

Insights on
governance, risk
and compliance

October 2013

Under cyber attack

EY's Global Information
Security Survey 2013



Building a better
working world

Contents

Today's cyber realities

You could be under cyber attack – now! 2

A significant percentage of executives reading this report will soon learn that hackers have breached the security perimeter of their organization.

Improve

Awareness of cyber threats propels improvements 3

Our survey suggests that many more organizations recognize the extent and depth of the threats they face and that they are making improvements to protect themselves. Yet, despite the progress they are making, organizations need to do more – and quickly – to combat cyber risks that are increasing exponentially in number and complexity.

Expand

Leading practices to combat cyber threats 9

Although organizations have made great strides in improving their information security programs, our findings suggest that there are 10 specific areas that leading organizations should take to expand on these improvements.

Innovate

To survive, innovation must power transformation 14

We asked respondents to rank 13 emerging technologies according to importance, familiarity and confidence in capabilities. The results show that organizations are placing more emphasis on what is in front of them and what they know and not nearly enough on what may be just around the corner or appearing on the horizon.

Conclusion

Combating cyber attacks requires leadership and accountability 20

The pace of technology evolution will only accelerate in the years to come – as will the cyber risks. Addressing these risks requires proactive thinking with tone-from-the-top support. Not considering risks until they arise gives cyber attackers the advantage.

Welcome



Paul van Kessel
EY Global RISK Leader



Ken Allan
*EY Global Information
Security Leader*

Welcome to *Under cyber attack: EY's Global Information Security Survey 2013.*

As many organizations have learned, sometimes the hard way, cyber attacks are no longer a matter of if, but when. Hackers are increasingly relentless and often politically motivated. When one tactic fails they will try another until they breach an organization's defenses. At the same time, technology is increasing an organization's vulnerability to attack through increased online presence, broader use of social media, mass adoption of mobile devices, increased usage of cloud services and the collection/analysis of big data.

In addition, regulators are seeing this threat and are putting pressure on businesses to comply with rules and regulations, to admit to cyber breaches publicly, and to submit to detailed examinations. Businesses should not allow themselves to fall into the regulatory trap; leaders should look to what they need to do to manage their residual risks and fully understand where they stand.

Organizations must be prepared to combat against and manage and mitigate cyber attacks that can occur anytime, anywhere.

Our 16th annual information security survey explores three levels of response to cyber risk in an environment where cyber attacks are numerous, constant and increasingly complex:

- 1. Improve** – Improvements and challenges: the improvements organizations are making to address the cyber threats they currently face and the challenges that still need more work
- 2. Expand** – Leading practices: the steps leading organizations are taking to stretch or expand current improvements to more proactively address new threats
- 3. Innovate** – Innovation in security: the solutions organizations need to develop to address technologies that are just around the corner or may be soon appearing on the horizon

Our survey explores the experiences of more than 1,900 client organizations and how they are responding to today's cyber threats. In addition to our survey, we interviewed a number of senior executives representing organizations that in EY's experience demonstrate leading practices in addressing cyber risks. We have also used analyses from EY security professionals and secondary research to provide depth and context to our survey findings.

We would like to extend a personal note of thanks to all of our survey participants. We appreciate the time they took to share their experiences with us.

We welcome the opportunity to discuss in greater detail the implications of these findings and look forward to hearing from you.

Paul van Kessel

EY Global RISK Leader

Ken Allan

EY Global Information Security Leader

Today's cyber threats

You could be under cyber attack – now!

Cybersecurity attacks have increased exponentially in the last few years. Every day, as the rapid-fire evolution of technology marches forward, new, more complex cyber risks emerge, threatening significant harm to an organization's brand and bottom line. Everyone and every organization is a target.

In the time it takes to review this report, a significant percentage of readers will learn of an attack that will have breached their organizations' security. The infiltration could have occurred days, weeks or even months ago – and they don't even know it. When the knowledge and magnitude of the breach does surface, the associated costs to the organization may be staggering. We need only to think of the high-profile attacks on well-known brands and organizations that appear in the world press daily, and consider the number of data records lost and the financial and reputation costs, to understand the impact.

In our Global Information Security Survey 2012 report, titled *Fighting to close the gap*, we addressed the notion of a widening gap between the current state of an organization's information security program versus where it needs to be to successfully defend the more insidious cyber attacks the majority of organizations face. In our Global Information Security Survey 2013 report we find that organizations are moving in the right direction, but more still needs to be done – urgently.

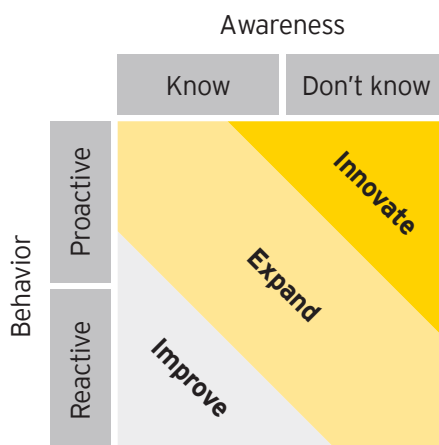
We have structured our Global Information Security Survey 2013 report to explore three areas:

1. **Improve.** For many organizations, this is the current state. Over the past year, organizations have made substantial progress in improving their defenses against cyber attacks. Yet their position remains reactive, addressing the threats they know, but not seeking to understand the threats that may be just around the corner.

2. **Expand.** Leading organizations are taking bolder steps to combat cyber threats. They are more proactive in determining both the known and unknown risks within their security programs. However, there remains room to expand security measures.

3. **Innovate.** Organizations aspiring to be information security innovators need to set their sights on new frontiers. These organizations need to continuously review, rethink and potentially redesign their entire information security framework in order to be better prepared. In many cases, innovating may require a fundamental transformation of the information security program to proactively fortify against both the known and the unknown risks in the cyber risk environment.

In the pages that follow, we explore the actions organizations have taken to address current threats, how leading organizations are looking beyond today's threats in an effort to prepare for the cyber risks that may be on the horizon, and how new technologies and new ideas can help organizations proactively prepare for a future that is certain to challenge even the most sophisticated and robust information security programs and functions.





Improve

Awareness of cyber threats propels improvement

Knowing that an attack will inevitably occur sparks improvements.



70%

of organizations indicate that information security policies are owned at the highest organizational level



76%

of organizations conduct self-assessments or commission an independent external assessment of the information security measures taken by third parties with data access

Awareness of cyber threats propels improvement

Our survey indicates that many organizations recognize the extent and depth of the threats they face – from the top of the organization to the shop floor. For nearly three-quarters of organizations surveyed, information security policies are now owned at the highest organizational level.

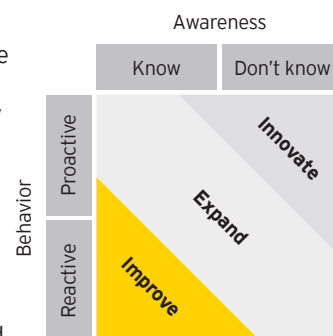
In 10% of organizations the information security function reports directly to the CEO. Information security professionals in 35% of the organizations we surveyed present information security to the board and those at the top of the governing structure on a quarterly basis; a little more than 1 in 10 report monthly. In our Global Information Security Survey 2012 the percentage of information security professionals who reported to senior executives monthly was zero.

Information security is now seen as vital to the ongoing health and success of the organization. Formal security operations (antivirus, IDS, IPS, patching, encryption, etc.) are mature in a majority of organizations.

Data protection is no longer being treated as another line item in a contract or something that organizations simply assume third parties do. Three-quarters of respondents indicate that their organizations mandate self-assessments, or commission an independent external assessment, of the information security measures performed by external partners, vendors or contractors who have access to their data.

However, although organizations have made strides in the right direction, there remains room for improvement. Many organizations are increasing investment in information security, yet many information security professionals continue to feel that their budgets are insufficient to address mounting cyber risks.

Similarly, although organizations feel they are addressing the right priorities, many indicate that they do not have the skilled resources to support their needs. Even though the trend is shifting focus away from “keeping the lights on” and toward improvement and innovation, many organizations are still leaving themselves exposed. Furthermore, a lot of organizations with technologies installed and running (antivirus, IDS, IPS, etc.), still find that the configuration and the processes around them (e.g., patch management, threat intelligence) are not adapted to today’s needs. It’s not surprising that many organizations feel that some aspects of their security management processes are not yet fully mature.



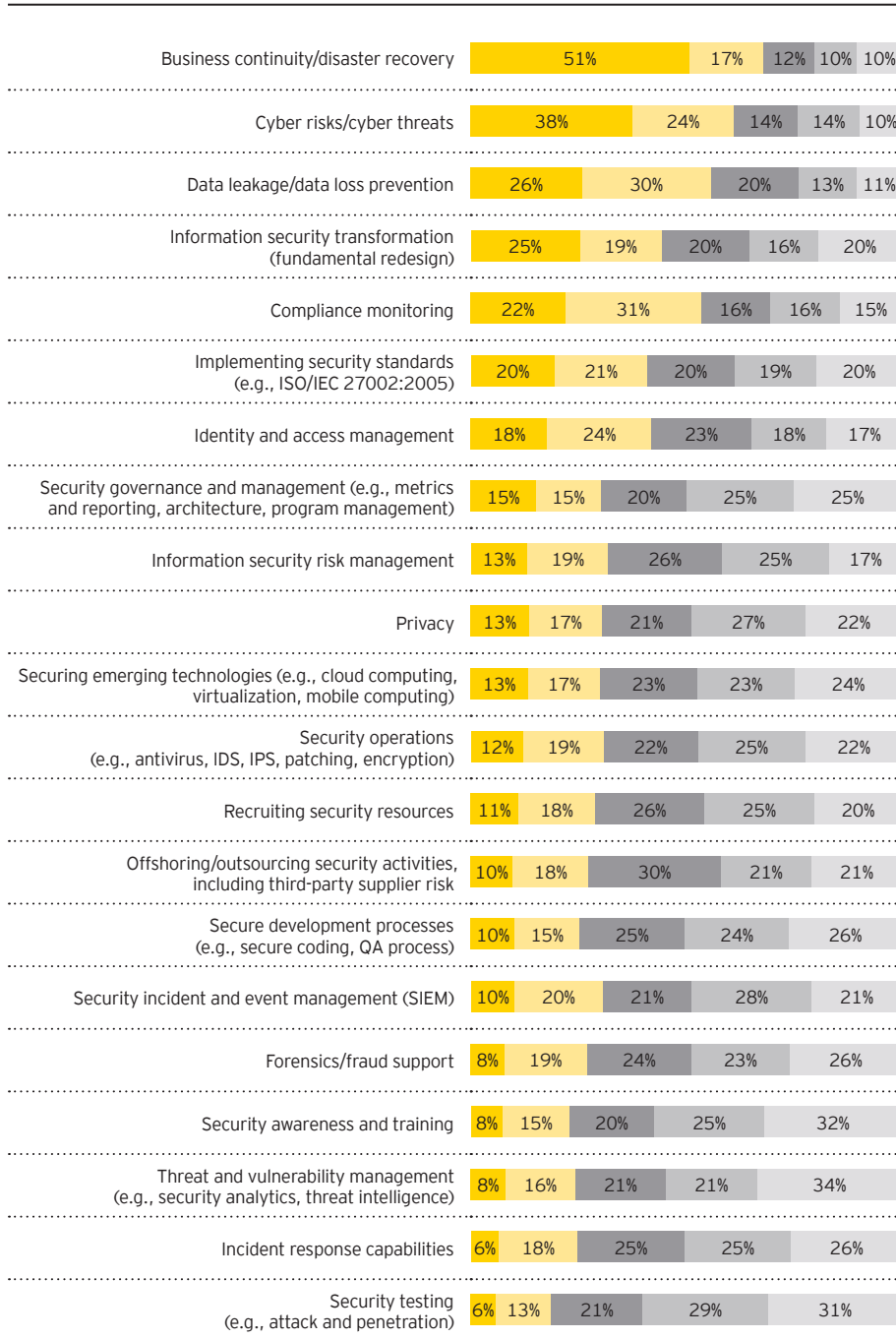
Maturity of information security management processes in surveyed organizations

Security operations (antivirus, IDS, IPS, patching, encryption, etc.)	14%	46%	33%	7%	
Security testing (web applications, penetration testing, etc.)	8%	28%	35%	22%	7%
Security awareness, training and communication	6%	24%	41%	26%	3%
Security governance and management (e.g., metrics and reporting, architecture, program management)	5%	23%	41%	26%	5%

Key: ■ Very mature ■ Mature ■ Developed ■ Not yet developed ■ Nonexistent

Results shown on a scale of 5 to 1, where 5 is very mature and 1 is nonexistent

Which information security areas do you define as “top priorities” over the coming 12 months?



Survey respondents were asked to mark five items showing their top priority with a 1, down to their fifth priority with a 5

Key: 1st 2nd 3rd 4th 5th



35%

of organizations have their information security professionals present information security to the board or members of the top governing structure quarterly

Based on findings from our Global Information Security Survey 2013, the following pages show the leaps forward that organizations are making in the fight against cyber crime; these are placed alongside the steps that they still need to make in today's environment.

The leaps that organizations are making



68%

of respondents state business continuity and disaster recovery as their top two priorities

Organizations are making moves to focus more on the right priorities

Generally, organizations name business continuity and disaster recovery as their top information security priority for the next 12 months. Cyber risks and cyber threats, data leakage and data loss prevention, information security transformation, and compliance monitoring round out the top five.

Financial institutions place even greater emphasis on cyber risk and cyber threats. It is also a concern for any organizations with US\$1 billion or more in revenue.



43%

of organizations indicate that information security budgets are on the rise

Organizations are investing more in information security

Overall, 43% of survey respondents indicate that their budgets are on the rise.

Within the government and public sectors, some respondents reported budget increases, but a majority indicate that their budgets have stayed the same as last year.

Small businesses with a turnover of less than US\$10m or businesses located in rapid-growth markets report the highest increases as a percentage of their budgets.



46%

of spend will be directed toward security improvement, expansion and innovation in the next 12 months

Organizations are shifting their focus from operations and maintenance to improving and innovating

Although security operations and maintenance remains important, it is less of a focus for the next year than for the year before.

Respondents' attention is shifting toward security improvement, expansion and innovation. In the year to come, 46% of spend will be directed to these initiatives.



46%

of organizations align their information security strategy to the organization's business strategy

Organizations demonstrate alignment among strategies and drivers

Nearly half of the organizations we interviewed align their information security strategy with the organization's business strategy; more than half align their information security strategy with their IT strategy.

Financial services organizations exhibit the strongest strategy alignment.

This suggests a consolidation of organizational strategies and drivers, as well as an increased understanding of the imperative for an information security strategy, regardless of an organization's size or industry.



68%

of organizations say their information security function partially meets organizational needs

Efforts to improve cybersecurity programs are growing

Since 2012 there has been a small drop (6% versus 8%) in the number of organizations saying that their information security function does not meet organizational needs, and a slight increase in those who say that it fully meets their needs.

At the same time, 68% believe that their information security function partially meets organizational needs and that improvements are underway. Among financial services organizations, this number rises to 74%.

Overall, information security functions are making the right improvements to more effectively meet the needs of the business and create value for the organization.

The steps that organizations still need to take

Information security departments continue to struggle with a lack of skilled resources, executive awareness and support

Although information security is focusing on the right priorities, in many instances, the function doesn't have the skilled resources or executive awareness and support needed to address them. In particular, the gap is widening between supply and demand, creating a sellers' market. Fifty percent of recipients cite a lack of skilled resources as a barrier to value creation. Similarly, where only 20% of previous survey participants indicated a lack of executive awareness or support, 31% now cite it as an issue.

As a result, although the information security department itself is making great strides toward improvement, support from the rest of the organization appears to lag behind.



50%

of respondents cite a lack of skilled resources as a barrier to value creation

Information security departments are still feeling the pinch

Although budgets are on the rise, information security functions continue to feel that budget constraints are their biggest obstacle to delivering value to the business. Sixty-five percent cite an insufficient budget as their number one challenge to contributing to the levels the business expects; among organizations with revenues of US\$10 million or less this figure rises to 71%.

Information security's number one obstacle to success mirrors the business's perception of their value. Although 17% of respondents indicate that information security fully meets the needs of their organization, 68% continue to feel that the department only partially meets organizational needs, with improvements underway.

Information security organizations need to make a better job of articulating and demonstrating the value of investments in security.



65%

of respondents cite budget constraints as their number one obstacle to delivering value to the business

Despite the security improvements organizations have made, many remain exposed

Nearly one-third of organizations still do not have a threat intelligence program, and slightly more than one-third have an informal program. In terms of vulnerability identification, nearly one in four has no program.

Financial services are the most mature of the industries we interviewed, although organizations of US\$1 billion in revenue or more also reported higher levels of maturity in their cybersecurity programs.

However, organizations, regardless of industry or size; should be concerned by the overall lack of maturity and rigor in a number of security areas. These critical issues must improve. In many cases, organizations will need to urgently invest more to improve and innovate. After all, the cost of a breach can be far more costly.



35%

of respondents feel they are leaders or pioneers in security programs

A lack of alignment in other critical areas is still too common

Although there have been improvements in alignment to business and IT strategies (for example, threat modeling needs to actively identify all areas of risk and move from a technology-led activity to a business-focused activity), many organizations have made no moves to improve their alignment with the organization's risk appetite or with today's risk environment. Financial services organizations are more aligned, while organizations in rapid-growth markets are less aligned.

This lack of alignment suggests that when setting budgets or determining resource requirements, too few organizations consider the cyber risks they are prepared to accept or must defend against at all costs, and far too many organizations only look inward to satisfy themselves that they are adequately protected against cyber risks – a view that may be costly when an attack occurs.



62%

of organizations have not aligned their information security strategy to their risk appetite or tolerance

Threats are growing too, often at a faster pace

Thirty-one percent of respondents say the number of security incidents within their organization has increased over the last 12 months by at least 5%.

When taking action to improve their information security function, organizations need to determine whether the improvements they are making will address the expected volume and frequency of existing and emerging threats, and whether they can implement them fast enough to keep pace with the threat landscape. Very specifically, organizations need to understand how effectively these actions will help to protect their business processes.



59%

of organizations cite an increase in external threats



31%

of respondents say the number of security incidents have increased over the previous 12 months



32%

of respondents say that phishing has most changed their risk exposure



45%

of respondents say mobile computing has most changed their risk exposure

Despite the efforts organizations have made over the course of the last 12 months to improve their information security programs, much more still needs to be done. Only 23% of respondents rated security awareness and training – a key component of continuous improvement activities – as their number one or two priority; 32% ranked it last. The only security area rated a lower priority by more respondents was threat and vulnerability management, an activity for which 31% of respondents had no program; this is surprising, as without it organizations have little visibility into where the cyber threats are and where a cyber attack may be coming from.

For as much progress as organizations have made, many organizations still have a long way to go. As the rate and complexity of cyber attacks continue to increase, organizations need to act quickly to avoid leaving themselves exposed to a costly and brand-damaging security incident that shakes the confidence of consumers and shareholders.

Based on actual incidents, these threats and vulnerabilities have most changed respondents' risk exposure over the last 12 months

Vulnerabilities (Vulnerability is defined as the state in which exposure to the possibility of being attacked or harmed exists)

Vulnerabilities related to mobile computing use	45%	48%	7%
Vulnerabilities related to social media use	32%	61%	7%
Vulnerabilities related to cloud computing use	25%	68%	7%
Careless or unaware employees	24%	58%	18%
Outdated information security controls or architecture	18%	60%	22%
Unauthorized access (e.g., due to location of data)	15%	71%	14%

Threats (Threat is defined as a statement to inflict a hostile action from actors in the external environment)

Phishing	32%	58%	10%
Malware (e.g., viruses, worms and Trojan horses)	31%	55%	14%
Spam	29%	57%	14%
Cyber attacks to disrupt or deface the organization	20%	69%	11%
Fraud	17%	74%	9%
Cyber attacks to steal financial information (credit card numbers, bank information, etc.)	14%	76%	10%
Cyber attacks to steal intellectual property or data	13%	77%	10%
Natural disasters (storms, flooding, etc.)	10%	75%	15%
Internal attacks (e.g., by disgruntled employees)	9%	78%	13%
Espionage (e.g., by competitors)	8%	82%	10%

Key: ■ Increased in past 12 months ■ Same in past 12 months ■ Decreased in past 12 months

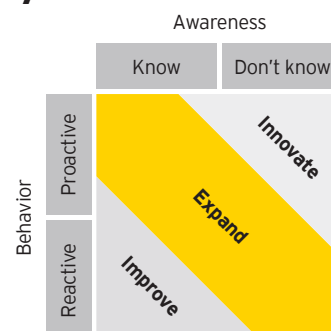
Expand

Leading practices to combat cyber threats

Organizations must signal support from the top to be proactive and ready for the unknown. Those that are satisfied with merely being reactive may not survive the next attack.

Leading practices to combat cyber threats

For the most part, organizations have improved their information security programs over the last 12 months. However, our findings suggest that leading organizations take improvements one step further. In particular, there are 10 areas that we have grouped into four categories where we see leading companies expanding improvement opportunities. See diagram on pages 12-13.



Commitment from the top

- ▶ **Board support.** Organizations need executive support to establish a clear charter for the information security function and a long-term strategy for its growth.

Organizational alignment

- ▶ **Strategy.** Information security must develop strong, clearly defined relationships with a wide range of stakeholders across the business and establish a clearly defined and formalized governance and operating model.
- ▶ **Investment.** Organizations need to be willing to invest in cybersecurity.

People, processes and technology to implement

- ▶ **People.** Today's information security function requires a broad range of capabilities with a diversity of experiences. Technical IT skills alone are no longer enough.
- ▶ **Processes.** Processes need to be documented and communicated, but information security functions also need to develop change management mechanisms to quickly update processes when opportunities for improvement arise.
- ▶ **Technology.** To gain the most value from a technology solution, information security functions must supplement their technology deployment efforts with strategic initiatives that address proper governance, process, training and awareness.

Operational enablement

- ▶ **Continuous improvement.** Organizations must establish a framework for continuously monitoring performance and improving their information security programs in the areas of people, process and technology.
- ▶ **Physical security.** Organizations should ensure that all their information security technology is physically secure, especially with consideration for access to Wi-Fi. A security operations center (SOC) can enable information security functions to respond faster, work more collaboratively and share knowledge more effectively.
- ▶ **Analytics and reporting.** Signature and rule-based tools are no longer as effective in today's environment. Instead, information security functions may wish to consider using behavior-based analytics against environmental baselines.
- ▶ **Environment.** Information security requires an environment that includes a well-maintained enterprise asset management system (which includes criticality of supported business processes) to manage events associated with business priorities and assess the true risk or impact to the organization.

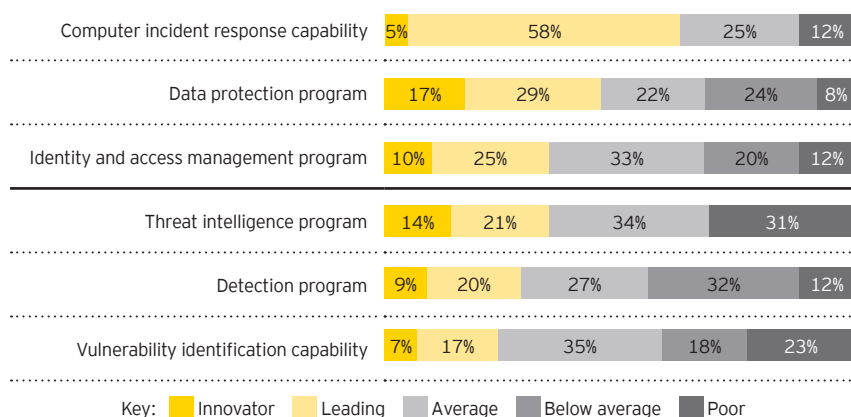
In addition to our survey findings, this year we elected to interview a select number of executives from organizations that, based on our experience in information security, we believe are more successfully protecting their organization from cyber risks and threats by being proactive and focused on the unknown.

We considered these interview responses within the context of our survey findings. We then augmented these results by drawing on the knowledge of our information security professionals and our considerable experience serving our clients. By layering the survey data, client experience and EY knowledge, we developed a clear understanding of the cascading, cumulative effect each improvement area identified has within the four expanded improvement categories. Ultimately, if an organization does not embark on its journey from the beginning (i.e., seek to make improvements at the “commitment from the top” stage), then it cannot achieve lasting change, or expand on previous successes, in any of the categories that follow.

Information security program maturity scale

In our survey, we asked respondents to rank the maturity of their information security programs in six key areas.

The responses to well-established information security approaches, such as identity and access management program, are below what is needed, and more recent approaches, such as threat intelligence and vulnerability identification, are less mature and need more attention.



We have taken the responses and ranked them from innovator to poor. Organizations are innovators if they have an advanced program and poor if they have no program at all.

Executives at the highest level of an organization need to commit to strive for information security maturity – and be accountable for achieving it. Without it, none of the other improvements the information security function seeks to implement will realize their intended benefits.

On the following pages we have captured the leading practices we noted during our one-on-one interviews with clients. Implementing one or more of these leading practices in isolation will help; it will improve the status quo of your information security. However, implementing leading practices in each of the 10 focus areas in concert will result in a significant expansion of your cyber threat responses and in a step change in your information security level.

The leading practices that enable improvement

Commitment from the top

“Our information security solution has changed from the traditional architecture of protecting the business practices itself to protecting the services that can complete the overall business practices. This turns the closely business coupled model into a relatively flexible loosely coupled model, providing security functions by means of services, packaging security services to release into the system.”

Financial services organization

“From our point of view, the most successful practice within information security was the changing of the idea: from considering issues solely on the operational level in the past, to the new approach, which is risk-oriented. Analysis, reporting, presentation and other methods are used to spot potential problems, and these problems are communicated and solved together with the business departments now in a more active way, which was rather passive in the past.”

Technology organization

“We drive the self-optimization process of information security management system through internal/external monitoring, including internal audit, internal information security risk assessment, internal security checking, external information technology audit, external compliance checking, etc.”

Financial services organization

“It’s important to have skilled professionals with business vision. The biggest challenge in today’s security market is to find professionals who are capable to innovate and adapt to the changes in the required speed.”

Mining and metals organization

Executive and board support

- Articulate risk appetite to provide clear, unambiguous direction
- Incentivize timely remediation of security issues, e.g., via internal audit or information security functions
- Measure information security performance and the criteria for success
- Foster an information security culture throughout all levels of the organization
- Understand how security events can impact the business, its services and its products
- Integrate information security insights directly into management decision-making processes
- Translate information security threats into their impact on the P&L and balance sheet

Organizational alignment

Strategy

- Identify and involve all relevant stakeholders
- Establish an organization-wide SOC, including comprehensive threat intelligence and vulnerability monitoring
- Align security strategy with overall business strategy
- Determine which security functions sit in-house versus outsourced and in the cloud
- Increase business and stakeholder confidence through use of trusted standards (ISO, COSO, COBIT, etc.) and consider alignment or formal certification
- Conduct independent third-party assessments – then get a second, independent opinion
- Define what is considered to be a “secure” organization; define KRI and KPI to monitor success
- Leverage the expertise of partners and vendors
- Build an information security organization and operating model that anticipates rather than reacts

Investment

- Identify who pays for cybersecurity
- Define a holistic risk framework to evaluate the increasing risk landscape
- Prioritize security initiatives to drive security investment
- Categorize expected benefits, e.g., brand protection, risk reduction, improved compliance and cost reduction
- Decrease the spend on maintenance and incidents; increase the spend on improvement and innovation

Every business is a potential target for a cyber attack. The motives, methods and opportunities may differ, but we have found that organizations at any one of the following stages in their life cycle are even more at risk:

- **Major organizational or structural change.** Although new technologies are driving marketing and customer-oriented initiatives, accompanying information security measures are not necessarily keeping up the pace. Marketing and development functions are not always as aware of – or prepared to respond to – the risks and threats that come with new technologies. Organizations can also disconnect and distract employees, causing them to forget or discard tested security measures and protocols.
- **Mergers and acquisitions.** New systems, policies, procedures and safeguards can create gaps in information security systems, measures and protocols. Mergers and acquisitions also often come with headcount reductions, activating many highly motivated disgruntled ex-employees familiar with their organizations’ systems, processes and security measures.
- **Entering new markets.** New markets usually means new processes, vendors, buyers, systems – even new languages and cultures. All of these factors come with varying levels of security risk and threat awareness. Unfamiliar governmental regulations on privacy, communications and data security further complicate the security environment.
- **Headline grabbers.** Hackers and cyber attackers often use public relations disruptions to target companies whose attention is focused elsewhere. Employees and shareholders can act erratically and unpredictably, straining the organization’s ability to identify and address an increased volume of threats on a variety of platforms. Reactive “emergency” actions designed to solve a short-term problem run the risk of actually creating openings and issues that can pose long-term risks

People, processes and technology to implement

Operational enablement

People

- ▶ Raise employee awareness of their security responsibilities and appropriate use of organization's assets, IP, data and technology
- ▶ Screen and hire the right people with the right skills and competencies, including those in high-risk roles
- ▶ Make information security part of the performance assessment of employees
- ▶ Know and control who holds elevated privileges
- ▶ Cultivate "security knowledge champions" in the business

Processes

- ▶ Use tested, enforceable contract clauses to make partners and vendors responsible and accountable for information security
- ▶ Describe information security processes to gain an understanding of rules and procedures and get everyone speaking the same language
- ▶ Align to a recognized information security standard, e.g., ISO 27001
- ▶ Ensure information security is an integral part of the GRC (risk management) function of the organization, not a stand-alone function
- ▶ Establish ongoing assurance monitoring of controls within outsourced third-party services
- ▶ Differentiate between compliance and regulatory requirements and defining the threat landscape
- ▶ Involve the business in the risk management process to improve key risk identification and increase security awareness
- ▶ Implement cyber governance into the business and business processes
- ▶ Anticipate potential security breaches and build adequate incident response and communications approach

Technology

- ▶ Build clear relationships among information technology, operational technology and information security
- ▶ Balance the technology choices with the threats and vulnerabilities the technology brings
- ▶ Ensure information security is an integral part of IT projects; as a result new information systems are secure from the start
- ▶ Understand the inventory of technologies you rely on and develop specific standards for them
- ▶ Develop the capability to monitor technology assets hosting sensitive data and critical business services in real time
- ▶ Routinely test security at an application level as well as an infrastructure level
- ▶ Align your information security efforts to the safety of your product, the robustness of your services and/or the customer experience
- ▶ Make information security part of your product/service offering

Continuous improvement

- ▶ Leverage intelligence from industry bodies, law enforcement agencies, peer organizations, regulatory authorities and professional advisers
- ▶ Continually reassess new technologies and the threat landscape to confirm focus is on the right priorities
- ▶ Establish a security simulation sandbox or capability to test security from a hacker's perspective
- ▶ Always remain vigilant; listen to what is going on in the market, understand new trends in information security and new threats, and adjust the risk assessment accordingly
- ▶ Implement an innovation function within the information security function to anticipate information security issues in new technologies

Functional security

- ▶ Understand the link between physical security and network security in light of wireless devices
- ▶ Effective prevention requires close cooperation between information security, human resources, IT and legal
- ▶ Improve coordination between physical, IT security and information security
- ▶ Systematically perform risk analysis on emerging technologies

Analytics and reporting

- ▶ Commission independent assessments from multiple parties within and outside the organization to assess the effectiveness of GRC and the information security function
- ▶ Build a holistic capability to correlate seemingly unconnected events and to detect behavioral anomalies using analytical tools and models
- ▶ Establish a dedicated security assurance reporting capability in order to measure security vulnerability and compliance improvements
- ▶ Investigate and assess current external threat level, then provide early warnings to IT and the business and establish crisis response teams
- ▶ Present to the board the impact of cybersecurity threats on the P&L, balance sheet, reputation and brand
- ▶ Coordinate with service providers and certification bodies to exchange information and leading practices

Environment

- ▶ Align first, second and third lines of defense to re-confirm responsibilities and reduce overlap in duties
- ▶ Effective prevention requires close cooperation between information security and IT
- ▶ Know critical assets and their vulnerabilities; monitor attacks on infrastructure level closely

"Key to successful practices is comprehensibility and applicability. People prefer practical hands-on in contrast to complex theoretical approaches. You need to identify the information-related risks across the business process using straightforward, standardized questions and challenge the received information by verification, then use this information to identify your 'crown jewels' and consider all relevant stakeholders. Then you can outline the business impact and the risk assessment, in combination with proposed measures to mitigate the risk."


Oil and gas organization

"Partnership with third parties has enabled us to design an information security strategy and associated improvement program with external market knowledge and expertise, as well as to flex resource requirements to help with surges in demand for security architecture and design, security testing and security incident response and investigation. Co-sourcing/outsourcing is viewed as much if not more as a capability enhancement play than it is for cost reduction."

Financial services organization

"It's vital to have the right players lined up in the 'Core Command Center' – the right functions (coordination among info sec, IT, line of business leaders, communications and marketing, physical security people. You need all the names in advance of the people who know all the right connections to all aspects of the business. And the right 'seniority' level has to 'be in the room' – i.e., people with decision-making authority in real time."

Financial services organization

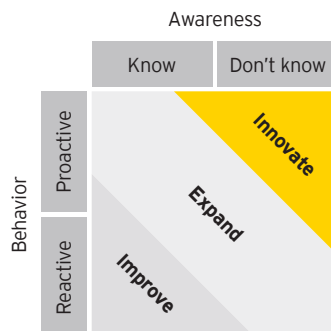


Innovate

To survive, innovation must power transformation

**Innovative information security solutions
can protect organizations against known
cyber risks and prepare them for a great
unknown: the future.**

Over the course of the last year, many organizations have made improvements to their current information security programs to better protect themselves from known cyber risks. Leading organizations have expanded the opportunities for improvement to more proactively anticipate both known and unknown cyber risks. However, to be a cyber threat innovator, organizations need to reach well beyond the 10 leading practices in four key categories that we have articulated. Innovators must constantly scan the horizon, searching for the vulnerabilities in each opportunity emerging technology brings.



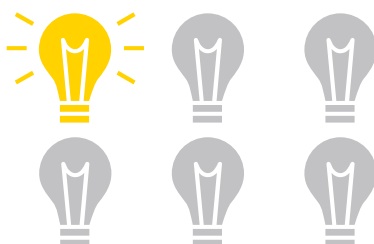
Budget allocations toward security innovation are inching their way up, enabling organizations to channel more resources and effort toward innovating solutions that can protect them against the great unknown: the future.

However, many organizations still feel that their budgets are insufficient to become innovating pioneers. As such, it is critical to focus time and effort when assessing new technologies to not only understand the benefits, but also the critical knowledge gaps and associated cyber risks: that is, an organization's familiarity with a technology and how capable it is to address these risks. Once the unknown becomes known, the organization can then prioritize and address the risks in order of importance.



50%

of respondents indicate that their budgets will increase anywhere from 5% to 25% or more in the next 12 months



14%

of spend in the coming 12 months will be on security innovation (emerging technology)

Emerging technologies and trends

In our survey, we ask respondents to rank by level of importance the following 13 emerging technologies and trends. We have grouped these technologies and trends into three categories: current, around the corner and on the horizon.

◆ Current technologies

Current technologies have been on many organizations' radar for several years now and in many cases have already been implemented. These include:

- ▶ **Digital devices**, which includes the security and risk considerations for:
 - Smartphones and tablets
 - Software applications
 - Web-based applications (HTML5) and website design to fit mobile screens
- ▶ **Social media** in the context of a digital business enabler and network facilitator

● Around the corner

Technologies around the corner have been a focus of consideration for a short while and may be close to broader implementation or adoption. These technologies include:

- ▶ **Big data**, which we describe as the exponential volume and complexity of data under management
- ▶ **Enterprise application store**, which encompasses associated costs versus increased productivity of employee requests for applications
- ▶ **Supply chain management**, in the context of how external assets (customers, suppliers, vendors, contractors and partners) impact security
- ▶ **Cloud service brokerage** as it pertains to how brokers manage cloud security, privacy and compliance issues
- ▶ **Bring your own cloud**, including personal cloud infrastructures that can be owned, managed and operated by an organization, third party or a combination of both, and may exist on or off the premises or concern data and applications access that only cloud owners manage

■ On the horizon

Technologies on the horizon are moving away from the concept or idea phase and one day may become reality. These technologies include:

- ▶ **In-memory computing**, which involves data storage in the main random access memory instead of complicated databases, allowing real-time analyses of high-volume data
- ▶ **Internet of things** (for example, embedded sensors, image recognition technologies), which are used in security programs but more often will be applied to our day-to-day lives
- ▶ **Digital money** and the associated regulations and legislation needed to address fraud and money laundering issues relating to mobile money services
- ▶ **Cyber havens**, where countries provide data hosting without onerous regulations

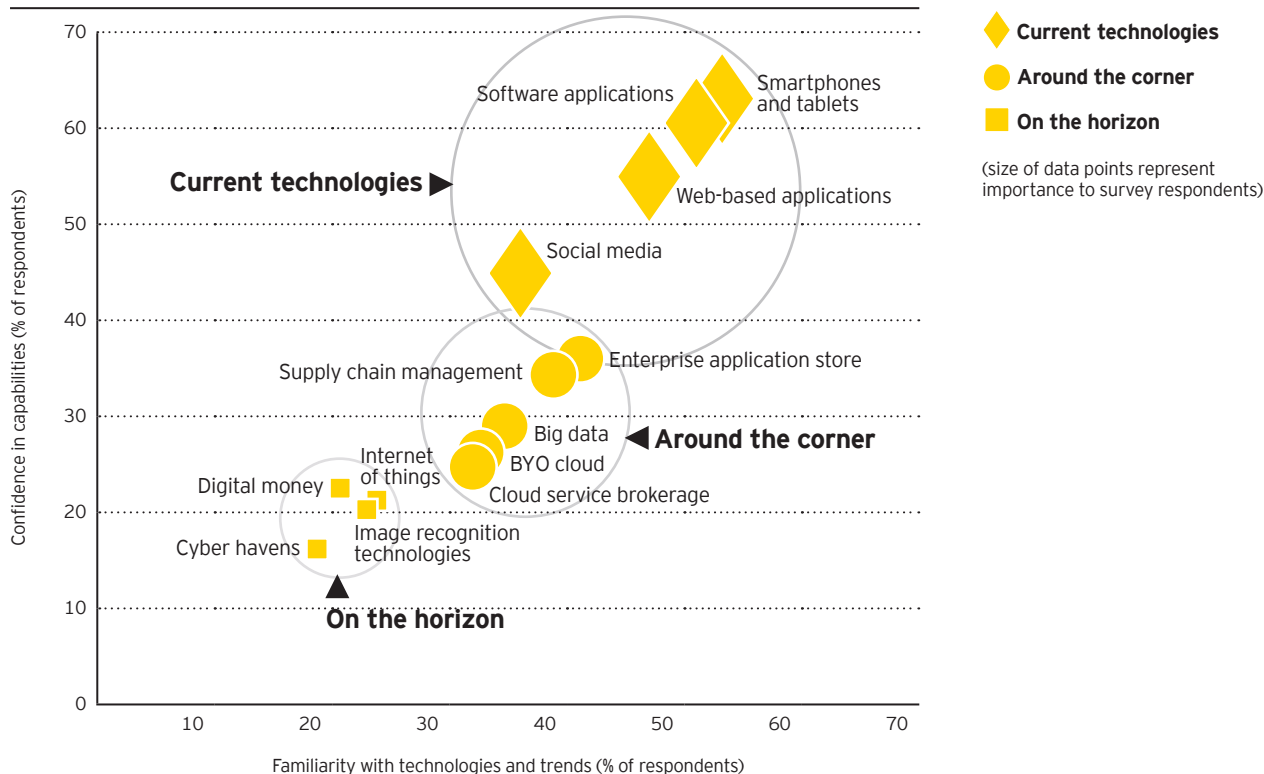
In addition to asking respondents to rank emerging technologies and trends based on their level of importance, we asked them to rank their level of familiarity with each, and then their confidence in being able to address the implications of these new technologies.

- **Familiar:** Are the emerging technologies known?
- **Capability:** Are we able to deal with the security implications of emerging technologies?
- **Importance:** How much focus do we put on emerging technologies threats?

We also asked our interviewees for their perspectives on emerging technologies and trends, like bring your own cloud. From these results, and the observations of our security professionals, we have developed a correlation diagram that ranks level of importance against the level of familiarity and capabilities.

The horizontal axis depicts familiarity, while the size of the circle indicates level of importance. Unsurprisingly there is a correlation between how familiar an organization is to how important it considers that technology to be. The vertical axis plots how confident an organization feels today in its capabilities to defend against cyber threats and minimize vulnerabilities.

Emerging technologies and trends





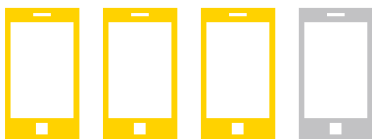
26%

say BYO cloud is important



19%

say in-memory computing is important



70%

find security of smartphones and tablets important



71%

find security of software applications important

◆ High rankings for current technologies

As demonstrated in the “Emerging technologies and trends” correlation diagram (page 17), current technologies and trends carry the most weight in terms of level of importance, familiarity and confidence in capabilities. For the most part, organizations are aware of these technologies and in many instances have already adopted them.

However, although we expected a high score for digital devices, a score of 70% for smartphones and tablets is not high enough given the devices’ ubiquity. A few years ago, organizations could not imagine employees using their personal smartphones and tablets for work purposes. In fact, bring your own device (BYOD) only entered the market in 2009; widespread adoption of BYOD has only occurred recently.

Yet, as we continue to hear about sensitive or confidential security breaches by those using smartphones and tablets, the question becomes: Who is responsible for the smartphone’s data – employer or employee? And how often is the smartphone being updated and security notifications appearing?

As current technologies become further entrenched in an organization’s network and culture, organizations need to keep in mind how employees use the devices, both in the workplace and in their personal lives. This is especially true when it comes to social media. Survey findings suggest that this continues to be an area where organizations still don’t feel confident in their capability to address risks.

If organizations still don’t have a high level of confidence after four years of mobile device use in the workplace, how will they face the challenge of managing and defending against personal and hosted clouds? Moreover, if organizations are putting all their energy into addressing current technology issues, how will they protect themselves against technologies that are just around the corner or are about to appear on the horizon?

Organizations need to be more forward-looking. As we see with digital devices and social media, organizations should have been preparing for current technologies as they were appearing on the horizon. If resources are still working to improve capabilities for technologies that are right in front of them or already behind them then they will have no time to prepare a defense that proactively protects the organization from technologies that are just around the corner.

Leading practice recommendations from some of our respondents:

- ▶ “If you have fallen behind, have two-way discussions with the business and IT – not to roadblock, or own or control, but to get things moving and make things happen.” – *Retail and wholesale organization*
- ▶ “Privacy, security and fraud functions need to integrate. What customers and employees see as private information will have to change.” – *Financial services organization*
- ▶ “The weakest element in information security is the human factor. As a result, we are constantly improving the awareness programs and introducing new security instruments.” – *Financial services organization*
- ▶ “We see the threats and risks rising in the application landscape. Whereas we used to protect the network and the exposed systems, we now need to protect all systems – at application level – throughout the whole network, including the content of information used in applications (e.g., emails and attachments).” – *Retail and wholesale organization*

● Average importance for technologies and trends that are just around the corner

Respondents rank technologies categorized as being around the corner (i.e., those that have been on organizations' radar for a period of time but may not yet be implemented or widely adopted) as average in terms of level of importance, familiarity and confidence in their capabilities to address related cyber risks.

Organizations typically view these technologies as offering opportunities to improve their performance and create competitive advantage. This is where familiarity and confidence in capabilities needs to increase today, as the importance of these technologies is likely to grow significantly in the near future.

When considering technologies appearing around the corner, respondents share these observations:

"Plan to close the gap through partnership or co-sourcing. Strengthen the monitoring capabilities; exploit existing tools and technologies. Increase due diligence of service providers; produce more robust incident management processing and establish threat intelligence."
– Financial services organization

"Security intelligence is the key to the future. ... We need big data techniques to find the bad guys."
– Financial services organization

The terms big data, supply chain management and enterprise application store (sometimes known as shadow IT) have already entered the corporate lexicon. Bring your own cloud and cloud service brokerage are as close to being adopted within organizations as BYOD was just a year ago. Organizations need to know now the cyber risks associated with these technologies, the organization's vulnerabilities to these risks and how they can mitigate them. Determining the cyber threats at the time of adoption is simply too late.

■ More attention needed on technologies and trends on the horizon

With so much effort focused on what is right in front of them, organizations are not giving enough consideration to technologies and trends categorized as being on the horizon – for now. As the speed at which technologies emerge and are adopted accelerates, the future may be closer than we think.

Mature organizations are already beginning to consider these technologies. They are reviewing, rethinking and, in some cases, completely redesigning their information security programs to prepare for future technologies and to capture the potential benefits of innovation.

Respondents considering technologies and trends on the horizon share the following observations:

"You can never say that you are fully successful in information security; this would be complacent. It is a continuous fight to close any potential gaps between threats and security measures. To this end, we 'get out of the box': we try to listen to the market, understand new trends in information security, to identify new threats and how we can deal with them. One must always be vigilant. The most important thing is to take a holistic view, be open-minded and open to discussion and collaboration. Not only within the boundaries of the organization, but also across organizations."
– Financial services organization

"New technologies will create new issues you have to think about in advance."
– Professional services organization

If organizations want to get ahead of cyber threats – or at least keep pace – they need to be proactive not only about the known and unknown risks associated with technologies just around the corner, but also about those just beginning to appear on the horizon. Organizations need to devote resources now to understanding both the opportunities and the threats – and to act on their findings. Organizations also need to be prepared to fundamentally transform their information security programs where necessary. Otherwise, the gap between an organization's information security program and the cyber threats it faces will only continue to grow.



Conclusion

Combating cyber attacks requires leadership and accountability

The rapid-fire pace of technology (r)evolution that we have seen in recent years will only accelerate in the years to come – as will the cyber risks. Not considering them until they arise gives cyber attackers the advantage. In fact, chances are, they're already in!

Organizations are making good progress in improving how they manage the risks they already know. However, with only 17% of respondents indicating that their information security function fully meets the needs of the company, they still have a long way to go.

And they are running out of time. The volume of cyber risks that organizations don't know, particularly when it comes to emerging technologies that are just around the corner or appearing on the horizon, is growing at a rate too fast for many organizations to keep up with.

New technologies now drive marketing and customer-oriented initiatives, while information security chases associated cyber threats from behind. Mergers or acquisitions, structural changes within the organization or entering new markets all place additional stress on the information security function to provide adequate protection.

As our survey findings indicate, organizations need to place more emphasis on improving employee awareness, increasing budgets and devoting more resources to innovating security solutions. These efforts need to be championed by executives at the highest level of the organization, who need to be aware that 80% of the solution is non-technical – it's a case of good governance.

Cyber attacks aren't going to stop!

In the past 12 months, more than twice as many respondents indicate that the frequency of attacks has gone up compared to those who indicate that they've decreased. If they succeed in infiltrating an organization's security perimeter, the consequences are distracting at the least, paralyzing at the worst. Security breaches can derail key objectives; undermine the confidence of shareholders, analysts and consumers; damage your brand reputation; and cause significant financial harm.

Too frequently, information security is perceived as a compliance necessity and a cost burden to the business. Executives need to view information security as an opportunity that can truly benefit the company and its customers. They need to look at the leading practices outlined in this report and consider how they can be applied to their business. However, with respondents indicating that they are devoting only 14% of their budget spend on innovating new security solutions in the next 12 months, the possibility of hackers wreaking havoc on organizations becomes not only likely, but inevitable.

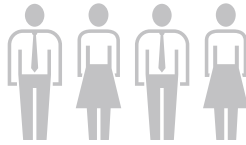
“Cyber crime is the greatest threat for organizations’ survival today.”

Ken Allan

EY Global Information Security Leader

Survey methodology

Profile of participants



1,909
respondents



64
countries worldwide



25
industry sectors

EY's Global Information Security Survey was conducted between June 2013 and July 2013. More than 1,900 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 take part. We distribute a questionnaire to designated EY professionals in each country practice, along with instructions for consistent administration of the survey process.

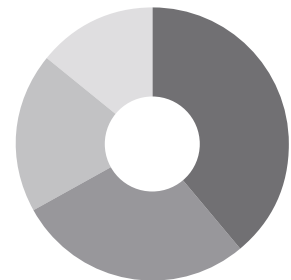
The majority of the survey responses were collected during face-to-face interviews. When this was not possible, the questionnaire was conducted online.

If you wish to participate in future EY Global Information Security Surveys, please contact your EY representative or local office, or visit www.ey.com/giss and complete a simple request form.

Respondents by industry sector

Aerospace and defense	47
Airlines	12
Asset management	42
Automotive	66
Banking and capital markets	361
Chemicals	35
Cleantech	5
Consumer products	116
Diversified industrial products	128
Government and public sector	128
Health care	37
Insurance	125
Life sciences	47
Media and entertainment	57
Mining and metals	39
Oil and gas	43
Power and utilities	61
Private equity	3
Professional firms and services	73
Provider care	12
Real estate	69
Retail and wholesale	98
Technology	179
Telecommunications	72
Transportation	54

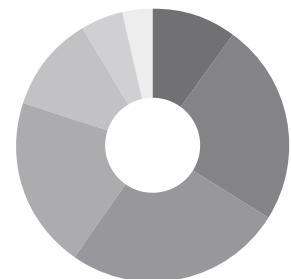
Respondents by area (1,909 respondents)



Key:

EMEA	39%
Americas	28%
Asia-Pacific	19%
Japan	14%

Respondents by total annual company revenue



Key:

US\$10–US\$50 billion	196
US\$1–US\$10 billion	455
US\$100 million–US\$1 billion	492
US\$10–US\$100 million	388
Less than US\$10 million	217
Government, nonprofit	96
Not applicable	65

Additional thought leadership resources

EY regularly publishes **Insights on governance, risk and compliance**, including thought leadership on information security topics. These perspectives are designed to help clients by offering timely and valuable insights that address issues of importance for C-suite executives. Please visit www.ey.com/GRCinsights

Beating cybercrime. Security Program Management from the Board's perspective.

Most organizations struggle to keep pace with the breakneck velocity of these changing technologies and threats, creating hazardous gaps between the true risks that threaten their viability and their ability to respond and mitigate these risks effectively. Organizations can benefit from an objective assessment of their information security programs and structures via EY's Security Program Management approach.

www.ey.com/spm



Cybersecurity: considerations for the audit committee

Cybersecurity is not just a technology issue; it's a business risk that requires an enterprise-wide response. Boards of directors are starting to take note, particularly members of the audit committee, who now list cybersecurity among their top concerns.

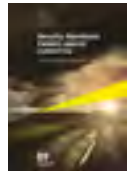
[http://www.ey.com/Publication/vwLUAssets/Cybersecurity_Considerations_for_the_audit_committee/\\$FILE/Cybersecurity_considerations_for_the_audit_committee_GA0001.pdf](http://www.ey.com/Publication/vwLUAssets/Cybersecurity_Considerations_for_the_audit_committee/$FILE/Cybersecurity_considerations_for_the_audit_committee_GA0001.pdf)



Security Operations Centers against cyber crime. Top 10 considerations for success.

Understanding that security information attacks can never be fully prevented, companies should advance their detection capabilities so they can respond appropriately. A well-functioning Security Operations Center (SOC) is at the heart of all such efforts. We explore the top 10 considerations critical to the success of your SOC.

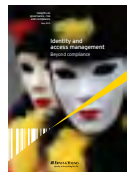
www.ey.com/soc



Identity and access management (IAM): beyond compliance

IAM is evolving into a risk-based program with capabilities focused on entitlement management and enforcement of logical access controls, leveraging new technologies to transform from a compliance-based program into a true business enabler.

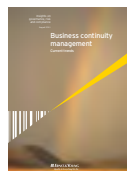
www.ey.com/iam



Business continuity management

Approximately 50% of companies neglect to take steps to safeguard their businesses in the event of a disaster, which could potentially threaten their existence. Disasters and the resulting non-availability of resources can be devastating, and leading companies have increasing awareness of the need to develop, maintain and sustain effective business continuity management programs.

www.ey.com/bcmtrends



Privacy trends: the uphill climb continues

As the privacy landscape continues to evolve and mature, trends are forming around how market conditions are impacting organizations' privacy decisions. Our report highlights the three megatrend categories playing increasingly large roles as we enter a new era in privacy protection: governance, technology and regulation.

www.ey.com/privacy2013



Key considerations for your internal audit plan: enhancing the risk assessment and addressing emerging risks

The internal audit risk assessment and the ongoing refresh processes are critical to identifying and filtering the activities that internal audit can perform to provide measurable benefit to the organization. The processes begin by identifying these emerging risks and focus areas and their corresponding practical, value-based audits.

www.ey.com/iaplan



Please also see this book on cybersecurity published by EY and ISACA: http://www.ey.com/US/en/Newsroom/News-releases/News_Five-Things-Every-Organization-Should-Know-about-Detecting-and-Responding-to-Targeted-Cyberattacks

EY's risk services

We have an integrated perspective on all aspects of organizational risk. We are the market leaders in internal audit and financial risk and controls, and we continue to expand our capabilities in other areas of risk, including governance, risk and compliance, as well as enterprise risk management.

We innovate in areas such as risk consulting, risk analytics and risk technologies to stay ahead of our competition. We draw on in-depth industry-leading technical and IT-related risk management knowledge to deliver IT controls services focused on the design, implementation and rationalization of controls that potentially reduce the risks in our clients' applications, infrastructure and data. Information security is a key area of focus where EY is an acknowledged leader in the current landscape of mobile technology, social media and cloud computing.

The leaders of our RISK practice are:

Global RISK Leader		
Paul van Kessel	+31 88 40 71271	paul.van.kessel@nl.ey.com
Area RISK Leaders		
Americas		
Jay Layman	+1 312 879 5071	jay.layman@ey.com
EMEIA		
Jonathan Blackmore	+44 20 795 11616	jblackmore@uk.ey.com
Asia-Pacific		
Iain Burnet	+61 8 9429 2486	iain.burnet@au.ey.com
Japan		
Shohei Harada	+81 3 3503 1100	harada-shh@shinnihon.or.jp

The information security leaders within our RISK practice are:

Global Information Security Leader		
Ken Allan	+44 20 795 15769	kallan@uk.ey.com
Area Information Security Leaders		
Americas		
Jose Granado	+1 713 750 8671	jose.granado@ey.com
EMEIA		
Ken Allan	+44 20 795 15769	kallan@uk.ey.com
Asia-Pacific		
Mike Trovato	+61 3 9288 8287	mike.trovato@au.ey.com
Japan		
Shinichiro Nagao	+81 3 3503 1100	nagao-shnchr@shinnihon.or.jp



About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the 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 ey.com.

About EY's Advisory Services

Improving business performance while managing risk is an increasingly complex business challenge. Whether your focus is on broad business transformation or more specifically on achieving growth, optimizing or protecting your business having the right advisors on your side can make all the difference. Our 30,000 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 exceptional client service. We use proven, integrated methodologies to help you solve your most challenging business problems, deliver a strong performance in complex market conditions and build sustainable stakeholder confidence for the longer term. We understand that you need services that are adapted to your industry 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 your strategy and change initiatives are delivering the value your business needs.

© 2013 EYGM Limited.
All Rights Reserved.

EYG no. AU1885
1304-1063727 EC
ED 0114.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

www.ey.com/giss