www.pwc.com/security

Defending yesterday

Key findings from The Global State of Information Security® Survey 2014

Advisory Services
Security

While organizations have made significant security improvements, they have not kept pace with today's determined adversaries. As a result, many rely on yesterday's security practices to combat today's threats.

pwc

Methodology

The Global State of Information Security® Survey 2014 is a worldwide study by PwC, CIO magazine, and CSO magazine. It was conducted online from February 1, 2013, to April 1, 2013. Readers of CIO and CSO magazines and clients of PwC from around the globe were invited via e-mail to take the survey. The results discussed in this report are based on the responses of more than 9,600 executives including CEOs, CFOs, CISOs, CIOs, CSOs, vice presidents, and directors of IT and information security from 115 countries. Thirty-six percent (36%) of respondents were from North America, 26% from Europe, 21% from Asia Pacific, 16% from South America, and 2% from the Middle East and Africa. The margin of error is less than 1%. All figures and graphics in this report, unless otherwise noted, were sourced from survey results.

Table of contents

The heart of the matter

While information security risks have evolved and intensified, security strategies—historically compliance-based and perimeter-oriented—have not kept pace.

The result? Today, organizations often rely on yesterday's security strategies to fight a largely ineffectual battle against highly skilled adversaries who leverage the threats and technologies of tomorrow.

These sophisticated intruders are bypassing outdated perimeter defenses to perpetrate dynamic attacks that are highly targeted and difficult to detect. Many use well-researched phishing exploits that target top executives. Compounding matters, the attack surface—partners, suppliers, customers, and others—has expanded as an ever-greater volume of data flows through interconnected digital channels.

These factors have combined to make information security progressively more complex and challenging. It has become a discipline that demands pioneering technologies and processes, a skill set based on counterintelligence techniques, and the unwavering support of top executives. A key tenet of this new approach is an understanding that an attack is all but inevitable, and safeguarding all data at an equally high level is no longer practical.

The Global State of Information Security® Survey 2014 aims to measure and interpret how global organizations implement practices to combat today's highly skilled adversaries. This year's survey indicates that executives are elevating the importance of security. They are heeding the need to fund enhanced security activities and believe that they have substantially improved technology safeguards, processes, and strategies.

But while organizations have raised the bar on security, their adversaries have done even more. This year's survey shows that detected security incidents have increased 25% over the previous year, while the average financial costs of incidents are up 18%.

The survey also reveals that many organizations have not deployed technologies that can provide insight into ecosystem vulnerabilities and threats, identify and protect key assets, and evaluate threats within the context of business objectives. And for many companies, security is not yet a foundational component of the business strategy, one that is championed by the CEO and board, and adequately funded.

Put simply, few organizations have kept pace with today's escalating risks—and fewer still are prepared to manage future threats.

"You can't fight today's threats with yesterday's strategies," **says Gary Loveland, PwC Principal.** *"What's needed is a new model of information security, one that is driven by knowledge of threats, assets, and the motives and targets of potential adversaries."*

In this new model of information security, knowledge is power. Seize it.

An in-depth discussion

As digital technologies become universal, they have transformed the business environment.

Today, organizations are increasingly interconnected, integrated, and interdependent. They employ technology and ubiquitous connectivity to share an unprecedented volume of information assets with customers, service providers, suppliers, partners, and employees. These sophisticated technologies enable organizations to perform business tasks with a velocity and degree of efficiency that are unprecedented.

But this evolved business ecosystem also imperils organizations by putting them at the mercy of adversaries who would exploit these technologies and processes to disrupt operations and even destroy businesses. As a result, security threats have become a critical business risk to global organizations.

The traditional reactive approach to information security strategy, which typically relegates security to an IT challenge, remains commonplace.

But it is no longer effective, nor is it defensible.

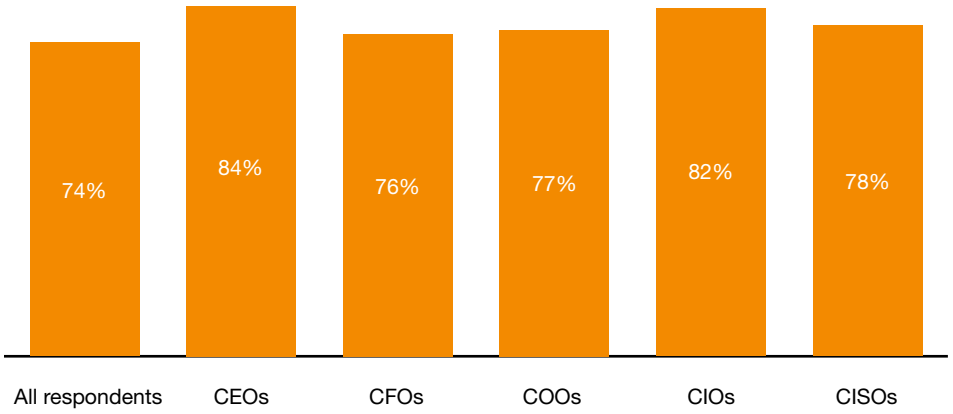
Today's new world of security risks demands that organizations treat information security threats as enterprise risk-management issues that can critically threaten business objectives. Safeguarding all data at the highest level is no longer realistic or even possible.

Against this backdrop, we asked business, security, and IT executives to tell us how they are addressing information security imperatives, and how well their privacy and information security safeguards are aligned with business objectives. The results of The Global State of Information Security® Survey 2014 show that most executives across industries worldwide are confident in their organization's information security practices.

Strong confidence in today's security practices

It is striking that, even in a climate of escalating and evolving risks, executives remain highly confident in their organization's security capabilities and activities. Globally, 74% of respondents say their security activities are effective. (Figure 1) And this optimism is strongest at the top of the org chart. For instance, 84% of CEOs say they are confident in their security program, and 78% of CISOs—those with direct responsibility for security—report confidence. Among executives, CFOs are the least confident. A regional view shows that respondents from South America (81%) and Asia (76%) report the highest levels of trust in their security programs.

Figure 1: Confidence in security activities (somewhat or very confident)



More than

80%

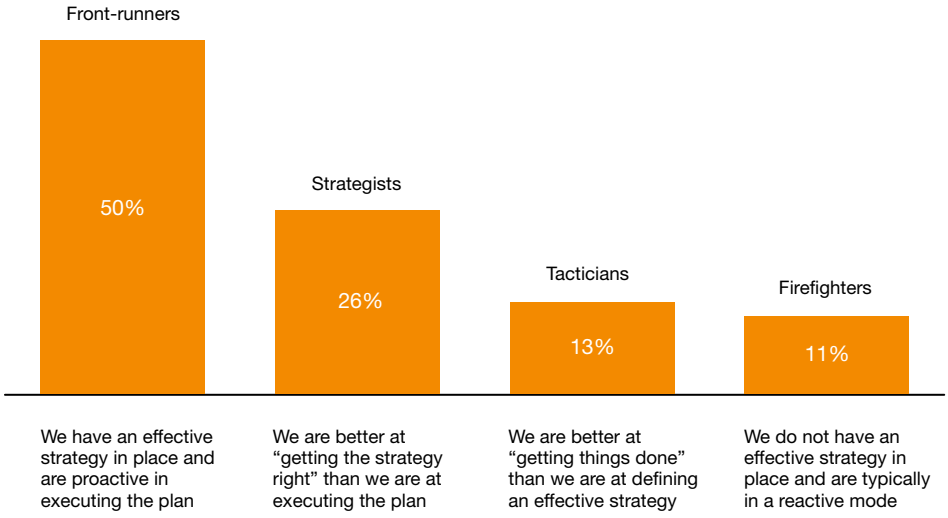
say security spending and policies are aligned with the business.

Another measure of confidence can be gleaned from how well executives perceive their organization's security program to be aligned with business strategy and overall spending. By that count, optimism is equally robust. More than 80% of respondents say security spending and policies are aligned with business objectives, an increase over last year for both categories. These levels of confidence suggest respondents understand that security is an integral part of the business agenda—and can contribute to bottom-line benefits.

Optimism also extends to how respondents rank their overall security strategy and their ability to proactively execute that strategy. We asked respondents to tell us how they rate their security approach, and results show they rank themselves higher than the past two years.

We label those who report they have an effective strategy in place and are proactive in executing the plan Front-runners, since they exhibit two key attributes of leaders. Among this year's respondents, 50% say they have the attributes of a Front-runner, a 17% jump over last year. (Figure 2) About one in four (26%) say they get strategy right but may not successfully execute the plan, a category we call Strategists. Those who consider themselves better at "getting things done" than defining effective strategy—Tacticians—account for 13% of respondents. And the group that we call Firefighters, which do not have a strategy in place and are typically in a reactive mode, comprise 11% of respondents.

Figure 2: How respondents characterize their approach to information security



Are Front-runners really leaders?

Self-assessments are, by their very nature, biased. So we took a closer look at the data and created a series of requirements that define "true leaders" on the basis of reported capabilities rather than self-perception. To qualify as leaders, respondents must:

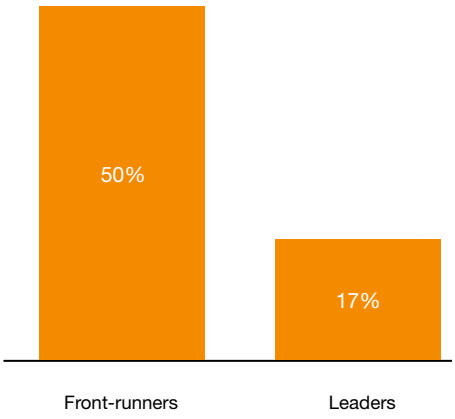
- Have an overall information security strategy.
- Employ a chief information security officer (CISO) or equivalent who reports to top leadership: the CEO, CFO, COO, CRO, or legal counsel.
- Have measured and reviewed the effectiveness of their security measures within the past year.
- Understand exactly what type of security events have occurred in the past year.

Filtering for these qualities shows that Front-runners are not necessarily leaders. Based on these criteria, only 17% of all survey respondents rank as true leaders. (Figure 3) We also found that, compared with Front-runners, real leaders detect more security incidents, have a better understanding of what types of security incidents occur and the source of those incidents, and report lower average financial losses as a result of security incidents.

Real leaders detect more security incidents, have a better understanding of what types of security incidents occur and the source of those incidents, and report lower average financial losses as a result of security incidents.

Regionally, leaders are most likely to be based in Asia Pacific (28%) and North America (26%), followed by Europe (24%), South America (21%), and the Middle East and Africa (1%). Industries most represented among leaders include technology (16%), financial services (11%), and retail and consumer (9%).

Figure 3: Front-runners vs. leaders



Another cause for optimism: Budgets are rising

If most respondents see themselves as highly competent in their information security practices, those who control the company purse strings also appear to be optimistic about the security function—or perhaps they understand that today's elevated threat landscape demands a boost in security investment. Either way, substantial increases in security funding are a good sign for security efforts. While budgets vary significantly across industries and by company size, overall respondents say security budgets average $4.3 million this year, a 51% gain over 2012. Despite this increase, however, information security budgets represent only 3.8% of the total IT spend this year, a relatively small investment.

Average information security budgets have increased

51%

over last year.

But what about the future? Optimism is high there, too. Almost half (49%) of respondents say that security spending over the next 12 months will increase, up from 45% last year. Regionally, respondents from South America (66%) and Asia Pacific (60%) expect that security investments will rise. Only 38% of North America respondents forecast an uptick in security spending, making them the least sanguine on spending.

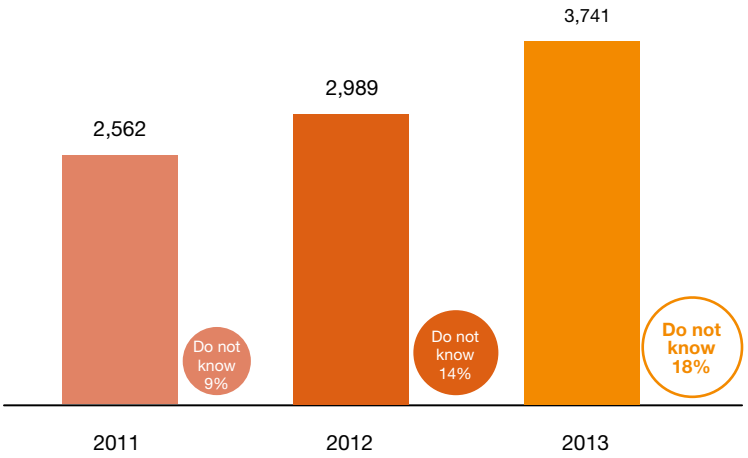
Today's incidents, yesterday's strategies

It has been all but impossible to ignore the barrage of news reports about increasingly sophisticated—and often successful—security breaches over the past year. Given the sometimes sensational, and often click-driven nature of news reporting, it's only natural to question the accuracy of reports concerning cyber intrusions.

The results of this year's survey corroborate some—but not all—of the reporting concerning security incidents.

One fact is indisputable: Security incidents are increasing. (We define a security incident as any adverse incident that threatens some aspect of computer security.) Survey respondents report a 25% jump in detected incidents over last year. (Figure 4) This would seem to validate the headlines trumpeting elevated security threats. On the other hand, an increase in detected incidents could also mean that organizations are getting better at identifying incidents.

Figure 4: Average number of security incidents in past 12 months



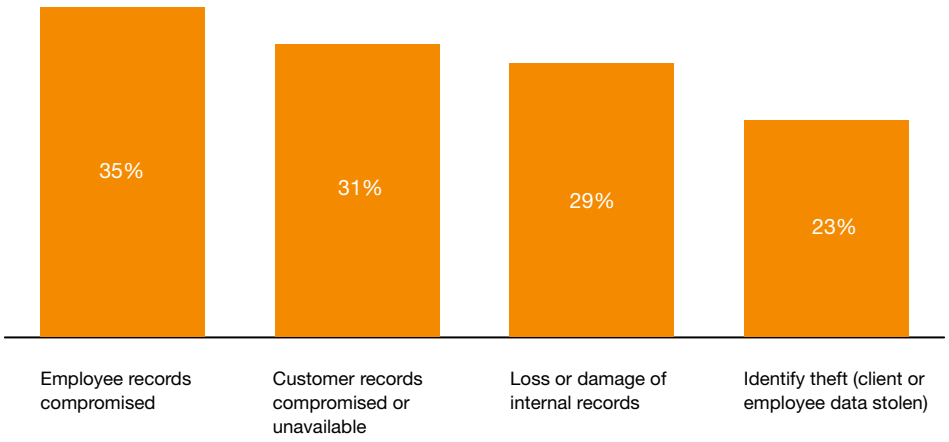
"Incidents are increasing not only because there are more threats out there, but also because some companies have invested in new technologies to better detect them," **says Mark Lobel, PwC Principal.** *"In that regard, increased detection of security incidents should be seen as a positive development."*

But the number of respondents who do not know the frequency of incidents continues to climb year over year—it's now at 18% —and that would seem to contradict the notion that organizations are becoming more adept at detecting intrusions. This finding, in fact, is more likely to suggest that old security models in use may be broken or ineffective.

The increase in incidents combined with a concurrent rise in the volume of business data being shared digitally results in an unsurprising finding: Proliferating data loss. This year, 24% of respondents reported loss of data as a result of security incidents, a hike of 16% over 2012.

Delving into the types of data exploited reveals some interesting findings. Compromise of employee records (35%) and customer records (31%) led the pack of data impacted. (Figure 5) Year after year, survey respondents tell us that employee and customer data are the most valuable information they hold—so presumably their security efforts would center on protecting these types of data. Yet the fact that employee and customer data are the most likely types of information to be siphoned off suggests that current data-protection efforts are not effective or focused on the right risks.

Figure 5: Impact of security incidents



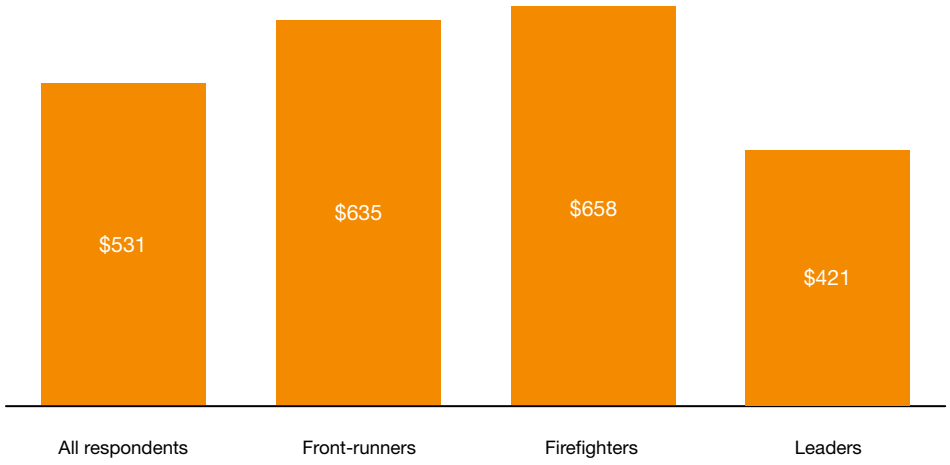
Note: Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

The compounding costs of loss

It would seem logical that, as the number of security incidents rise, so too would the financial costs. And so it is: We found that average financial losses associated with security incidents rose 18% over last year.

"Overall, the costs and complexity of responding to incidents are increasing," **says Shane Sims, PwC Principal.** *"This includes the cost to investigate; the cost to understand business risks and contain incidents; the cost to manage notification to regulators, customers, and consumers; and the cost of litigation. Also, the cost of remediation is rising because more records across more jurisdictions are being impacted, and security controls have not kept pace with the ever-changing threat landscape."*

Figure 6: Average cost per security incident



Parsing the data a bit more, we discovered that financial losses are accelerating sharply among respondents that report high-dollar value impact. Case in point: The number of respondents who report losses of $10 million-plus has increased 51% since 2011. We expect certain industries that have historically been proactive in investing in security initiatives would report lesser losses, but surprisingly, this wasn't the case. Industries reporting losses of $10 million or more included pharmaceuticals (20%), financial services (9%), and technology (9%).

Overall, the average cost of intrusions on a per-incident basis is $531. (Figure 6) Respondents we identified as leaders report the lowest cost per-incident, at

an average of $421—no surprise there. What we didn't expect to see is that self-identified Front-runners spend is $635 per incident—almost as much firefighters, those who are, by their own assessment, the least prepared to run an effective security program. This calls into question the real-world efficacy of Front-runners.

Insiders, outsiders, and hackers

As noted, headlines don't always reflect boots-on-the-ground reality in combatting threats. While high-profile incidents such as highly sophisticated intrusions attributed to advanced persistent threats (APTs) make for tantalizing copy, this type of incident is quite rare.

Indeed, reality is much more prosaic. Most respondents attribute security incidents to everyday insiders like current employees (31%) or former employees (27%). (Figure 7) Many see these insider threats as far more significant than headline-making, but infrequent, threats.

Figure 7: Estimated likely source of incidents

Note: Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

"I see the insider threat looming larger in my windshield than in the past," **says Michael A. Mason, chief security officer for Verizon Communications, adding that Verizon defines insiders as anyone who has access to Verizon's data.** *"And it's important to note that insider threats are not necessarily a 'bad guy' with bad intentions; it could be a good employee doing righteous work in an insecure manner. Our problems are more human than technological."*

Given the prevalence of employee risks, it is surprising that many organizations are not prepared to handle common insider threats. A separate survey co-sponsored by PwC, the 2013 US State of Cybercrime Survey, finds that one-third of US respondents do not have an incidence response plan for dealing with insider security incidents.[1] And among those that do have a response plan for internal incidents, only 18% of respondents describe the effort as extremely effective.

"One reason why organizations do not have effective plans in place for internal threats is that many classes of insiders, such as partners and suppliers, are invited within network perimeters and a certain level of trust is assumed," **says John Hunt, PwC Principal.** *"Businesses should understand that trust in advisors should not be implicit."*

Among external risk factors, it's important to note that some high-profile threat actors—hackers, in particular—do deliver on their risk potential. Consider this: 32% of survey respondents attribute security incidents to hackers, an increase of 27% over last year.

And what of high-publicity incidents such as attacks by foreign nation-states that employ APTs to exfiltrate information? Survey respondents say intrusions backed by foreign nation-states account for only 4% of detected incidents.

It's not a big concern for many companies, Verizon included. "Worrying about advanced persistent threats is, in some ways, like worrying about catching a cold while working in an anthrax factory," Mason says.

While APTs may present a remote risk potential, keeping abreast of rapidly evolving cyber threats is a priority for many large organizations, including Cablevision Systems Corporation, a multiple system operator (MSO) whose properties include cable TV, an Internet service provider, and a high-circulation daily newspaper.

"Like most MSOs, we are attuned to and follow the published reports denoting an increase in the detection of state-sponsored and cyber-terrorist activities, specifically as they relate to utilities and communication companies as targets," says Jennifer Love, senior vice president of security operations. "We use information from various sources, including the industry and government, to identify risks and guide decisions."

A weak defense against adversaries

To combat today's risks, organizations should be able to achieve ongoing insight and intelligence on ecosystem vulnerabilities and dynamic threats. Activities and investments should be driven by the best available knowledge about information assets, ecosystem threats, and vulnerabilities—and evaluated within the context of business activity.

For many, this represents a significant shift in thinking and planning. So it's not entirely surprising that many survey respondents report they have not implemented technologies and processes that provide insight into current risks. For instance, 52% of respondents have not deployed behavioral profiling and monitoring tools, and fewer (46%) do not employ security information and event-management technologies. Asset-management tools are critical to safeguarding data assets, yet are not in place for 39% of respondents we surveyed. Even established technologies that can be essential to protecting sensitive information are under-utilized. Most notably, we found 42% of respondents do not use data loss prevention tools.

[1] *2013 US State of Cybercrime Survey*, co-sponsored by CSO magazine, CERT Coordination Center at Carnegie Mellon University, Federal Bureau of Investigation, PwC, and the US Secret Service, March-April 2013

As data proliferates and is shared among more partners, suppliers, contractors, and customers, it is increasingly critical that businesses understand the risks associated with sharing data with third parties. What's more, organizations should ensure that third parties meet or beat their requirements for data security.

So it is worrisome to find that, in the US, many respondents do not have policies and tools to assess security risks of third parties, according to a separate survey co-sponsored by PwC.[2] For instance, only 20% say they evaluate more than once a year the security of third parties with which they share data or network access. Indeed, 22% say they do not evaluate third parties at all, while 35% say they evaluate third parties once a year or less. Similarly, only 22% of respondents say they conduct incident-response planning with third-party supply chain partners, while 52% never conduct incident-response planning for third party supply chains.

As noted, today's elevated and evolving threat environment requires that organizations understand that it is no longer practical—or, indeed, possible—to protect all information with equal priority. In a new model of security, businesses should identify and prioritize the information that really matters.

The information that really matters will vary by organization and by industry, of course. These "crown jewels" may include intellectual property (IP) such as product designs, marketing plans, executive communications, and business strategies. A more general definition can be stated as any information that could render significant hardship to the business if lost, stolen, or compromised.

Figure 8: Have policies to safeguard IP and trade secrets

Note: Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

Non-tangible assets such as IP now account for 80% of the value associated with S&P 500 firms, according to Ocean Tomo, the Intellectual Capital Merchant Banc™ firm.[3] And as the value of IP increases, so does its appeal to cyber criminals.

Despite the increasing value of IP and the potential consequences of its loss, this year's survey finds that many respondents do not adequately identify and safeguard their high-value information. For instance, only 17% of respondents classify the business value of data and only 20% have implemented procedures dedicated to protecting IP. (Figure 8) Slightly more (26%) maintain an inventory of assets and asset management. Survey results show that, in some industries, inclusion of policies to protect IP is actually declining.

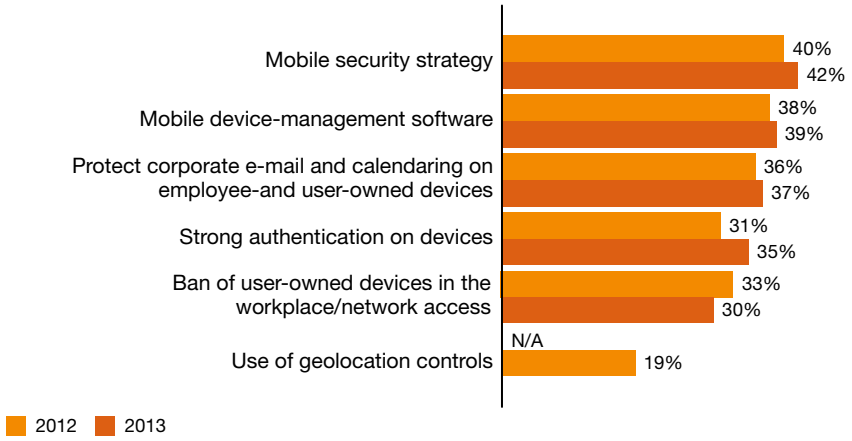
Another key risk to data security is the surge in the use of mobile devices such as smartphones and tablets, as well as the "bring your own device" (BYOD) trend. While the use of mobile devices to share and transmit data continues to increase, deployment of mobile security

[2] *2013 US State of Cybercrime Survey*, co-sponsored by CSO magazine, CERT Coordination Center at Carnegie Mellon University, Federal Bureau of Investigation, PwC, and the US Secret Service, March-April 2013

[3] Ocean Tomo, *Ocean Tomo's Annual Study of Intangible Asset Market Value*, April 2011

policies lags the proliferating use of smartphones and tablets. In fact, survey respondents indicate that efforts to implement mobile security programs do not show significant gains over last year and in some cases are actually declining. (Figure 9) For instance, only 42% say they have a mobile security strategy in place, and fewer (39%) say their organization has deployed mobile device management (MDM) software, a critical tool for automated management of a fleet of smartphones.

Figure 9: Initiatives launched to address mobile security risks



Note: Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

Only ***18%*** *of respondents say they have policies governing cloud services.*

Cloud computing has been around for more than a decade, and is commonplace—if not quite mainstream—in the corporate ecosystem. Almost half (47%) of respondents use some form of cloud computing, a healthy gain of 24% over the year before. Among those who use cloud services, 59% of respondents report that their security posture has improved.

So it is a bit surprising to learn that many organizations have not seriously addressed the security implications of cloud services. For instance, among survey respondents that use cloud services, only 18% say they have policies governing the use of cloud.

"A lack of policies for cloud computing represents a serious security gap for businesses," says Joshua McKibben, PwC Director. "The proliferation of data being shared, in combination with the increase in the use of mobile devices, creates an environment in which cloud services are more widely used—and potentially abused—by employees. At the same time, it is essential that businesses ensure that third-party cloud providers agree to follow security practices."

Advanced persistent threats, as noted, get more than their share of press, and that could account for the increase in those who seem to be taking APTs seriously. For instance, 54% of overall survey respondents say they have protection/detection management solution technology in place. Among industries, a higher percentage of aerospace and defense (61%), public sector (58%), and pharmaceuticals (58%) respondents say they have deployed an APT solution.

According to the 2013 US State of Cybercrime Survey, APT tools are most likely to include malware analysis, inspection of outbound traffic, rogue device scanning, and analysis and geolocation of IP traffic.[4]

[4] *2013 US State of Cybercrime Survey*, co-sponsored by CSO magazine, CERT Coordination Center at Carnegie Mellon University, Federal Bureau of Investigation, PwC, and the US Secret Service, March-April 2013

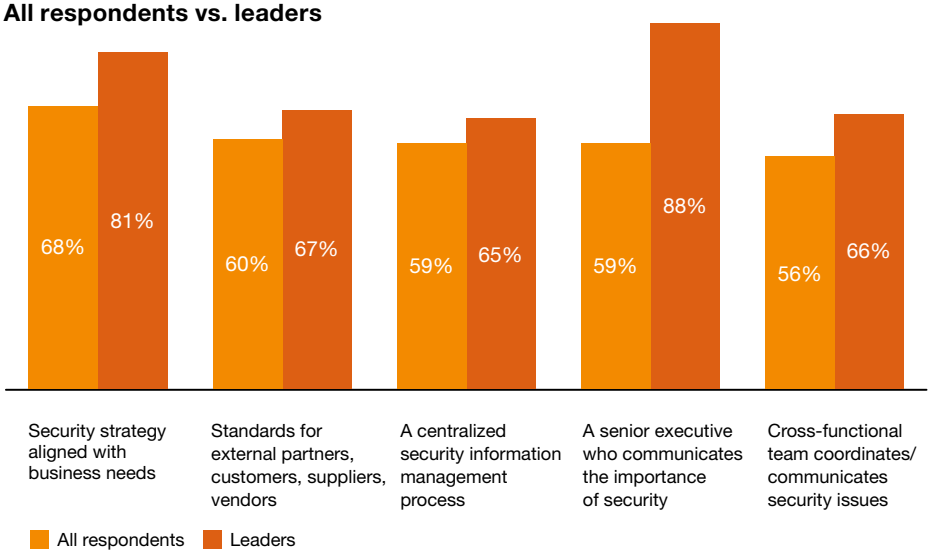
Preparing for the threats of tomorrow

Today, adversaries are constantly sharpening and evolving their capabilities to exploit new vulnerabilities. Addressing these threats will require that organizations approach activities and investments with best-available knowledge about information assets, ecosystem threats, and vulnerabilities. These activities should be evaluated within the context of business activity.

This year's survey indicates that those we define as leaders are enhancing their capabilities to do just that by implementing policies that elevate security to a top business imperative—not just an IT challenge. How so?

Leaders are aligning security with business needs, setting standards for external partners, and, in general, rethinking the fundamentals of security. (Figure 10) For instance, 88% of leaders have a senior executive who communicates the importance of information security across the enterprise. Another forward-thinking policy is to designate a cross-functional team that coordinates and communicates security issues, which 66% of leaders employ.

Figure 10: Security policies and safeguards currently in place—All respondents vs. leaders



Note: Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

"These types of policies demonstrate a new commitment to security, one that focuses on the involvement of top executives and the board to ensure that the company designs and implements an effective security program," **says Joe Nocera, PwC Principal.** *"It also underscores the need to raise security awareness among employees and third parties that handle sensitive data."*

"At Cablevision, the C-suite and board readily embrace security initiatives," **says Jennifer Love, SVP of security operations.** *"Our executives and board understand the importance of information security and express a keen interest in understanding what threats we face and what we are doing to mitigate our vulnerabilities."*

Policy and executive support are just a start, however. A measure of real intent can be gauged by whether companies have also deployed technologies to execute these policies.

Leaders are more likely to have deployed tools that provide a real-time analysis of suspicious activity logged on network hardware and applications. For instance, 66% of leaders say they have implemented security information and event management (SIEM) technologies. Similarly, 66% of leaders say they have deployed event correlation tools, which aggregate and correlate information from disparate tools like vulnerability and intrusion monitoring systems. Vulnerability scanning solutions, in place at 71% of leaders, assess networks and applications for weaknesses.

While our focus is on leaders who have implemented the technologies above, it's just as important to stress that, given today's elevated threat landscape, all organizations should strongly consider implementation of these safeguards when applicable.

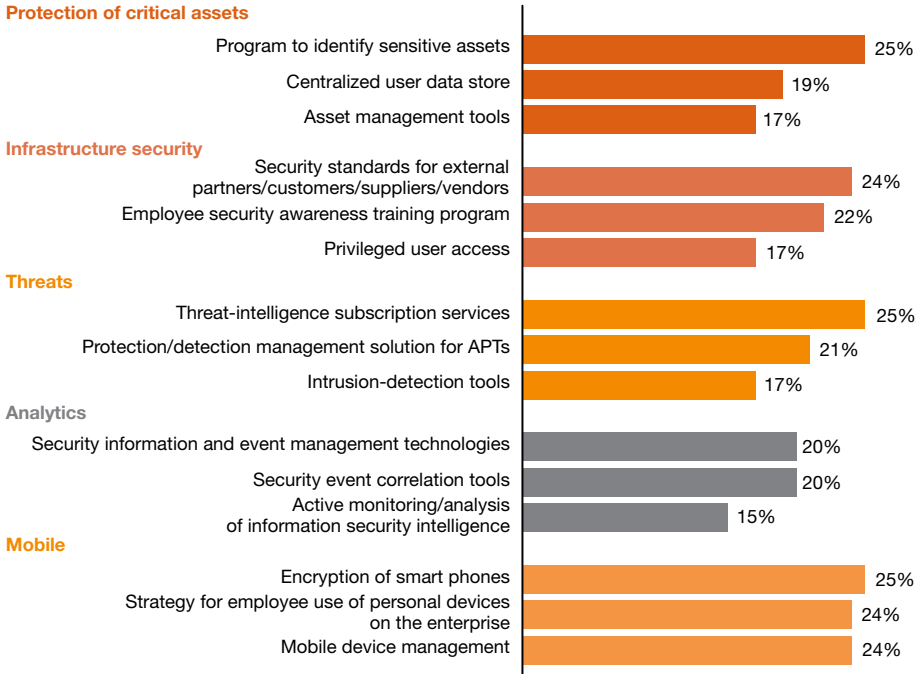
Another example can be found in employee security awareness and training programs. Employee awareness is critical to the success of any security program, and 60% of respondents say they have an employee security awareness training program in place. Because adversaries often target employees with social engineering schemes, 100% of respondents should implement an effective employee-training program.

"We see a lot of attacks that target what is in the employee's hands," **says Susan Mauldin, chief security officer for Equifax, the global consumer credit-reporting agency.** *"Because of this, our employee training and awareness is role-based and targets high-risk groups such as call-center employees, privileged users, and executives, with current training exercises focusing on targeted phishing attacks."*

To gauge respondents' priorities in preparing for the threats of tomorrow, we looked at priorities for implementation of process and technology safeguards over the next 12 months. We were interested in five categories in particular: protection of critical assets, infrastructure security, security threats, analytics, and mobile device security.

Effective security today requires that organizations identify and prioritize protection of "crown jewels." Twenty-five percent (25%) of respondents say they will prioritize over the next 12 months deployment of a program to identify sensitive assets, and 17% say they will prioritize asset management tools. (Figure 11) These types of solutions provide a key way to understand, value, and manage an organization's sensitive data.

Figure 11: Safeguards not in place but a top priority over the next 12 months



Note: Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

To enhance infrastructure security, almost one in four (24%) respondents say they will implement security standards for external partners, suppliers, vendors, and customers. This is critical as more organizations open their networks, applications, and data to third parties. What's more, technologies such as virtualization and cloud services have amplified the potential for compromise by a privileged inside user. Consequently, monitoring and managing privileged users is now a key challenge; we found that 17% of respondents plan to add privileged user access management tools over the next 12 months.

Other priorities focus on technologies that can help gain a better understanding of threats as well as improve security for mobile devices. For the first time, we asked respondents if they plan to add threat-intelligence subscription services as a means to obtain third-party assistance and early warnings about threat-intelligence risks and zero-day vulnerabilities. And many are: 49% of respondents say they currently use threat-intelligence subscription services, and among those that do not, 25% said implementation of these services would be a priority over the next 12 months.

At Equifax, top priorities include hardening employee devices in ways that will enable the financial services company to better understand threat actors. "We are taking a look at hardware that is used by employees and are basically sandboxing the environment to shield the computers from viruses and malware," Mauldin says. "This addresses risk, but it also helps us determine what types of threats are incoming and who is looking at Equifax as a target."

Given the soaring interest in Big Data, we also wondered whether organizations plan to leverage analytics as a means to improve security. It's a strategy that is gaining favor: Twenty percent (20%) of respondents say they will prioritize security information and event-management tools, and an equal number say security event-correlation technologies are a top priority.

"These types of technologies can help organizations detect patterns and anomalies in activity that can provide insight and intelligence on cyber threats facing the business," says Prakash Venkata, PwC Managing Director. "Armed with this insight, business leaders can anticipate and dynamically react to changes in their companies' cyber threat profile."

Another front-burner issue is mobile device security. Almost one in four respondents say they plan to prioritize encryption of smartphones, add mobile device management (MDM) solutions, and implement a strategy for the use of personal devices on the enterprise network.

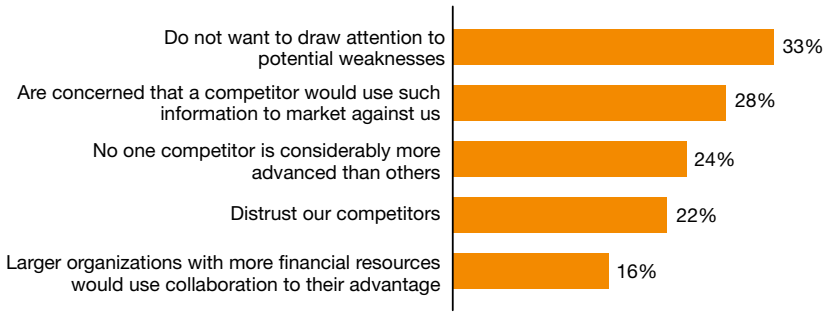
In the past year, sharing information about security threats—even among competitors—has emerged as a powerful offensive tool. We believe that collaboration can enable a business to more quickly adapt to market changes. In PwC's 5th Annual Digital IQ Survey,[5] we found that firms with collaborative C-suites intertwine business strategy and IT, which often improves the performance of a business.

So we were curious how global respondents, many of whom operate in an increasingly competitive environment, would view collaboration with others to improve security and share knowledge of threats. Many organizations see the merits of collaboration: We found that 50% of respondents say they collaborate with others, and among leaders, that number rises to 82%.

Equifax provides an example. "We participate in FS ISAC (the Financial Services Information Sharing and Analysis Center)," CSO Mauldin says. "This is very important to us because many government agencies also participate in FS ISAC, and it provides a proactive way to learn about evolving threats." Equifax participates in several other industry groups, and also collaborates with peers.

Among the 28% of respondents that do not collaborate, primary reasons for not sharing information include concerns about accentuating weaknesses, worries that a competitor might use information to its favor, and frank distrust of competitors. (Figure 12) Finally, 22% of respondents do not know if their organization collaborates with others.

Figure 12: Reasons for not collaborating on information security



Note: Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

[5] PwC, *PwC's 5th Annual Digital IQ Survey*, 2013

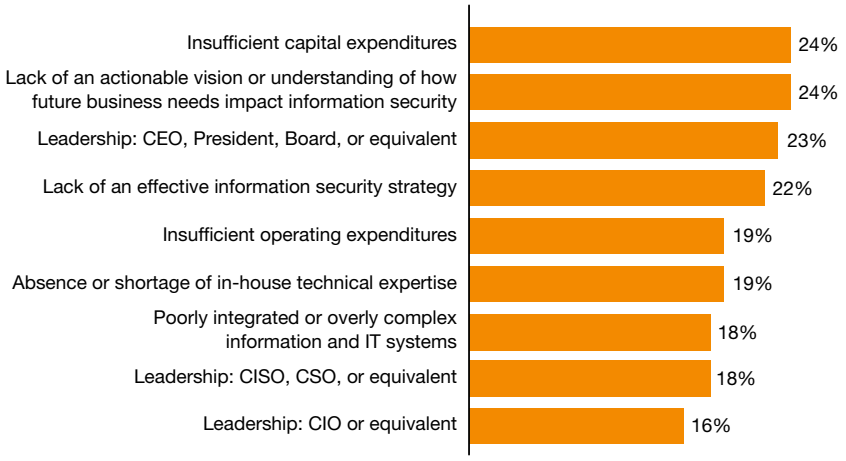
Obstacles to advancing security

While most security stakeholders agree that action should be taken to improve information security, there appears to be little consensus about the challenges of doing so. We asked respondents to identify the greatest obstacles to better security. The answers revealed a wide range of diverging opinions and, in some cases, finger pointing.

Overall, survey respondents say the most significant obstacles include insufficient capital funding, inadequate understanding of how future business needs will impact information security, committed leadership, and a lack of an effective security strategy. (Figure 13) Given the upward tick in security budgets this year, concern about funding may take care of itself. But it is troubling that deeply fundamental issues such as the understanding and alignment of security with future business needs and the efficacy of security strategies are among top concerns. Respondents are also very likely to point to executive leadership, the CEO in particular, as a top impediment to improved security.

And who or what do CEOs blame? Interestingly, chief executives overwhelmingly named themselves as obstacle No. 1. CFOs, meanwhile, point to CEOs as the leading hindrance, followed by the CIO, CISO, and CSO. Ask CISOs, the executives directly responsible for information security, and they'll put insufficient funding (both capital and operating) at the top of the list, followed by a lack of in-house technical expertise. CIOs flag a lack of strategy and vision, along with leadership of CEOs and security executives.

Figure 13: Greatest obstacles to improving information security



Note: Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

"This lack of clarity on obstacles to effective security shows, in part, that businesses have not engaged in sufficient dialogue around security. In this dialogue, employees, executives, and third parties all understand their role in information security, key priorities, and the biggest risks," **says David Burg, PwC Principal.** *"Building and sustaining a culture of security awareness will also require the full support of top executives, including the CEO and board. This must be an ongoing discussion."*

The global cyber-defense race

For several years, Asia Pacific has taken the lead in investment in security technologies, processes, and spending. As a result, the region pulled ahead of others in developing and implementing effective security programs. (Figure 14)

And it still holds the top spot. In fact, 28% of those whom we identify as leaders are from Asia Pacific, which represents only 21% of overall total respondents.

But Asia Pacific's high ranking in security practices is being vigorously challenged by South America. For the first time, South America seems poised to take the lead in information security investments, policies, and safeguards. The continent leads in key factors like security spending and employment of a CISO to oversee security, and is neck and neck with Asia Pacific in many others.

Nonetheless, Asia Pacific remains very strong in security spending and leading practices. Europe and North America, on the other hand, lag in many aspects, including employment of a CISO, inclusion of key policies such as backup and recovery/business continuity, and collaboration with others. North America exhibits some key strengths, such as requiring third parties to comply with privacy policies and employee awareness and training, but is behind in many other measures.

Figure 14: Security practices by region

	South America	Asia Pacific	Europe	North America
Security spending will increase over the next 12 months	66%	60%	46%	38%
Have an overall security strategy	75%	79%	77%	81%
Employ a Chief Information Security Officer	75%	74%	68%	65%
Have a senior executive who communicates the importance of security	68%	69%	51%	55%
Measured/reviewed effectiveness of security policies and procedures in past year	70%	69%	53%	49%
Have policy for backup and recovery/ business continuity	58%	55%	45%	47%
Require third parties to comply with privacy policies	55%	58%	55%	62%
Employee security awareness training program	54%	63%	55%	64%
Have procedures dedicated to protecting intellectual property (IP)	20%	24%	17%	21%
Have intrusion-detection technologies in place	64%	67%	63%	67%
Inventory of where personal data are collected, transmitted, and stored	53%	60%	52%	64%
Collaborate with others to improve security and reduce risks	66%	59%	45%	42%

Note: Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

Asia Pacific—Still the pacesetter

Asia Pacific remains the pacesetter in security spending and practices. Security investment is strong: Average security budgets have increased 85% over last year, and at 4.3%, Asia Pacific reports the highest IS budget as a percent of overall IT spending. Respondents are optimistic on the future IS spend, with 60% saying their security budget will increase over the next 12 months. However, average financial losses due to security incidents are up 28% over last year.

Average security budgets have increased

85%

in Asia Pacific.

Asia Pacific matches South America in key policies like employing a CISO to oversee the security program. The region is also highly likely to have adopted progressive new security measures, such as having a senior executive who communicates the importance of security (69%) and collaborating with others to enhance

security (59%). It is also most likely to deploy intrusion-detection technologies (67%) and have an inventory of where personal data is collected, transmitted, and stored (60%) when compared to South America.

Yet a year-over-year comparison reveals that Asia Pacific is beginning to stall in implementation of certain security policies and technologies. For instance, the number of respondents who report they have a policy for backup and recovery/business continuity is down over last year, and other key policies such as employee training and procedures dedicated to protecting IP are essentially static.

China comprises 33% of Asia Pacific respondents in this survey, followed by India (31%) and Japan (17%). By most measures, China eclipses other countries in security practices and policies. For instance, 60% of respondents from China use behavioral profiling and monitoring, 73% have centralized user data storage, and 72% employ vulnerability scanning tools, all higher than adoption rates of other countries. Sixty-two percent (62%) of Asia Pacific respondents have protection/detection management solutions for APTs and 66% have implemented SIEM technologies, results that outstrip other nations. What's more, no country has implemented security policies for mobile devices, BYOD, and social media at a higher rate than China. For instance, 71% of respondents from China have a policy in place for the use of personal devices on the enterprise network, compared with 64% in the US and 54% in India. In comparison with China, India is making solid overall gains in security programs and policies but it lags China on almost all counts.

South America: A new powerhouse from the south

South America shows solid gains in security spending, policies, and technologies. By many measures, the region matches—and sometimes surpasses—Asia Pacific.

For instance, information security budgets have jumped 69% over last year, and 66% of South America respondents say security spending will increase over the next 12 months. Security budgets comprise 4.1% of the overall IT spend, higher only in Asia Pacific. South America respondents are most likely to employ a CISO (75%) and to have a policy for backup and recovery/business continuity (58%). The continent leads in collaborating with others (66%) and is essentially tied with Asia Pacific in progressive policies such as having a senior executive who communicates the importance of security (68%). Average total financial losses due to security incidents are up modestly (4%) compared with last year.

75% *of South America respondents say their organization employs a CISO.*

Respondents from Brazil comprise the largest percentage of South America respondents (48% of the total), followed by Mexico (30%), and Argentina (21%). Brazil ranks high in many measures—behavioral profiling and monitoring (57%) and use of vulnerability scanning tools (63%), for instance—but generally lags China and the US.

South America is not without weaknesses. For instance, the percentage of respondents who say their organization has a policy for employee security awareness training is comparatively low at 54%, as is those who have an inventory of locations where personal data are collected, transmitted, and stored (53%).

Financial losses due to security incidents in Europe increased

28%

over last year.

Europe: Falling behind in funding and safeguards

Unlike other regions, investment in information security is down slightly (3%) over last year in Europe, and the continent continues to lag in adoption of key security safeguards.

In addition to a slight degradation of security investments, only 46% of European respondents believe security spending will increase over the next 12 months. While the number of detected security incidents is down 22% over last year, average financial losses due to security incidents shows a 28% increase.

Implementation of important policies, including backup and recovery/ business continuity (45%) and security awareness training and communications (21%), are comparatively low in Europe. Also lacking is the number of respondents who say they collaborate with others (45%) and those who have a mobile security policy (38%).

North America: Lagging and leading

Investment in security is soaring in North America, as is the number of detected security incidents. And while adoption of key policies remains low, North America leads in some important areas.

Average security budgets are up 80% over last year, although the outlook for future spending in the coming year is the lowest among all regions: Only 38% of North America respondents say security spending will increase over the next 12 months. The number of detected security incidents jumped 117% over 2012, while the average financial losses due to security incidents increased 48%.

North America leads other regions in some key practices, including having an overall security strategy (81%), requiring third parties to comply with privacy policies (62%), and employee security awareness training (64%). It also is most likely to inventory, collect, transmit, and store personal data (64%) and to use intrusion-detection technologies (67%). On the downside, North America is behind other regions in collaborating with others (42%) and employment of a CISO (65%). North American respondents are also least likely to

In North America, detected incidents increased

117%

over last year.

have reviewed the effectiveness of their security practices within the past year.

The US, which comprises 84% of North America respondents, ranks high in strategies for cloud computing (52%), mobile device security (60%), social media (58%), and BYOD (64%), second only to China in most factors.

What this means for your business

One thing is certain: yesterday's security defenses are not effective against today's rapidly evolving threats.

The results of The Global State of Information Security® Survey 2014 capture information security at an uncertain juncture, simultaneously poised on the threshold of change and stalled at the inertia of the status quo. Respondents demonstrate progress in deploying important new security safeguards on one hand, and inattention to key strategies like protection of intellectual property on the other. A renewed commitment to investing in security alongside an uncertain direction on how to improve practices.

Given the enormous changes and challenges wrought by today's evolving threat ecosystem, it's not entirely surprising that the way forward is ambiguous.

One thing is certain: Yesterday's security defenses are not effective against today's rapidly evolving threats. And the risks of tomorrow—uncertain at best and perilous at worst—will demand a completely new model of information security.

We suggest an evolved approach to what security can be, one that is driven by knowledge of threats, assets, and adversaries. One in which security incidents are seen as a critical business risk that may not always be preventable, but can be managed to acceptable levels.

We call this model Awareness to Action. At its most basic, this approach comprises four key precepts:

- **Security is a business imperative:** Effective security requires that you understand the exposure and potential business impact associated with operating in an interconnected global business ecosystem. An integrated security strategy should be a pivotal part of your business model; security is no longer simply an IT challenge.
- **Security threats are business risks:** You should view security risks as organizational threats. It is critical to anticipate these threats, know your vulnerabilities, and be able to identify and manage the associated risks. Ensure that suppliers, partners, and other third parties know—and agree to adhere to—your security policies and practices.
- **Protect the information that really matters:** Effective security requires that you understand and adapt to changes in the threat environment by identifying your most valuable information. Know where these "crown jewels" are located and who has access to them at all times, and proficiently allocate and prioritize your organization's resources to protect its most valuable information.
- **Gain advantage from Awareness to Action:** In this new model of information security, all activities and investments should be driven by the best-available knowledge about information assets, ecosystem threats and vulnerabilities, and business-activity monitoring. You should create a culture of security that starts with commitment of top executives and cascades to all employees and third parties. Engage in public-private collaboration with others for enhanced threat intelligence.

We can help you understand the implications of this new approach to information security and apply the concepts to the unique needs of your business, your industry, and your threat environment. Let us show you how to effectively combat the security threats of today and plan for those of tomorrow.

For more information, please contact:

Gary Loveland
Products & Services Industries
949 437 5380
gary.loveland@us.pwc.com

John Hunt
Public Sector
703 918 3767
john.d.hunt@us.pwc.com

Mark Lobel
Products & Services Industries
646 471 5731
mark.a.lobel@us.pwc.com

Dave Burg
Forensic Services
703 918 1067
david.b.burg@us.pwc.com

Joe Nocera
Financial Services Industry
312 298 2745
joseph.nocera@us.pwc.com

Dave Roath
Risk Assurance Services
646 471 5876
david.roath@us.pwc.com

Peter Harries
Health Industries
213 356 6760
peter.harries@us.pwc.com

Or visit: www.pwc.com/gsiss2014 to explore the data for your industry and benchmark your organization.