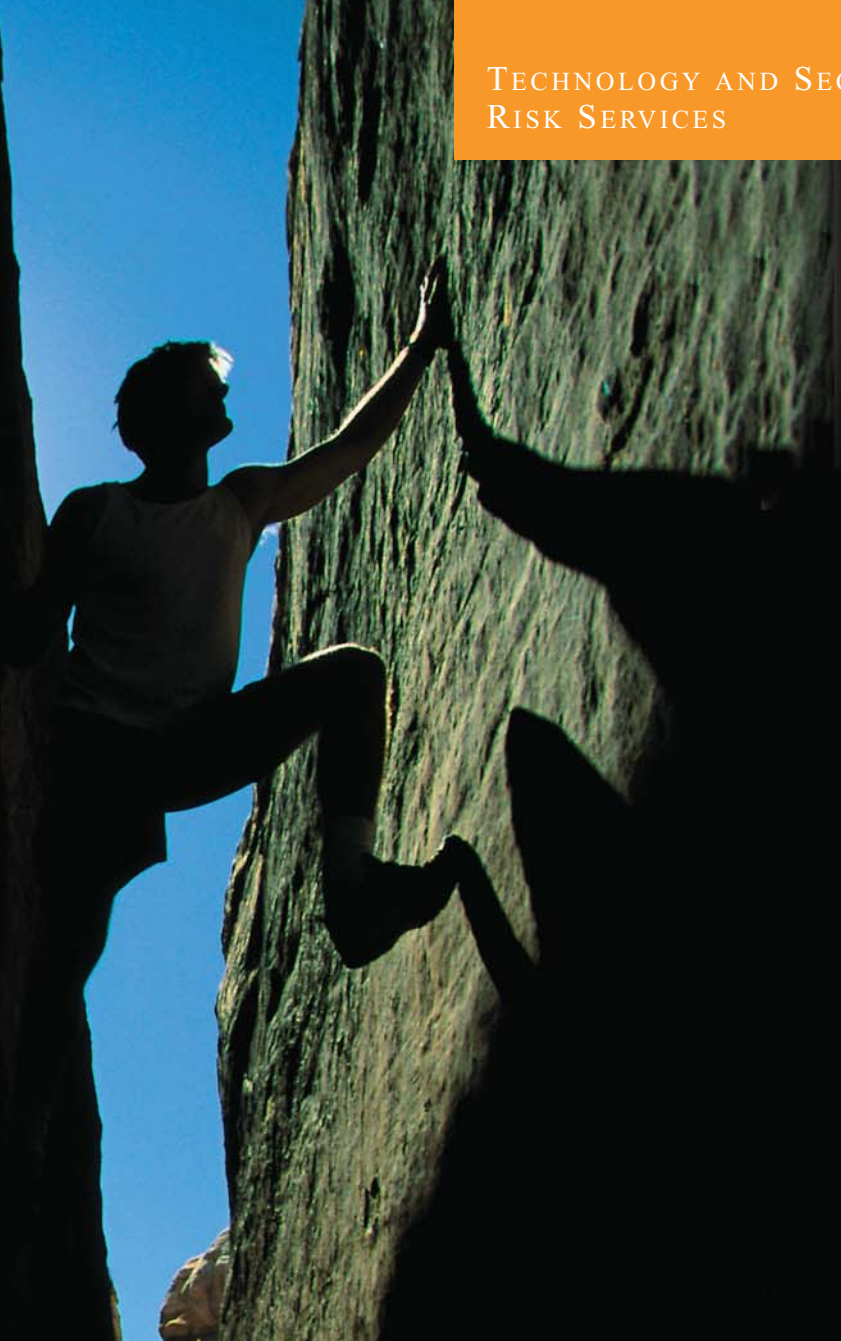


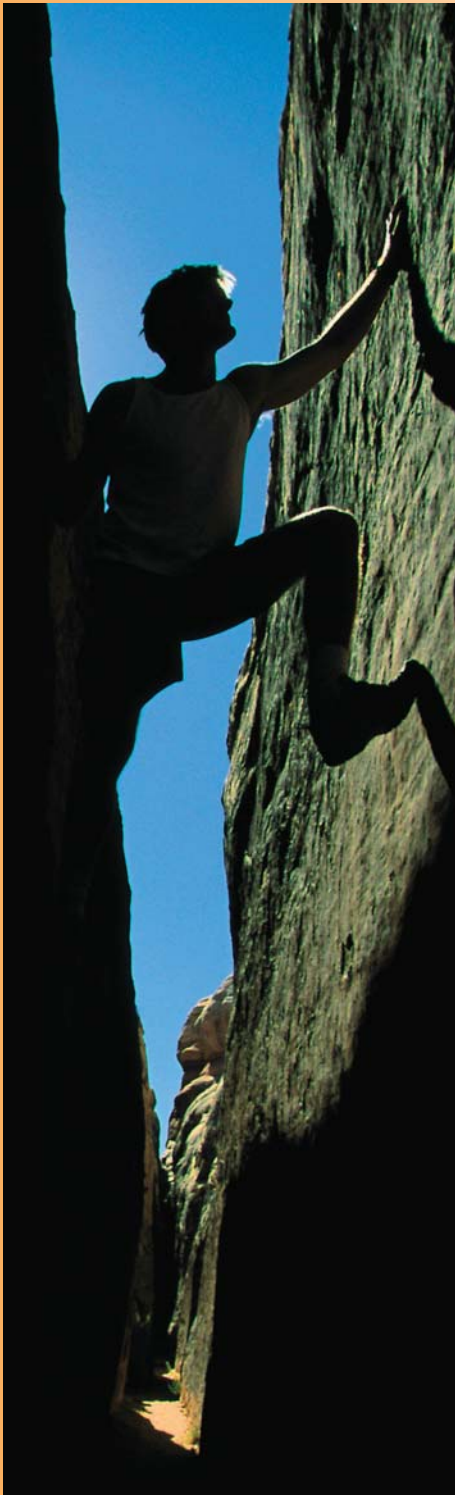
TECHNOLOGY AND SECURITY
RISK SERVICES



 **ERNST & YOUNG**
Quality In Everything We Do

Global Information Security Survey 2005

Report on the Widening Gap



**The gap continues to widen
between the growing risks
brought on by rapid changes in
the global business environment
and what information security
is doing to address those risks.**

Table of Contents

The Gap that Continues to Widen	2
Findings and Observations:	
▶ The Paradox of Compliance	4
▶ Growing Global Interdependency	8
▶ Business Demands Pushing the Adoption of Emerging Technologies	12
▶ Organizational Alignment and Delivery	15
Closing the Gap—A Call to Action	24
Our Survey Methodology	25

The Gap That Continues to Widen

This eighth edition of Ernst & Young's Global Information Security Survey was conducted across a global landscape in which organizations find themselves vulnerable to growing risks, brought on by rapid changes in the business environment and requirements to stay competitive. These changes are expected to accelerate in the coming years. Yet this year's survey indicates that information security—a critical part of organizations' ability to manage risk—is not doing nearly enough to keep up with these changes. The gap continues to widen between the growing risks and what information security is actually doing to address them. Many of our survey respondents recognize this gap. It now becomes imperative for them to take action to close it.



To bring you this report, we surveyed executives in over 1,300 organizations, in 55 countries from around the world who answered questions regarding their key drivers for information security and what actions they are taking in response to these drivers. Based on our analysis of their responses, we arrived at findings and observations that focus on four areas where the widening gap is clearly evident. What is significant about this survey is that the findings and observations are consistent for all of the organizations that participated, regardless of size or location. Consequently, we are confident that this report will be relevant to your organization.

The four areas we address are as follows:

The paradox of compliance

The sheer number of regulations and the consequences of not complying with them have brought information security into the boardroom. Yet many organizations are missing the rare investment opportunities that compliance offers to promote information security as an integral part of their business.

Growing global interdependency

With even more information flowing between companies, all organizations, whether global or not, need to consider their business partners, outsourcing arrangements, suppliers and customers. Each group needs to be confident with the others' information security. However, many organizations are not taking the required measures to obtain this assurance.

Business demands pushing the adoption of emerging technologies

Organizations are continually seeking more productive and competitive ways of working, which are driving the proliferation of rapidly developing technologies. These technologies bring with them serious threats that often are not being fully addressed in the right manner or timeframe.

Organizational alignment and delivery

Opportunities exist for information security to make significant contributions to organizations' strategic initiatives through proper organizational alignment and delivery. Yet most organizations continue to concentrate their information security activities on operational and tactical issues at the expense of addressing strategic concerns.

Understanding and acting on the findings and observations in this report is important as your organization confronts the widening gap between the growing risks and what information security is actually doing to address them. It can mean the difference between thriving and merely surviving.

We have identified, at the end of this report on page 24, actions that leading organizations are taking to close the widening gap. We encourage you to consider them as well.

The Paradox of Compliance

The sheer number of regulations and the consequences of not complying with them has brought information security into the boardroom. Compliance has surpassed worms and viruses as the primary driver of information security in 2005.

One might assume that with the attention information security is receiving due to regulatory compliance, each organization's information security posture is improving, and information security as a function is becoming more integral to the organization's strategic initiatives. Unfortunately, this is not happening. Instead, compliance is proving to be more of a distraction than a catalyst for information security becoming strategically aligned with organizations.

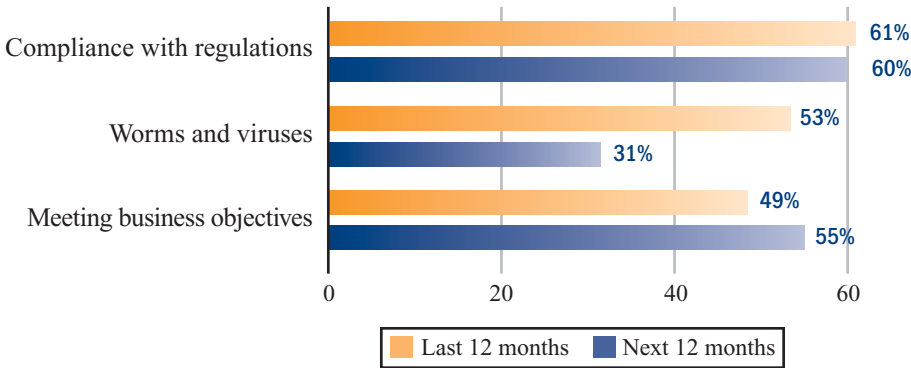
Findings and Observations

For the first time since Ernst & Young began the *Global Information Security Survey*, compliance with regulations has taken the lead as the primary driver of information security among nearly two-thirds of survey respondents, surpassing worms and viruses. This is particularly noteworthy in a year of phenomenal virus and worm activity, with blended threats increasing the speed of propagation and resulting damage, as well as an increase in criminal involvement. It is even more significant considering that a fifth

of survey respondents are not subject to heavy regulations.

Yet business, IT, and information security leaders alike are missing the rare investment opportunities that Sarbanes-Oxley, the EU's 8th Directive, and other regulatory requirements offer to promote information security as an integral part of their business. Instead, the opportunities are going largely unheeded.

The top three drivers that most significantly impacted or will significantly impact organizations' information security practices.

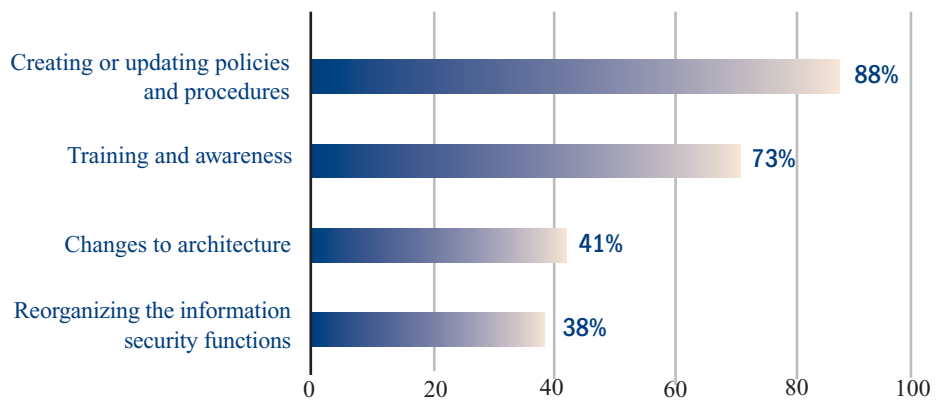


Multiple responses allowed.

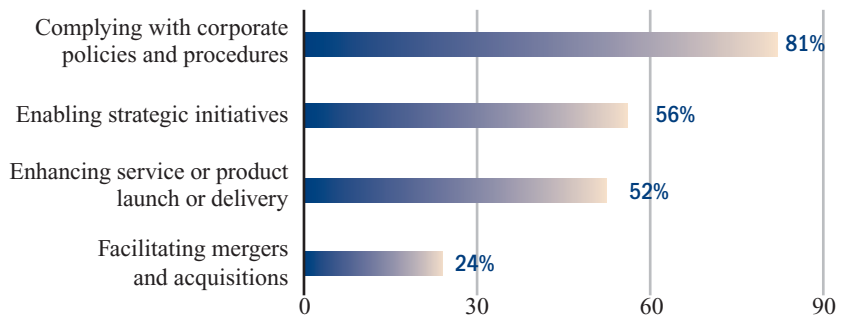
For example, nearly 90% of respondents who are implementing information security measures as a result of having to comply with internal control regulations focus on creating or updating policies and procedures. Nearly three-quarters of them conduct training and awareness. In contrast, only 41% report that they are using compliance with internal control regulations as an opportunity to reorganize their information security function or to make changes to their security architecture.

Furthermore when asked to identify important roles for the information security function, respondents reveal an imbalance in focus by rating *complying with corporate policies and procedures* at 81%, well ahead of enabling business objectives such as *strategic initiatives, product launches or delivery, and mergers and acquisitions*.

Information security measures that are being implemented by organizations as a result of having to comply with internal control regulations, such as Sarbanes-Oxley, the EU's 8th Directive or their equivalent.



Percentage of respondents who view information security as most important in supporting the following efforts.

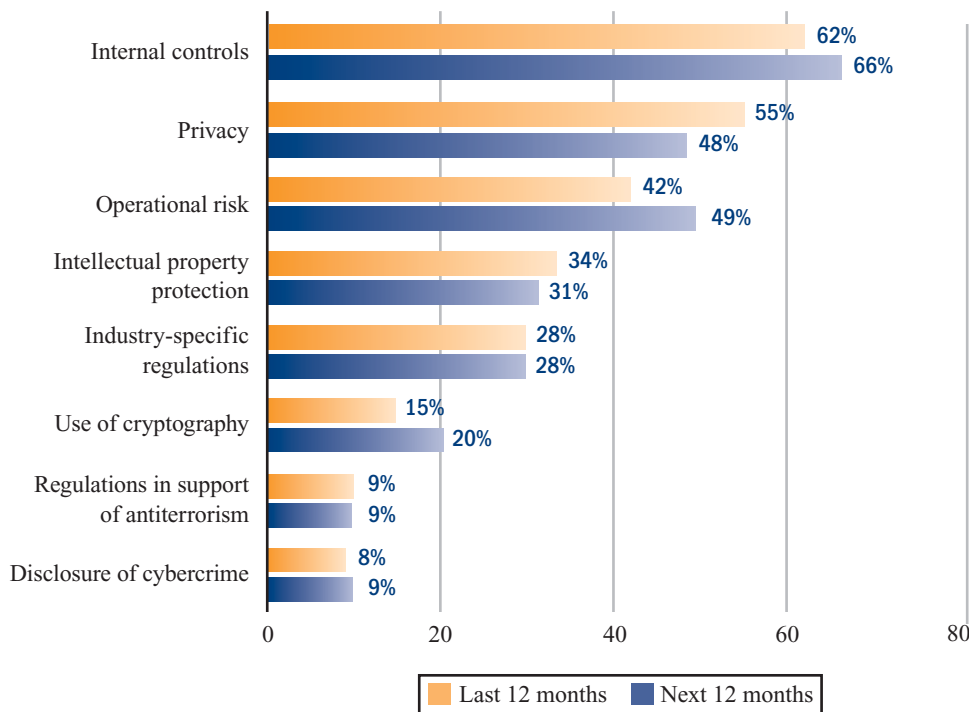


For the first time since Ernst & Young began the Global Information Security Survey, compliance with regulations has taken the lead as the primary driver of information security among nearly two-thirds of survey respondents, surpassing worms and viruses.

Regulations having the greatest impact

Internal control regulations were cited by two-thirds of respondents as the type of regulation having the greatest impact both now and in the next 12 months, followed by privacy at over 50%. But privacy demands are expected to decline over the next 12 months. Regulations on operational risks are expected to increase in impact over the next 12 months ahead of privacy, particularly in regulated industries. Industry-specific regulations are expected to remain steady in fifth place, behind intellectual property protection. Respondents expect requirements to use cryptography to increase from 15% to 20%, although regulations in support of antiterrorism and disclosure of cybercrime are expected to remain steady at just below 10%.

Top regulations or requirements that impact organizations' information security practices.



Multiple responses allowed.

Compliance with regulations will continue to be the top driver for information security in the next 12 months

With the amount of effort still needed to address Sarbanes-Oxley, Basel II, and the European 8th Directive—to name but a few—compliance with regulations is expected to maintain its position as the top driver for information security going forward. Worms and viruses as drivers are anticipated to drop from second place to fifth place in the next 12 months. In any case, we expect information security to continue functioning primarily in an operational role to address compliance, unless organizations seize the investment opportunities that compliance offers to promote information security as an integral part of their business.

Only 41% of survey respondents report that they are using compliance with internal control regulations as an opportunity to reorganize their information security function or to make changes to their security architecture.

Growing Global Interdependency

The world is getting smaller, and business is leading the way. Globalization has fulfilled its promise. It is no longer enough for organizations to consider just their own information security issues and threats. With even more information flowing between companies, all organizations, whether global or not, need to consider their business partners, outsourcing arrangements, suppliers and customers. The value to organizations created by these arrangements can quickly diminish or disappear altogether due to perceived or real security, privacy, or identity breaches. Each group needs to be confident with the others' information security.

The most mature organizations recognize that risks lie everywhere—within the organization and in the extended enterprise of business partners, suppliers, customers and other members of the distribution channel. Leading organizations recognize their dependence on third parties, over whom they have less direct control. They give a high degree of attention to vendor risk management—a process of assessing and mitigating risks that includes due diligence and regular reviews of practices and procedures supporting vendors' products and services. These organizations understand that outsourcing of key business and IT functions provides both opportunities and risks that need to be managed. They evaluate the risks and effectiveness of outsourcing projects, applying risk assessment frameworks that include both quantitative and qualitative variables and considerations.

Many organizations are not paying adequate attention to vendor risk management. One-fifth of respondents do not address the issue of vendor risk management at all, and one-third report they have only informal procedures in place to do so.

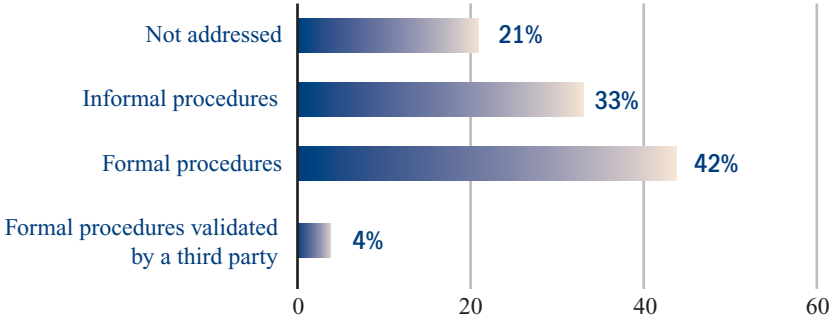
In contrast, this survey indicates that many organizations are not paying adequate attention to vendor risk management. This is particularly true for information security, where assumptions—not proven evidence from independent reviews or certification—dominate as the basis of reliance. Consequently, organizations face an increasing exposure to potentially harmful new risks and a severe reduction in the anticipated benefits of vendor and outsourcing arrangements the moment a perceived or real breach in security, privacy, or identity occurs.

Findings and Observations

Vendor risk management processes are immature and inadequate

Organizations do not demand enough from third parties to provide a viable basis for managing the risks in the relationships. One-fifth of respondents do not address the issue of vendor risk management at all, and one-third report they have only informal procedures in place to do so. In today’s fast-changing risk environment, this approach to dealing with third parties exposes organizations to significant risks that should not go unmanaged.

How organizations are addressing vendor risk management.



Almost three-quarters of respondents believe vendors and partners have the ability to support their organizations’ policies, procedures, and standards, yet only one-sixth of these organizations require independent third-party reviews of their vendors or third parties. Only one-quarter of respondents require vendors or partners to be certified. To minimize organizations’ risks, any decisions to work with third parties, particularly for co-sourcing or outsourcing arrangements, should be supported by rigorous due diligence activities prior to making a contractual commitment. A provision for review activities should also be built into the contracts, with regular and structured reviews against expectations as part of an ongoing arrangement.

Organizations themselves should consider applying recognized standards or becoming certified as a way of demonstrating to their customers a commitment to good information security.

Most common organizational requirements of vendor and business partner risk management process.

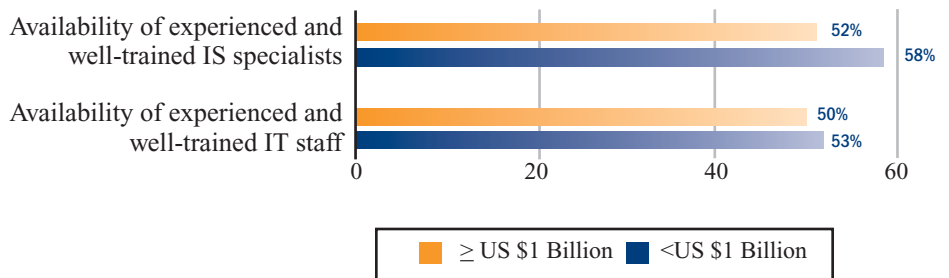


Multiple responses allowed.

Weak links are everywhere

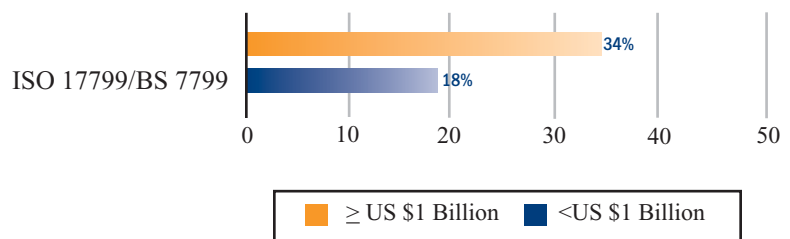
There is a widespread belief that smaller organizations should be of greater concern than larger organizations in their approach to security, because they have limited access to the resources available to larger organizations. This may be true, but responses to our survey show remarkably few differences between larger and smaller organizations in many respects. They have similar challenges with acquiring experienced and well-trained IT and information security specialists. Both larger and smaller organizations still have a way to go in adopting and becoming certified in information security standards. Smaller organizations that are hoping larger organizations will set the standard for information security should recognize that larger organizations face many of the same implementation challenges as they do.

Percentage of respondents reporting availability of experienced and well-trained IT and information security staff as their greatest challenge.



Multiple responses allowed.

Percentage of organizations that have formally adopted and/or become certified in ISO 17799/BS 7799.



Both larger and smaller organizations face similar challenges with acquiring qualified information security specialists and adopting and becoming certified in information security standards.

Business Demands Pushing the Adoption of Emerging Technologies

Organizations' need for more productive and competitive ways of working is driving the proliferation of rapidly developing technologies such as voice-over IP telephony, open source, and server virtualization. These technologies hold the potential of increasing organizations' competitive advantage. But they also bring with them serious threats that must be mitigated. Business demands and the declining cost of wireless connectivity are driving the rapid widespread adoption of mobile technology. But with these devices leaving the safety of the corporate controlled environment, the information assets and intellectual property they carry are increasingly becoming the responsibility of individuals to protect—a responsibility that many organizations have not yet fully accepted nor anticipated.

Emerging technologies are a fact of life for organizations competing in a rapidly changing business environment. The question is, how well is information security keeping up? According to our survey, some organizations do recognize the extent to which information security risks are inherent in emerging technologies. However, many others do not. Organizations that are acting on these risks are not necessarily taking adequate steps. And, although survey respondents consider emerging technologies to be a growing security concern over the next 12 months, a significant number of them have no plans to take action during that time period or beyond.

As organizations adopt emerging technologies, they need to be aware of the related risks, such as immature controls, intellectual property infringement and quality concerns. They then need to take timely action to address them.

Findings and Observations

Recognition and actions not commensurate with the risks

Half of the survey respondents recognize the significant information security concerns of emerging mobile technologies, including mobile computing, removable media, and wireless networks. This recognition no doubt reflects their widespread visibility and usage. However, among the rapidly developing technologies of voice-over IP telephony, open source, and server virtualization, the level of concern drops off significantly at 21%, 10% and 8% respectively, despite the serious threats they bring with them.

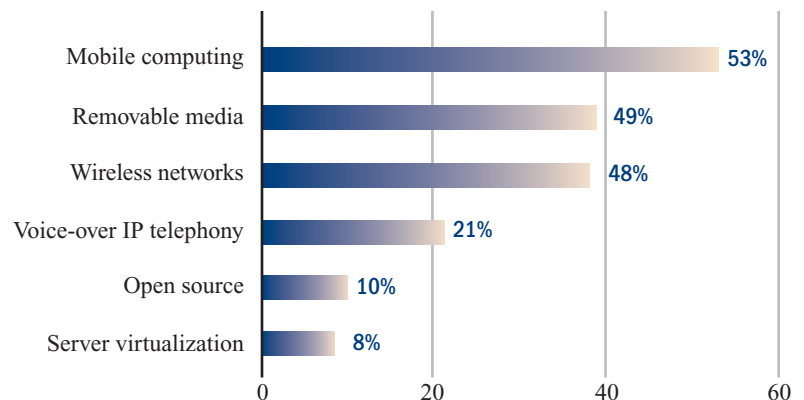
As organizations adopt emerging technologies, they need to be aware of the related risks, such as immature controls, intellectual property infringement, and quality concerns. They then need to take timely action to address them.

When it comes to mobile technology, although widely recognized as a security concern, not all organizations are taking sufficient measures to manage the risks. Such measures need to start with recognizing that information security is everyone's responsibility. From this perspective, communication about security threats and practices needs to flow both vertically and horizontally in the organization. In addition, new types of assets and distributed protective measures are required.

Currently, less than half of organizations make provision for general users of information to be trained or made aware about the impact of information security issues, and even fewer receive training on responding to security incidents.

Half of the survey respondents recognize the significant information security concerns of emerging mobile technologies. However, among other rapidly developing technologies, the level of concern drops off significantly, despite the serious threats they bring with them.

The top new technologies that organizations have identified as significant security concerns.



Although survey respondents consider emerging technologies to be a growing security concern in the next 12 months, over a quarter of them have no plans to take action during that time period or beyond.

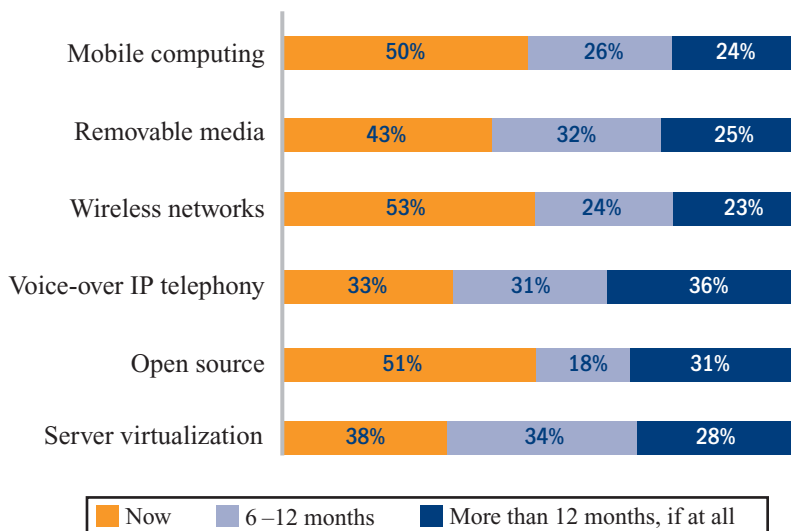
Despite rising concerns, no immediate plans in place for many organizations

Forty-two percent of survey respondents report that new technologies will become a significant driver of information security for them in the next 12 months. This is up from 34% of survey respondents who say it currently is a significant driver. While it is encouraging that close to half of them are already addressing to some degree the security concerns of many of these technologies, between a quarter and a third of survey respondents say that they have no plans in place for at least 12 months, if at all, to address the security concerns of:

- ▶ mobile computing
- ▶ removable media
- ▶ wireless networks
- ▶ voice-over IP telephony
- ▶ open source
- ▶ server virtualization

Given that business demands are driving the rapid development and adoption of these emerging technologies, the risks associated with this inaction can only continue to grow and become more serious.

When organizations plan to address emerging technology concerns.



Organizational Alignment and Delivery

With proper organizational alignment and delivery, information security can make significant contributions to the organization's strategic initiatives and overall risk management. Organizations that employ information security in this way continuously involve business, IT, and information security leaders in identifying specific areas where information security can contribute to strategic initiatives, such as mergers and acquisitions, outsourcing, and product launches. They apply recognized information security standards, leading practices and the appropriate resources.

However, we observe many organizations that are not following this example. Instead, they continue to focus information security activities on operational and tactical issues at the expense of addressing strategic concerns. They are not doing nearly enough to adapt, even though awareness about information security has risen as a critical issue among boards and executive management.

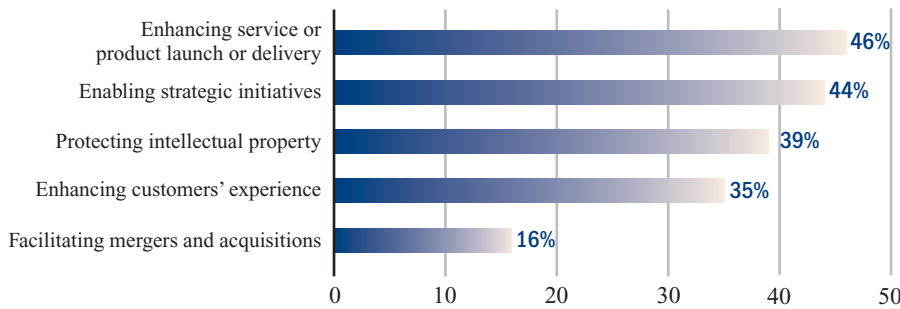
Findings and Observations

Integrating information security with risk management

Two-thirds of survey respondents report that they have an official information security function, which is good news. In many cases, this situation has been driven by the need of organizations to reinforce their internal controls and overall enterprise risk management posture. However, more than a quarter of survey respondents report that their information security function is not integrated with their organization's overall risk management process. For these organizations, information security and risk management are most likely operating in silos, where they are undertaking projects that are either redundant or focused on areas that contribute minimally to improving their organization's overall risk profile.

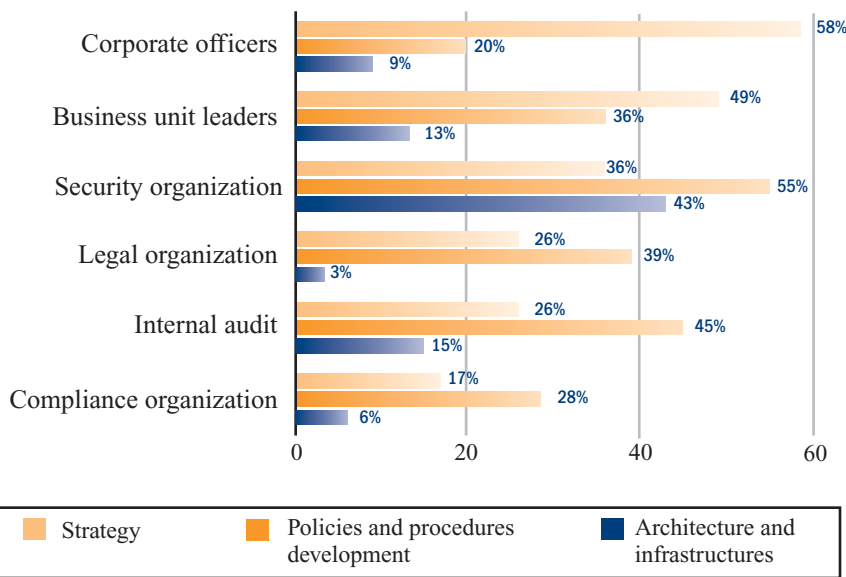
Two-thirds of survey respondents report that they have an official information security function, which is good news. However, more than a quarter of them report that their information security function is not integrated with their organization's overall risk management process.

Percentage of information security functions that are proactively involved in the following strategic efforts.



Sorted by percent "involved".

Who reviews information security activities and action plans when significant change occurs in the organization?



Multiple responses allowed.

The survey results go on to indicate that even more information security functions than reported are separate from organizations' overall risk processes. Less than a third of survey respondents meet monthly with internal audit, compliance, and business unit leaders. Less than half of them report that they are proactively involved in enhancing product launches or delivery, enabling strategic initiatives, protecting intellectual property, or enhancing customers' experiences. Less than a quarter are proactively involved in facilitating mergers and acquisitions.

Another indicator of limited integration between information security and risk management is the reported low involvement of legal departments, internal audit, and compliance, despite their vital roles in risk management. Fewer than half of these groups are reported to play a role in reviewing or developing information security action plans when significant organizational changes occur.

In addition, less than half of business unit leaders are involved in these activities. Corporate officers fared slightly better, with over half of them involved in reviewing their organizations' information security strategies. But they are otherwise disengaged.

Applying formal procedures to critical initiatives

Many organizations are applying formal information security procedures as a component of good execution. But they represent only about half of the survey respondents. They are using formal procedures to address information security issues in the application development process, vendor risk management, and training and awareness. The remaining organizations are applying only informal information security procedures or none at all. This is particularly concerning, where over 60% of survey respondents report Web application security is a major concern, yet slightly more than 40% of them do not formally address information security in their application development process.

Deploying information security capabilities

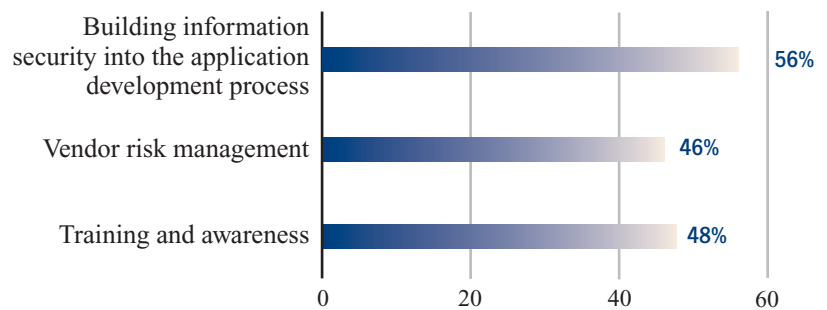
Almost all of the survey respondents state that they are effective in identifying systems critical to their organization. However, many respondents report that they typically do not meet with business unit leaders about information security matters, nor consider themselves particularly capable in identifying critical system functions and assets.

Survey respondents rate themselves relatively high for regularly conducting vulnerability and penetration assessments. Yet they continue to experience a high number of incidents of worms and viruses.

Finally, survey respondents rate themselves very effective in implementing point solutions, such as patch and vulnerability management, and identity and access management. Yet the effectiveness of these solutions is doubtful when you consider that few information security processes are being deployed, and there is a reported prevalence of worms and viruses.

The inconsistency between how organizations perceive the effectiveness of their information security capabilities, and how well they are actually being deployed, leaves them seriously open to unrecognized risks.

Organizations that use formal procedures to address the following information security results.



Many organizations are applying formal information security procedures as a component of good execution. But they represent only about half of the survey respondents.

Outsourcing operational activities

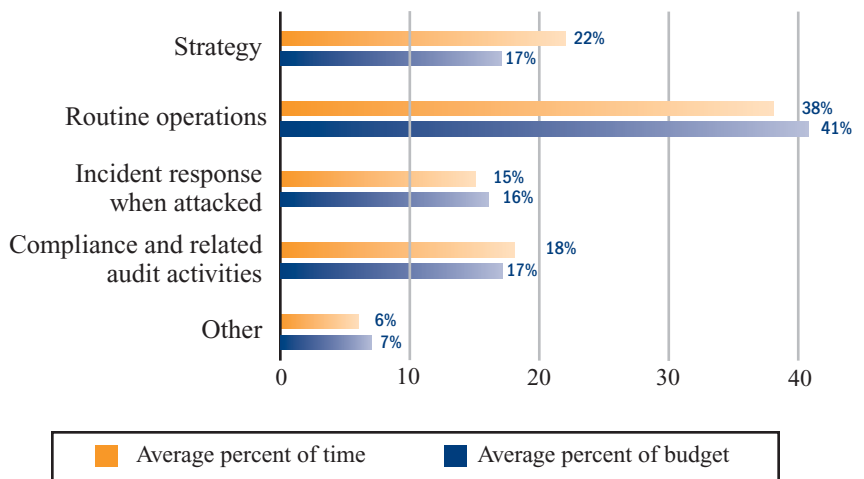
The value of outsourcing can be significant, considering that over half of the survey respondents indicated that their greatest challenge to executing strategic information security projects is the availability of experienced and well-trained IT and information security staff.

For instance, nearly three-quarters of survey respondents report that they still handle incident response in-house, and nearly 85% of survey respondents report that they do the same with project management. Both incident response in-house and project management lend themselves particularly well to outsourcing. In the case of project management, outsourcing offers the added benefit of acquiring specialized project management skills that normally do not reside within most organizations, but are critical to the success of most security projects.

Balancing time and budget between tactical and strategic activities

Survey respondents report that over half of their time and budgets are being allocated to routine operations and incident response. Considered both tactical and reactive, these activities provide minimal incremental value to the organization. Automating routine operations, in particular, offers an opportunity to reduce the amount of time and money devoted to this area of information security. Another option that many leading organizations are using is outsourcing specialized operational activities. This allows them to redirect valuable internal resources, including staff, to more critical strategic projects, where only 22% of information security’s time and 17% of its budget are currently being allocated.

Allocation of time and budget for information security activities.



Percentages may not add up to 100% due to rounding.

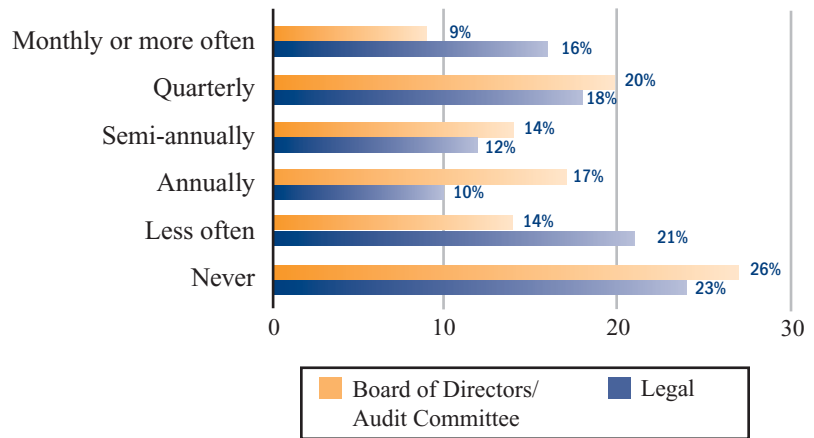
Communicating, reporting, and training

Communicating

As in prior years, survey respondents this year report meeting only infrequently, if at all, with their senior executives and boards to discuss business objectives and information security needs. Forty percent of survey respondents report meeting with their boards of directors and audit committees less than once a year or not at all. In addition, 44% of survey respondents report the same level of infrequency in meeting with their legal departments.

“Getting information security right” is a concern that executives and boards should share equally, given the strategic role information security plays in contributing to the organization’s performance. Security teams need clear direction from leadership regarding the prioritization and deployment of security-related initiatives, while leadership depends on reliable information to understand how information security is supporting the key initiatives and addressing regulations. Only by information security leaders and executive management talking to one another can organizations properly address their risks.

Frequency of meetings between information security leaders and their board of directors/audit committee and legal to discuss business objectives and information security needs.



Forty percent of survey respondents report meeting with their boards of directors and audit committees less than once a year or not at all. In addition, 44% of survey respondents report the same level of infrequency in meeting with their legal departments.

Reporting

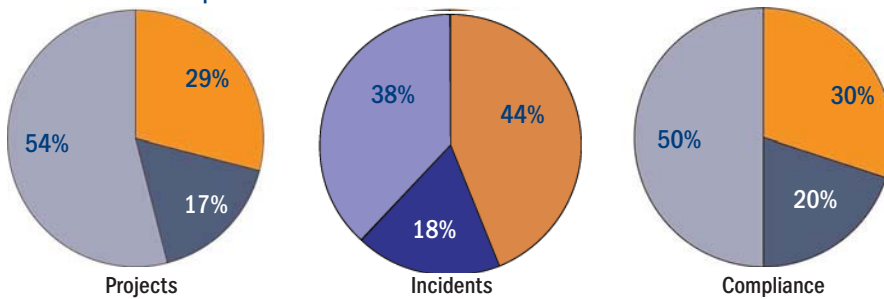
Regular reporting on information security projects, incidents, and compliance is equally as important as strong communication. Information security leaders should be providing these reports to boards of directors, and business unit leaders. These groups in turn should expect the reports to better understand how information security is supporting business initiatives and addressing regulatory compliance.

According to the survey, the most frequent reports being provided are primarily about projects, typically involving requests for investments or accounting for them. While slightly more than half of survey respondents provide these reports to their board of directors and business unit leaders at least once a year, the rest provide these reports less often or not at all. Reports about incidents and compliance are even less frequent. Over half of the survey respondents inform their board of directors and business

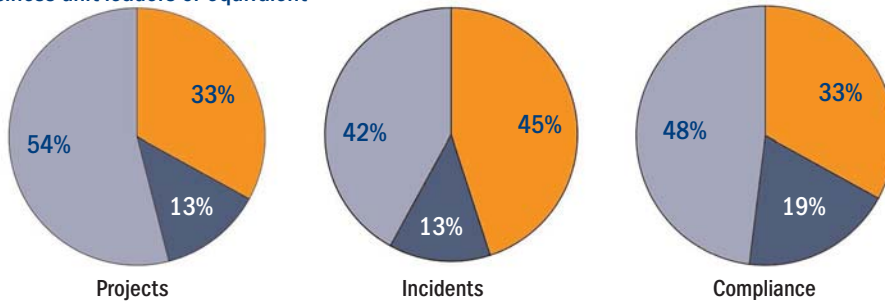
unit leaders about these matters less than annually, or not at all.

Frequency of information security leaders reporting to the following groups.

Board of directors or equivalent



Business unit leaders or equivalent



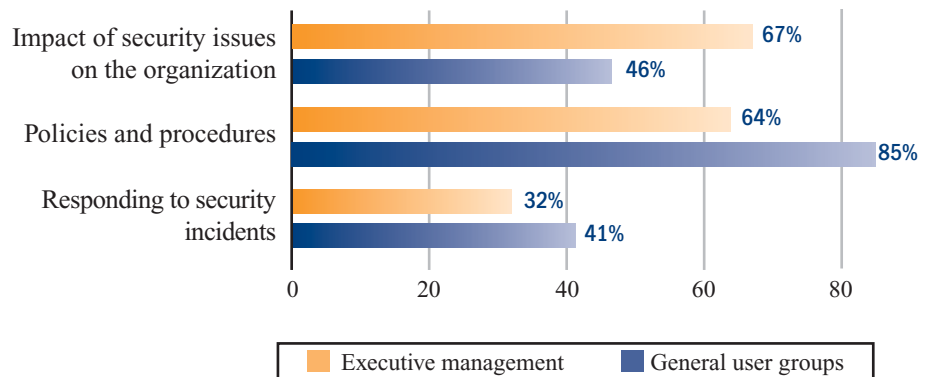
Training

When it comes to training and awareness, two-thirds of respondents' organizations are actively briefing executive management. This includes providing training and awareness on the impact of security issues to their organizations. However, the number of executives receiving training related to responding to security incidents drops to one-third. This leaves a substantial number of executives at a disadvantage when it comes to fulfilling their governance responsibilities and understanding the importance of their organizations following information security policies and procedures.

For general user groups of information, there is an even lower reported level of training participation. Less than half of organizations make provision for them to be trained on the impact of information security issues, and fewer still on responding to security incidents. With increasingly greater responsibility being placed on individuals because of trends such as mobile technology, organizations need to take seriously this finding—asking whether or not their employees are being adequately trained.

Less than half of organizations make provision for general user groups of information to be trained on the impact of information security issues, and fewer still on responding to security incidents.

Information security training and awareness programs being offered to organizations' executive management and general user groups.



Multiple responses allowed.

Information security certification requirements are reported to grow over the next 12 months, ahead of phishing and spyware—a clear indication that organizations are getting more serious about the value of certification. Twenty-five percent of organizations are using ISO 17799, and another 30% of them are planning to do so.

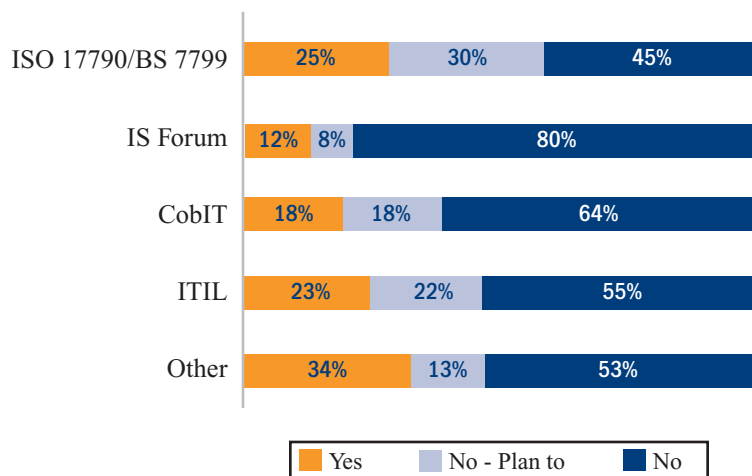
Recognizing the value of standards

There is a growing interest among survey respondents in information security standards and certification. Organizations are increasingly looking to adopt standards, which can provide a much needed framework for deploying effective information security practices and bringing about better alignment between information security and organizational objectives. According to the survey results, information security certification requirements are reported to grow over the next 12 months, ahead of phishing and spyware—a clear indication that organizations are getting more serious about the value of certification. Twenty-five percent of organizations are using ISO 17799, and another 30% of them are planning to do so.

Usage of ITIL is also gaining, even though security is not its primary focus. Almost a quarter of survey respondents are currently applying it, and an additional 22% are planning to do so—giving recognition to the importance of service standards.

Associated with the positive trend toward adopting information security standards is the recognition by organizations that standards demonstrate to clients and customers their commitment to good information security practices. Over two-thirds of survey respondents acknowledged this benefit.

Where organizations stand in formally adopting or becoming certified in each of the following standards.



Using standards for benchmarking

Recognizing the essential role of international standards as part of an effective information security program, Ernst & Young this year introduced an optional online benchmarking questionnaire as part of the *Global Information Security Survey*. It is derived from the latest version of the ISO 17799 security standard. This questionnaire provides organizations an excellent opportunity to compare their information security practices to an internationally recognized standard, and measure over time how they are maturing with respect to the standard.

Current Results

To date, 170 organizations from 27 countries have taken the opportunity to complete the benchmarking questionnaire. The results of these initial participants indicate specific areas where they can improve in their current information security practices, based on gaps between them and the ISO 17799 security standard.

From these results, the participating organizations can then identify information security practices that they need to remediate. While doing so, they can monitor their progress by periodically retaking the questionnaire. We will continue to make it available, so that more organizations may take advantage of it in the future.

For information on how your organization can participate, please visit www.ey.com.

Areas where participating organizations scored average or slightly above average* relative to the standard:

- ▶ Security policy
- ▶ Human resources security
- ▶ Access control
- ▶ Information systems acquisition, development, and maintenance
- ▶ Information security incident management

* Between 10.4 and 12 on a 20-point scale.

Areas where participating organizations scored below average** relative to the standard:

- ▶ Organizing information security
- ▶ Asset management
- ▶ Physical and environmental security
- ▶ Communications and operations management
- ▶ Business continuity management
- ▶ Compliance

** Between 8.2 and 9.9 on a 20-point scale.

Closing the Gap— A Call to Action

Even though many organizations recognize the widening gap between growing risks and what information security is doing to address them, action is still required to close the gap by applying sound information security practices. As a result, key risks will be more effectively mitigated and information security will become more of a strategic capability.

Referencing the four areas examined in this survey, we have identified the following actions that leading organizations are taking to close the widening gap. We encourage you to consider them as well.

- 1. Seize the opportunity that compliance offers to promote information security as an integral part of the business.**
 - ▶ Leverage compliance investments to improve critical elements of your information security function, such as architecture and organizational structure.
 - ▶ Integrate regulatory compliance into your information security practices to drive compliance efficiencies and achieve better overall risk coverage.
 - ▶ Establish a balance between information security efforts, focused on complying with corporate policies and procedures, and efforts to enable business objectives.
- 2. Increase the value of working with third parties, particularly in co-sourcing or outsourcing arrangements.**
 - ▶ Apply formal procedures, including a risk assessment framework to address the risks of third party business arrangements.
 - ▶ Expect independent reviews or certification of vendors in order to minimize exposure to new risks and realize the anticipated benefits of vendor outsourcing arrangements.
 - ▶ Apply recognized standards to your own information security function as a way of demonstrating to your clients and customers a commitment to good information security practices.
- 3. Take measures that enable business to be conducted more securely with emerging technologies.**
 - ▶ Thoroughly assess your organization's exposure to the risks of emerging technologies, especially those with immature controls in place or that rely extensively on user behavior for security.
 - ▶ Take comprehensive measures to address the risks that include training and awareness for individual users on their responsibilities for information security.
- 4. Put into place practices to more closely align information security with the organization.**
 - ▶ Integrate information security with your organization's overall risk management process.
 - ▶ Meet routinely with your board of directors, business unit leaders and regulators to:
 - Better understand their business initiatives and requirements, and how information security can support them.
 - Report on information security projects, incidents and compliance.
 - ▶ Reallocate scarce resources and budget to more strategic areas by automating routine operations and outsourcing specialized activities, such as incident response and project management.
 - ▶ Adopt or become certified in a standard that can provide a much needed framework for deploying effective information security practices and bring about better alignment between information security and organizational objectives.

Our Survey Methodology

This survey was conducted among executives in leading global companies, as well as government and non-profit agencies. More than 1,300 organizations in 55 countries from around the world participated. It was developed with the help of information security clients from organizations worldwide.

The questionnaire was distributed internationally to designated Ernst & Young professionals in each country practice within the Ernst & Young network, along with a protocol sheet to help minimize any possible interviewer bias. Most survey results were gathered from face-to-face interviews. However, when that was not possible, the questionnaire was delivered electronically. The primary respondents were chief information officers and chief information security officers.

Participants in the survey had the option to receive a Web address for the benchmarking portion of the survey, which was designed to be completed by a member of the responding organization's information security staff. The benchmarking survey gathered and provided the data to give survey respondents a detailed picture of how their organization compares with peers in implementing information security processes.

We would like to thank all of the survey participants for their input and all of the Ernst & Young teams who helped conduct the study, analyzed the findings, and assembled this report. Those of you who participated in the survey will receive on demand a benchmarking report of your responses compared with the global results and those of your industry and region. We hope you find it useful in improving information security within your own organization.

This publication has been carefully prepared but it necessarily contains information in summary form and is therefore intended for general guidance only, and is not intended to be a substitute for detailed research or the exercise of professional judgment. Ernst & Young can accept no responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

ERNST & YOUNG

www.ey.com

© 2005 EYGM Limited.
All Rights Reserved.

EYG No. DJ0001