www.pwc.com/pl/risk

Eye of the storm

Key findings from the 2012 Global State of Information Security Survey®

Advisory Services Security

As the global economy stalls again—and cyber crime and other threats to information security cloud the horizon—many see sunshine overhead.

pwc

Methodology

The 2012 Global State of Information Security Survey® is a worldwide security survey by PwC, ***CIO Magazine*** *and* ***CSO Magazine****. It was conducted online between February 10 and April 18, 2011. Readers of* ***CIO*** *and* ***CSO Magazines*** *and clients of PwC from around the globe were invited via email to take the survey. The results discussed in this report are based on the responses of more than 9,600 CEOs, CFOs, CISOs, CIOs, CSOs, vice presidents and directors of IT and information security from 138 countries. Twenty-nine percent (29%) of respondents were from North America, 26% from Europe, 21% from South America, 20% from Asia, and 3% from the Middle East and South Africa. The margin of error is less than 1%.*

Rapidly intensifying tropical depressions can develop a small, clear, and circular eye. These eyes can range in width from 2 to 200 miles.

But eyes typically exhibit significant fluctuations in intensity and can create headaches for forecasters.[1]

Predictions aside, what matters most is preparation.

[1] National Hurricane Center

Table of contents

The heart of the matter

The economic thunderheads of 2008 have passed. But across global markets and industries, dense cloud formations still linger over revenue, growth, and margin performance.

And visibility into when and how the next cyber threat to information will emerge is poor, at best.

It's common practice, during periods of economic overcast, for companies to withhold investment in new markets and capabilities, and even maintenance of existing operations—that is, until the forecast for revenues robust enough to cover significant portions of the investment become more compelling.

That strategy doesn't work for information security. After all, the cyber risks that threaten information often increase during contractions in the business cycle. This is especially true when funding crucial to maintaining the integrity of information security practices freezes up or gets pushed over to support other facets of the business.

So how are companies addressing information security imperatives right now? While the economic thunderheads of 2008 have passed, clouds still loom over revenue, growth and margin performance—and the global economic forecast for the next year doesn't appear promising.

Nonetheless, according to the results of the 2012 Global State of Information Security Survey®, the majority of executives across industries and markets worldwide are confident in the effectiveness of their organization's information security practices. This group includes more than 9,600 CEOs, CFOs, CIOs, CISOs, CSOs and other executives responsible for their organization's IT and security investments in more than 138 countries.

They have an effective strategy in place. They consider their organizations proactive in executing it. And their insights into the frequency, type and source of security breaches has leapt dramatically over the past 12 months.

Yet all is not in order. Some evidence points to a "crisis in leadership" and dangerous deficits in strategy. Capabilities across security domains are degrading. And security-related third-party risks are on the rise.

Sunshine overhead can be misleading—especially when it coincides with low barometric pressure. If 2008 was just the initial eyewall, there are high winds ahead—and much preparation to complete. And, given the growing strength of the updrafts across many dimensions of cyber crime—from Advanced Persistent Threats (APT) to the sudden leaks of massive volumes of confidential data—the reasons to do so quickly and strategically are mounting.

Why are executives confident, and where have organizations made progress in addressing information security over the past year? What are the signs of vulnerability and weakness in security-related capabilities? And which priorities and opportunities should executives address now in order to prepare for the cyber threats ahead?

An in-depth discussion

Threats to security—like the weather—are hard to predict.

Many executives point to the sunshine and clear skies overhead. Others eye the low barometric pressure.

I. A world of front-runners: Respondents categorize their organization

Finding #1

This year, a surprisingly high percentage of respondents consider their organization, in effect, a "front-runner" in information strategy and execution.

Finding #2

These "front-runners" see client requirement as the greatest justification for information security spending—and are passionate about protecting data.

Finding #3

Curiously, "strategists" are far more likely to clamp down on funding for information security than any of the other three groups.

Finding #1. This year, a surprisingly high percentage of respondents consider their organization, in effect, a "front-runner" in information strategy and execution.

Two of the most crucial drivers of information security effectiveness are (1) whether an organization has an effective information security strategy in place, and (2) whether it is proactive in executing it. We often encounter companies, for example, that "have a plan but don't act on it" or do not have a plan and are constantly in "fire-fighting" mode, among other combinations of these variables.

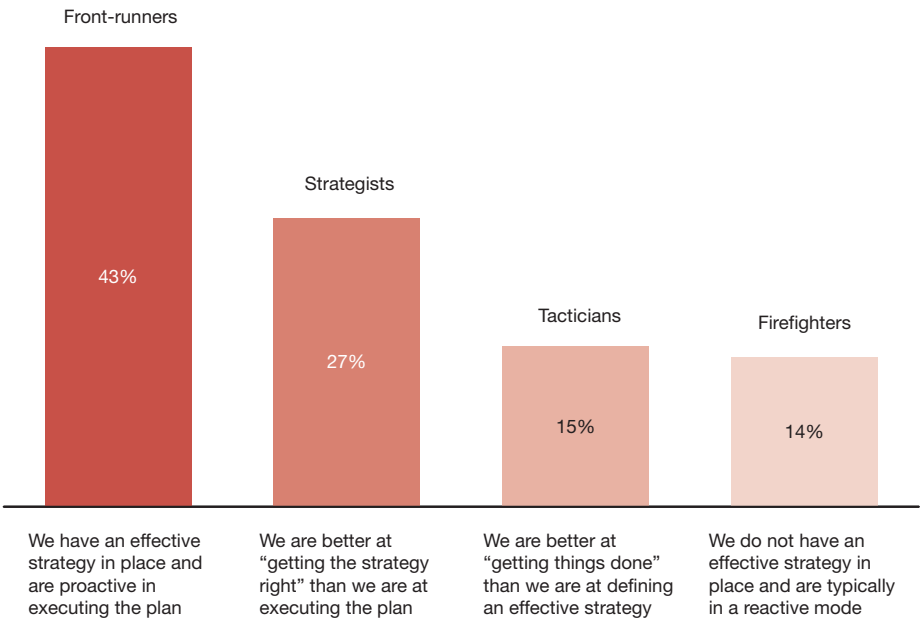
Curious about how this year's more than 9,600 respondents would categorize their organization's approach to protecting information security, we asked the question directly—and then, for analytical purposes, organized respondents as belonging to one of four groups: Front-runners, Strategists, Tacticians and Firefighters.

Surprisingly, nearly half (43%) identified themselves, in effect, as Front-runners—i.e., their "organization has an effective strategy in place and is proactive in executing the plan."

Another 27% identified themselves, in effect, as Strategists—i.e., "better at 'getting the strategy right' than executing the plan." Only 15%—the group we label Tacticians—agreed that they are "better at 'getting things done' than they were at defining an effective strategy." And the 14% that we call Firefighters admitted that they do not have an effective strategy in place and are typically in a reactive mode. (Figure 1)

What does this data tell us? After all, from a statistical perspective, it bears no resemblance to the bell-shaped curve of the standard normal distribution. The data does, however, give us some intriguing insights into perceptions—and how respondents view some key facets of their organizations' security stances.

Figure 1: How survey respondents characterize their organization's approach to information security



Source: The 2012 Global State of Information Security Survey®
Numbers reported may not reconcile exactly with raw data due to rounding.

Finding #2. These "front-runners" see client requirement as the greatest justification for information security spending—and are passionate about protecting data.

All four of these groups agreed that the two most important business issues or factors driving their information security spending were economic conditions and the need to ensure business continuity and disaster recovery.

But when asked about how information security is "justified" in their organization, the responses varied markedly. (Figure 2)

While Strategists, Tacticians and Firefighters point first and foremost to legal and regulatory requirements—the "stick", as it were—Front-runners are significantly more likely to point to the "carrot" or client requirement.

Similarly, Front-runners are clearly more passionate about protecting all kinds of information—from financial data and intellectual property to company, customer and employee information. (Figure 3)

These are interesting, and maybe even exciting, results. While the leadership pool is a bit statistically crowded, this is a welcome sign, as we first pointed out last year, that after 15 years or so, the leading edge of information security practices continue to take on a far more customer-facing, business-supporting, strategic value-building role.

Figure 2: How information security is justified

	Front-runners	Strategists	Tacticians	Firefighters
Client requirement	50%	32%	27%	21%
Legal or regulatory requirement	45%	36%	44%	24%
Professional judgment	43%	36%	37%	22%
Potential liability or exposure	41%	30%	40%	22%
Common industry practice	41%	35%	30%	17%

Source: The 2012 Global State of Information Security Survey®
Not all factors shown. Totals do not add up to 100%.

Figure 3: Percentage of respondents who consider the following types of information extremely important

	Front-runners	Strategists	Tacticians	Firefighters
Customer information	73%	57%	63%	45%
Financial data	65%	43%	48%	40%
Intellectual property and trade secrets	63%	42%	42%	34%
Corporate information	60%	41%	42%	31%
Employee information	51%	37%	40%	28%

Source: The 2012 Global State of Information Security Survey®
Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

Finding #3. Curiously, "strategists" are far more likely to clamp down on funding for information security than any of the other three groups.

There are other provocative insights embedded in the responses presented by these four sets of respondents. One of them, in fact, pulls the curtain back on a trend in global information security practices and cyber crime prevention that has persisted since 2008—that is, the reluctance to commit scarce funds to the information security mission, even at the risk of degradation in security-related capabilities.

All four of these groups—Front-runners, Strategists, Tacticians, and Firefighters—are actively reducing budgets for security initiatives and deferring security-related initiatives. But one group in particular—the Strategists—is doing so at a dramatically higher rate. (Figure 4)

Why? We have a few clues. With hard-won insights into the frequency, type and source of security breaches and cyber crimes, Front-runners are most likely to report financial losses. At the other end of the spectrum, Firefighters are typically smaller firms and, understandably, more likely to be financially constrained.

What about Tacticians? If you don't have an effective strategy in place, you're not likely to have strategic insight into why funding is critical and these valuable investments should be made.

So why are Strategists so spectacularly more likely than any other group to tighten the purse strings on information security? It's hard to know. Maybe some, without a sustained focus on execution, are simply not seeing the value of results on the ground. And perhaps others are confident in their strategy and simply focusing spending exclusively on the most important areas.

Figure 4: Percentage of survey respondents who report that their organization is reducing budgets for security initiatives or deferring initiatives

Has your company deferred any security-related initiatives?	Front-runners	Strategists	Tacticians	Firefighters
Yes, for initiatives requiring capital expenditures	47%	69%	54%	37%
Yes, for initiatives requiring operating expenditures	44%	67%	48%	36%

Has your company reduced the cost for any security-related initiatives?	Front-runners	Strategists	Tacticians	Firefighters
Yes, for initiatives requiring capital expenditures	47%	69%	52%	35%
Yes, for initiatives requiring operating expenditures	47%	68%	50%	36%

Source: The 2012 Global State of Information Security Survey®
Not all factors shown. Totals do not add up to 100%.

II. Confidence and progress: A decade of maturation

Finding #4

A clear majority of respondents are confident that their organization's information security activities are effective.

Finding #5

Companies now have greater insights than they've ever had into cyber crimes and other incidents—and they're translating this information into investments specifically focused on three areas: prevention, detection and web-related technologies.

Finding #6

After three years of cutting information security budgets and deferring security-related initiatives, respondents are "bullish" about security spending.

Finding #4. A clear majority of respondents are confident that their organization's information security activities are effective.

More than seven out of ten respondents admit they feel confident, at some level, in the effectiveness of their organization's information security capabilities. (Figure 5)

That makes sense. After all, information security—as a critical business function better understood now than at any time in the past several decades—isn't a "patchwork of technical guesses" any longer. Or merely a line item in the CIO's budget.

In many respects, the survey's respondents appear to believe, in effect, that "in our organization—given what we know about cyber crime, data breaches and other threats—information security is doing its job."

Figure 5: Percentage of respondents who are confident in the effectiveness of their organization's information security activities

Source: The 2012 Global State of Information Security Survey®

Finding #5. Companies now have greater insights than they've ever had into cyber crimes and other incidents—and they're translating this information into investments specifically focused on three areas: prevention, detection and web-related technologies.

Just a few years ago, almost half of this survey's respondents couldn't answer the most basic questions about the nature of security-related breaches. (Figure 6)

Now, approximately 80% or more of respondents can provide specific information about security event frequency, type, and source.

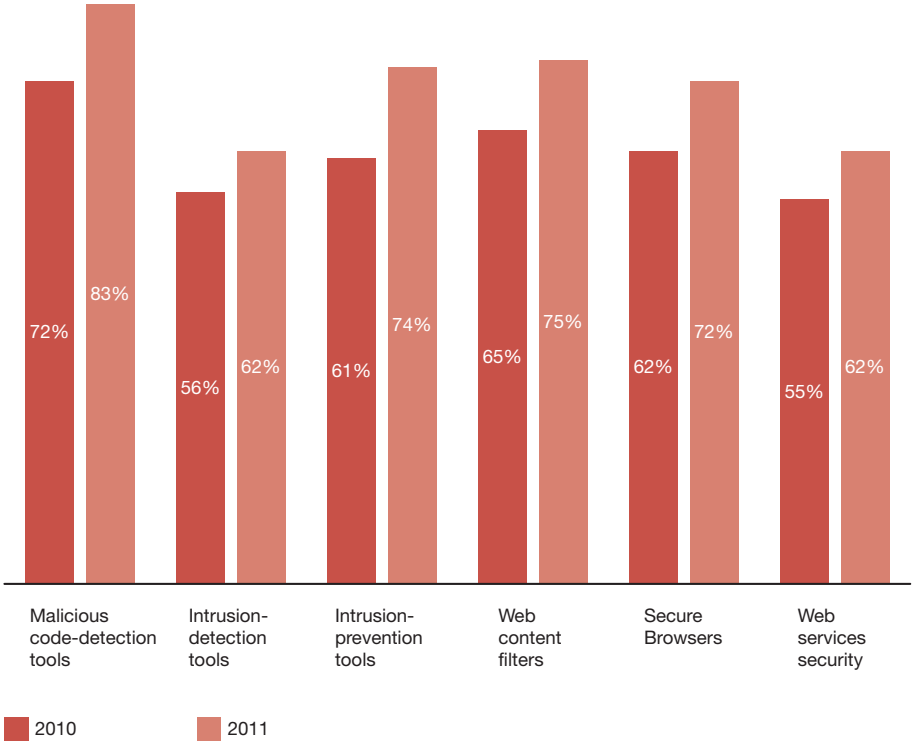
That's a huge gain in perspective—and it appears to be influencing where organizations are placing their bets, at a time when funding to support the function is not as freely available as it was before 2008. Where exactly are these investments being made? In prevention, detection and web-related technologies—three sets of capabilities that, across regions, industries and organizational size, are attracting more sunshine this year than any single other core security-related area. (Figure 7)

Figure 6: Percentage of respondents who cannot answer ("do not know", "unknown") questions about the frequency, type and source of security breaches over the last 12 months

Respondents who answered "Do not know" or "Unknown"	2007	2008	2009	2010	2011
How many incidents occurred in past 12 months?	40%	35%	32%	23%	9%
What type of incident occurred?	45%	44%	39%	33%	14%
What was the source of the incident?	N/A	42%	39%	34%	22%

Source: The 2012 Global State of Information Security Survey®
Totals do not add up to 100%.

Figure 7: Percentage of respondents who report information security safeguards related to the following detection, prevention and web-related areas



Source: The 2012 Global State of Information Security Survey®
Not all factors shown. Totals do not add up to 100%.

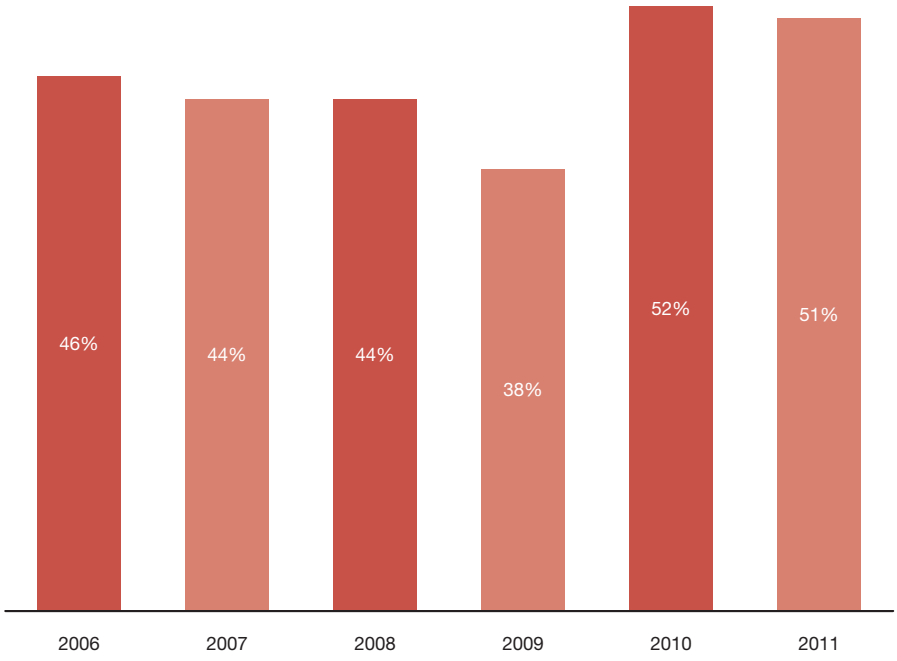
Finding #6. After three years of cutting information security budgets and deferring security-related initiatives, respondents are "bullish" about security spending.

Is the spending drought about to ease? Half of all respondents believe that it will, at some point over the next 12 months. (Figure 8)

What isn't fully clear is which factors are driving this level of expectation. Some respondents may be anticipating that fiscal restraints will relax in the months ahead, perhaps because business is better. Others may base their forecast on need—and the belief that, given the evolving profile of cybercrime and the threat environment, funding "has to improve."

What is evident, however, is that many of the vulnerabilities that began emerging last year, two years after the global economic downturn, are still present—and, just like shutters banging as the winds increase, demanding attention.

Figure 8: Percentage of respondents who believe that information security spending will increase over the next 12 months



Source: The 2012 Global State of Information Security Survey®

III. Vulnerability and exposure: Capability degradation since 2008

Finding #7

One of the most dangerous cyber threats is an Advanced Persistent Threat attack. Few organizations have the capabilities to prevent this.

Finding #8

After three years of economic volatility—and a persistent reluctance to fund the security mission—degradation in core security capabilities continues.

Finding #9

Managing the security-related risks associated with partners, vendors and suppliers has always been an issue. It's getting worse.

Finding #10

That 72% worldwide confidence rating in security practices may seem high—but it has declined markedly since 2006.

Finding #7. One of the most dangerous cyber threats is an Advanced Persistent Threat attack. Few organizations have the capabilities to prevent this.

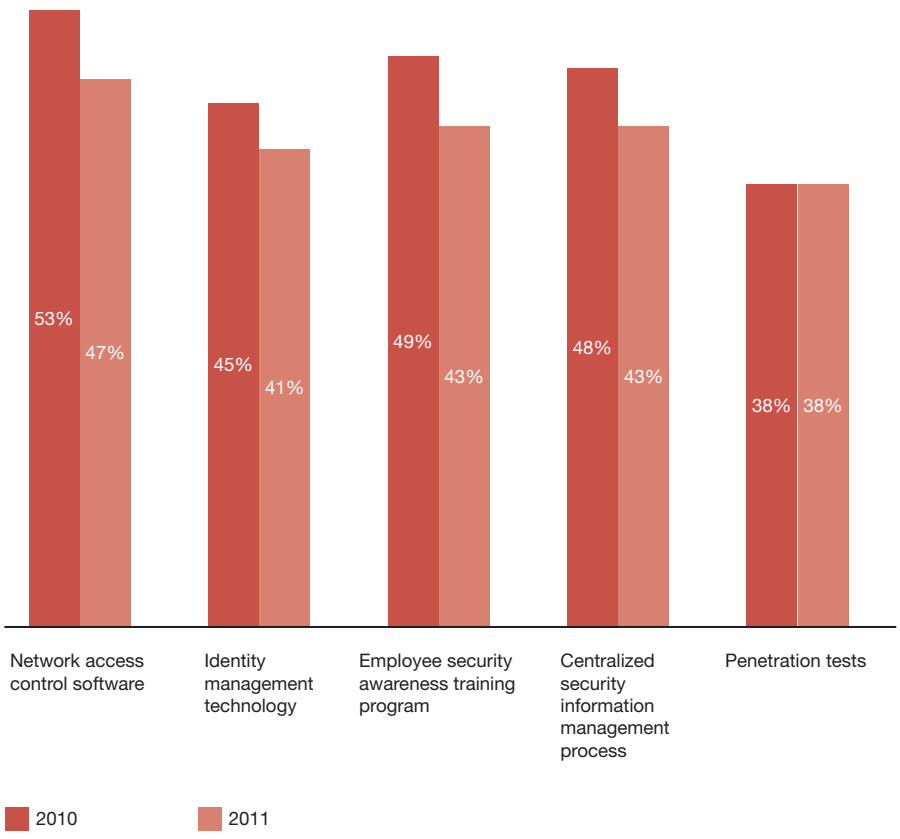
The most sophisticated, adaptive and persistent class of cyber threats is no longer a rare event. In the few short months since this survey was launched on February 10, 2011, for example, leading organizations worldwide have been targeted by Advanced Persistent Threat attacks. These entities include national governments, nuclear laboratories, security firms, military contractors and an international organization that oversees the global financial system.

Yet APT isn't just a threat to the public sector and the defense establishment. It's an increasingly urgent issue for the private sector as well.

This year, significant percentages of respondents across industries agreed that APT drives their organization's security spending. These included 43% of consumer products and retail respondents, 45% of financial services respondents, 49% of entertainment and media respondents and 64% of respondents from the industrial manufacturing sector.

Are companies prepared? Only 16% of respondents say their organization's security policies address APT. In addition, more than half of all respondents report that their organization does not have core capabilities directly or indirectly relevant to countering this strategic threat—such as penetration testing, identity management technology or a centralized security information management process. (Figure 9)

Figure 9: Percentage of respondents who report that their organization has the following APT-related capabilities in place



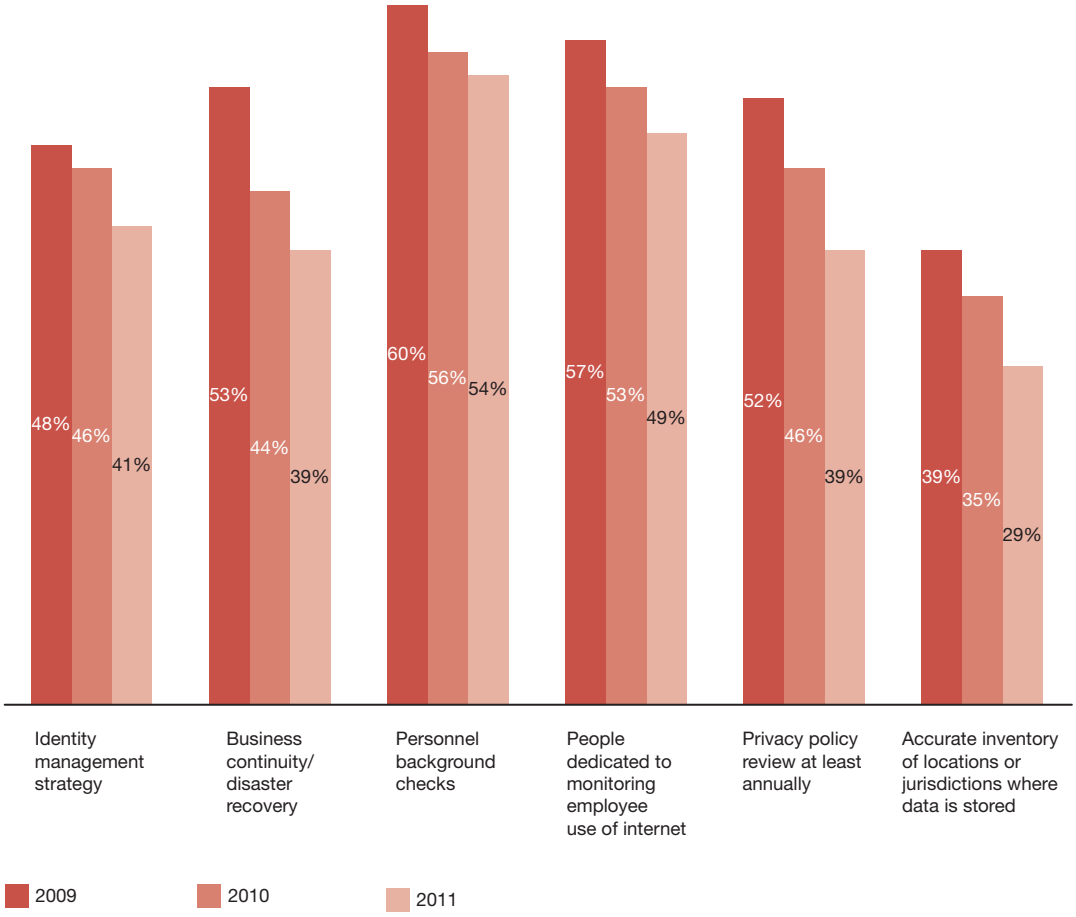
Source: The 2012 Global State of Information Security Survey®
Not all factors shown. Totals do not add up to 100%.

Finding #8. After three years of economic volatility—and a persistent reluctance to fund the security mission—degradation in core security capabilities continues.

While the gains in capabilities associated with prevention, detection and web-related technologies are pronounced, maturity levels for other processes and technologies continue to decline.

This degradation is evident across capabilities such as identity management and business continuity / disaster recovery as well as personnel background checks, and the dedication of resources to monitoring employee use of the Internet and information assets. It's also evident across privacy-related assets and practices such as reviewing privacy policies at least annually and maintaining an accurate inventory of locations or jurisdictions where data is stored.

Figure 10: Percentage of respondents who report that their organization has the following security- and privacy-related capabilities in place



Source: The 2012 Global State of Information Security Survey®
Not all factors shown. Totals do not add up to 100%.

Finding #9. Managing the security-related risks associated with partners, vendors and suppliers has always been an issue. It's getting worse.

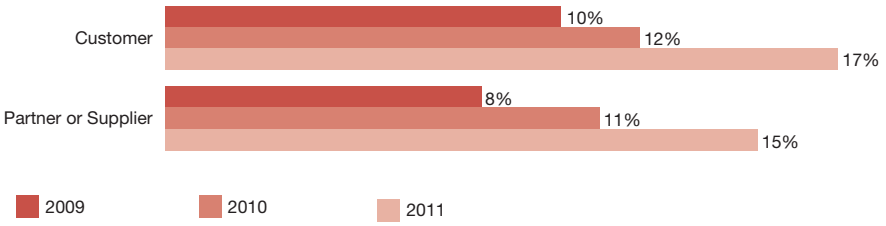
Insider risk has always been a focus for CISOs, CSOs and others charged with "protecting the house." For years, the most commonly suspected source of breaches has been employees, both current and former. And they still are. But less attention is typically paid to other classes of insiders, such as partners and suppliers, and—since many companies invite customers inside their network perimeters—customers as well.

That has been a weakly rational strategy, if only because partners, suppliers and customers have for many years, ranked "low on the suspicion list."

That's changing. And fast. (Figure 11)

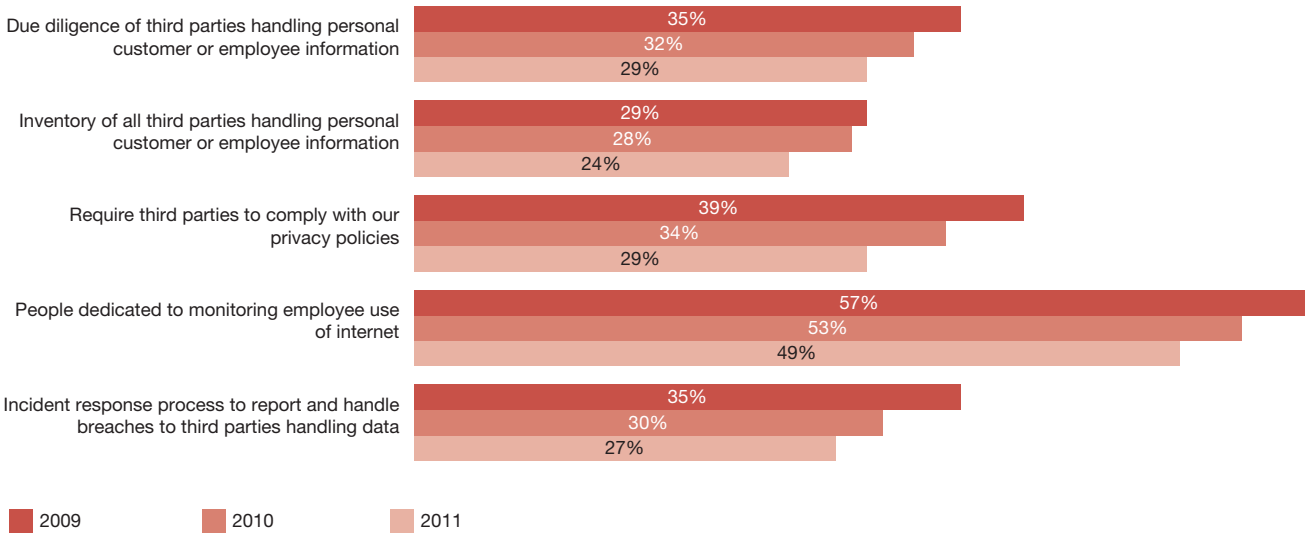
What *should* change quickly—and now with suspicions rising, they may very well over the next 12 months—are the maturity levels for a host of security capabilities that together represent the "front line" in managing third party-related risk. (Figure 12)

Figure 11: Percentage of respondents who estimate the following as the source of breaches



Source: The 2012 Global State of Information Security Survey®

Figure 12: Percentage of respondents who report that their organization has the following capabilities in place to counter the risks associated with third parties



Source: The 2012 Global State of Information Security Survey®
Not all factors shown. Totals do not add up to 100%.

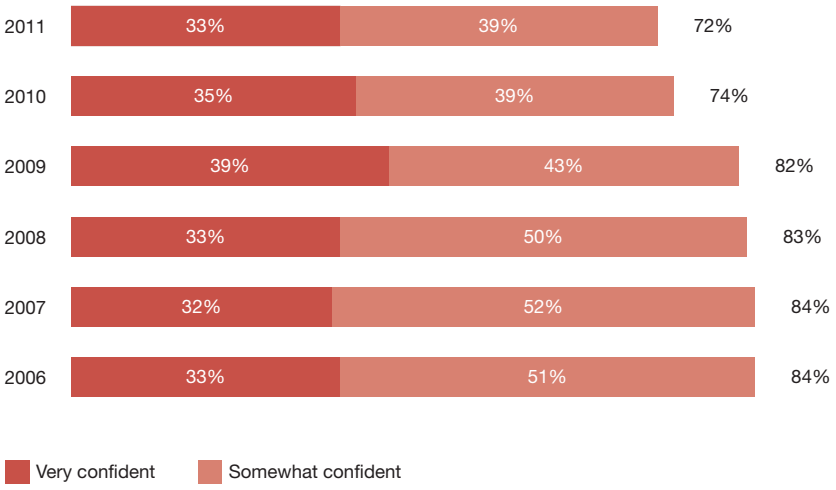
Finding #10. That 72% worldwide confidence rating in security practices may seem high—but it has declined markably since 2006.

Confidence is usually a good trait—as long as it isn't based on hubris, hope or inaccurate information.

But a decline in confidence is telling. That 72% confidence rating worldwide may appear to reflect robust levels of self assurance—at least with respect to information security. But it's actually 12 points lower (84% in 2006) than it was a few years ago. (Figure 13)

The writing is on the wall. As challenges such as the Advanced Persistent Threats and other cyber security issues continue to emerge and the funding climate remains conservative, it's impossible to avoid the conclusion that business and IT personnel across the world are less sure that their organization is prepared to confront these threats to its information, operations and brand.

Figure 13: Percentage of respondents who are confident in the effectiveness of their organization's information security activities



Source: The 2012 Global State of Information Security Survey®

IV. Windows of improvement: Where the best opportunities lie

Finding #11

What are the greatest obstacles to effective information security? Leaders point to the lack of capital, among other factors—and shine the spotlight hottest at the "top of the house."

Finding #12

Mobile devices and social media represent a significant new line of risk—and defense. New rules are in effect this year for many organizations, though not yet the majority.

Finding #13

Cloud computing is improving security. But many want better enforcement of provider security policies, among other priorities.

Finding #11. What are the greatest obstacles to effective information security? Leaders point to the lack of capital, among other factors—and shine the spotlight hottest at the "top of the house."

This is a fascinating question because it reveals a rich mixture of organizational misalignment and dysfunction as well as enticing opportunities to improve information security across external challenges, internal resources and key leadership roles.

Chief Executive Officers (CEOs) believe the primary obstacle is the lack of capital and point next to themselves and the Board. That reflects honesty, and certainly accountability. Here's the surprise: the last-ranked "obstacle" on their list is the Chief Information Security Officer (CISO). This, apparently, is an illusion—as the CISOs, themselves, indirectly reveal in their answers to this question. (Figure 14)

What about Chief Financial Officers (CFOs)? It would be natural to anticipate that, with a gate-keeping role on the type of security investments being cancelled, cut back or deferred, they would, like the CEOs, list capital constraints as the leading obstacle. They don't. They too place the onus on the CEOs and the Board.

So how do leading representatives of the "technical executive team"—the Chief Information Officer (CIO) and the CISO—rank the greatest obstacles to the effectiveness of information security? Interestingly, and perhaps naturally—they place themselves at the bottom of the list and the CEO and Board very near the top. But the CIO and CISO apparently agree that the single greatest obstacle to information security is the lack of an actionable vision for the function, followed closely by the lack of an effective information security strategy.

On the one hand, the irony is hard to miss: if defining a clear vision and strategy isn't the CISO's job, whose is it? On the other hand, the opportunity this set of responses reveals is inspiring. Funding austerity is a condition few executives can do much about. But defining a clear vision and strategy is an elective procedure.

How dramatically more effective would information security be if the entire senior executive team turned to the CISO as one and—in a highly collaborative manner—supported his or her championship of a three-to-five year vision and strategy for how the information security function should best be tasked and resourced to both enable and protect the business?

How can a CISO "make this happen"? By placing far greater emphasis on communicating the importance of information security to the CEO, CFO and other C-suite leaders and taking care to articulate this value to each of them in their own respective "languages".

Figure 14: Percentage of CEOs, CFOs, CIOs and CISOs who identify the following factors as the greatest obstacles to improving the overall strategic effectiveness of their organization's information security function

	CEO	CFO	CIO	CISO
Leadership—CEO, President, Board or equivalent	25%	27%	25%	25%
Leadership—CIO or equivalent	14%	23%	18%	21%
Leadership—CISO, CSO or equivalent	12%	22%	16%	17%
Lack of effective information security strategy	18%	25%	25%	30%
Lack of actionable vision or understanding	17%	25%	30%	37%
Insufficient funding for capital expenditures	27%	23%	29%	29%
Insufficient funding for operating expenditures	23%	16%	23%	22%
Absence or shortage of in-house technical expertise	23%	19%	25%	23%
Poorly integrated or overly complex information/ IT systems	13%	14%	19%	30%

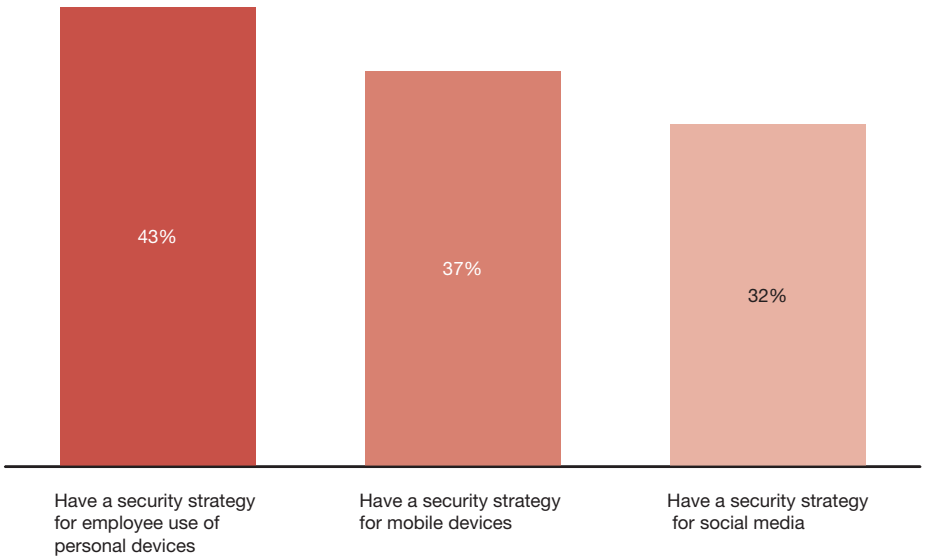
Source: The 2012 Global State of Information Security Survey®
Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

Finding #12. Mobile devices and social media represent a significant new line of risk—and defense. New rules are in effect this year for many organizations, though not yet the majority.

Many organizations worldwide are implementing strategies to keep pace with employee adoption of new technologies—particularly their use of mobile devices and social-networking tools. They are also creating rules about how employees can use personal technology within the enterprise.

More than half of all respondents, however, report that their organization does not yet have a security strategy for employee use of personal devices, including mobile devices, as well as social media. (Figure 15)

Figure 15: Percentage of respondents who report that their organization has the following security capabilities in place to address risks associated with mobile devices and social media



Source: The 2012 Global State of Information Security Survey®
Not all factors shown. Total does not add up to 100%.

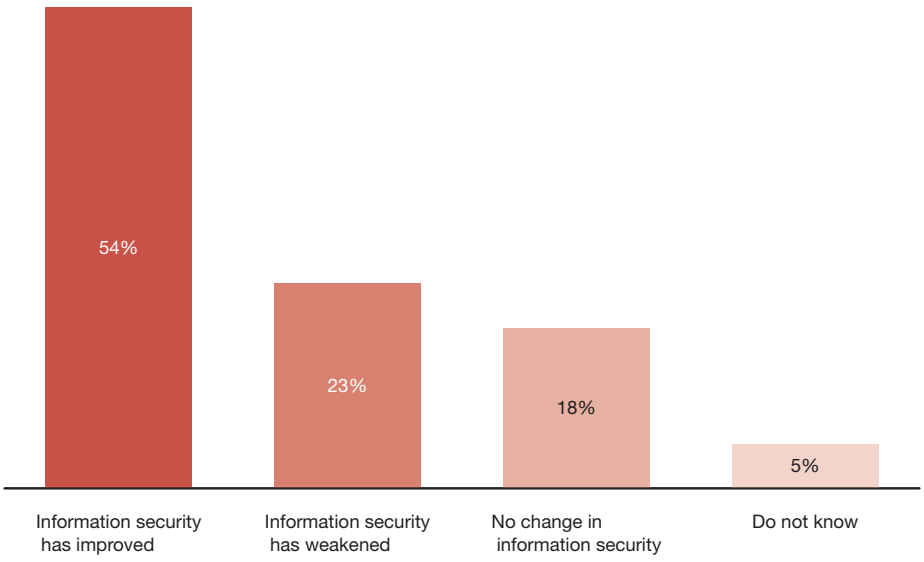
Finding #13. Cloud computing is improving security. But many want better enforcement of provider security policies, among other priorities.

More than four out of ten respondents report that their organization uses cloud computing—69% for software-as-a-service, 47% for infrastructure-as-a-service and 33% for platform-as-a-service.

Has the cloud improved security? More than half (54%) say it has, 23% believe that security has "weakened" and 18% see no change. (Figure 16)

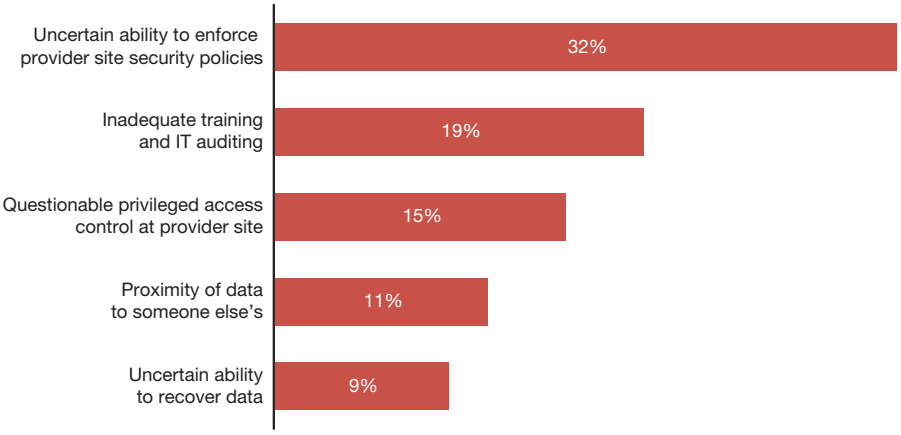
What about the greatest risks to cloud computing strategies? The largest one is perceived to be the uncertain ability to enforce provider security policies. Others include inadequate training and IT auditing, questionable privileged access control at the provider site, the proximity of data to someone else's and the uncertain ability to recover data, if necessary. (Figure 17)

Figure 16: The impacts of cloud computing on information security



Source: The 2012 Global State of Information Security Survey®

Figure 17: Percentage of respondents who identify the following as the greatest security risk to their organization's cloud computing strategy



Source: The 2012 Global State of Information Security Survey®
Not all factors shown. Total does not add up to 100%.

V. Global trends: Asia races ahead while the world's information security arsenals age

Finding #14

For several years, Asia has been firing up its investments in security. This year's results reveal just how far the region has advanced its capabilities.

Finding #15

As North American organizations continue their reluctance to fund security's mission at levels that they have in the past, capabilities continue to degrade.

Finding #16

In the face of economic uncertainty and in spite of a portfolio of security capabilities in decline, Europe pulls the purse strings even tighter.

Finding #17

Like most of the world, South America's armory of information security defenses is rusting. As the region's confidence in its security plummets, it thirsts for cash.

Finding #14. For several years, Asia has been firing up its investments in security. This year's results reveal just how far the region has advanced its capabilities.

Two years ago, as much of the world slowed or froze its funding for security, Asia began firing up its investment in this critical area. This year's data—compared to 2009 response levels, for example—reveals just how remarkably far Asia has advanced its own capabilities over a short 24-month period.

The numbers are dramatic. First of all, the region's insights into security incidents has soared as the percentages of Asian respondents who could not answer questions about the number, type and likely source of incidents have collapsed—in some cases, into the single-digit range.

With new visibility into incidents has come new awareness about the value of information security. Three out of every four Asian respondents (74%)—higher than response levels for any other region in the world—now agree that the increased risk environment fueled by the global economic downturn over the last few years has elevated the role and importance of the security function.

Not surprisingly, Asia's investments in security have continued—with remarkable results. While gains in capabilities are evident virtually across the board, some of the most significant since 2009 include greater-than-10-point surges in areas such as security strategy, privacy practices, intrusion and detection technologies, web-related defenses and data protection measures.

Not content to rest on its laurels, Asia's commitment to information security is likely to intensify over the next year. The number of Asian respondents who expect security funding to increase over the next 12 months has leapt from 53% in 2009 to 74% this year—an expectation rate far higher than any other region in the world. (Figure 18)

Finding #15. As North American organizations continue their reluctance to fund security's mission at levels that they have in the past, capabilities continue to degrade.

In sharp contrast to the trends evident in Asia, North America's long-term track record of advances in information security has begun to erode. In fact, many cracks in North America's information security defense are starting to appear.

Like Asia and other regions of the world, North American organizations are gaining insights into incidents and reporting higher levels of impacts to the business. But instead of strengthening their commitment to information security, the region's organizations are less likely to champion the importance of the security function than they were in 2009.

There are a few signs of new strength—to be sure—especially with respect to some detection, prevention and web-related technologies. Adoption rates for malicious code detection tools, for example, surged from 78% in 2009 to 86% this year.

Yet for the second year in a row, many of North America's capabilities appear to be slipping. This is true with respect to areas such as strategy, identity management and access control, data protection, third-party security and even security-related compliance capabilities. (Figure 18)

Figure 18: Differences in regional information security practices

	Asia		North America	
	2009	2011	2009	2011
Security spending will increase over next 12 months	53%	74%	29%	31%
Increased risk environment has elevated importance of security function	62%	74%	50%	45%
Don't know number of security incidents in past 12 months	21%	3%	41%	17%
Don't know types of security incidents in past 12 months	30%	6%	47%	20%
Don't know estimated likely source of incidents in past 12 months	32%	17%	45%	37%
Have overall security strategy in place	66%	76%	73%	58%
Use identity management solutions	49%	62%	47%	33%
Dedicate security personnel to internal business departments	48%	61%	42%	36%
Have malicious code detection tools	70%	81%	78%	86%
Have tools to discover unauthorized devices	54%	65%	57%	58%
Have vulnerability scanning tools	55%	71%	59%	59%
Have established a written privacy policy	59%	70%	65%	57%
Conduct due diligence of third parties handling personal data	33%	43%	45%	27%
Use data loss prevention (DLP) tools	44%	57%	49%	48%
Encrypt databases	65%	76%	59%	50%
Use secure browsers	63%	78%	68%	77%
Have implemented web services security	57%	71%	58%	58%

Source: The 2012 Global State of Information Security Survey®
Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

Finding #16. In the face of economic uncertainty and in spite of a portfolio of security capabilities in decline, Europe pulls the purse strings even tighter.

Europe is not having an easy time maintaining the strength of its information security practices. Asked about the impacts of current economic conditions on the security function, European respondents are much more likely this year than in 2009 to tick off a list of consequences.

They report that the regulatory environment has become more complex and burdensome. Risks to data have increased due to employee layoffs. And cost reduction efforts are making adequate security more difficult to achieve, among other impacts.

The year ahead may be even more difficult—from a security perspective. Compared to 2009, European organizations are significantly more likely to defer initiatives and reduce budgets for security-related capital and operating expenditures.

The news isn't all bad, however. Like other regions in the world, Europe has gained new insights into the type, frequency and source of incidents. It has made gains over the last year in prevention, detection and web-related technologies. And it is more likely to employ a Chief Information Security Officer than at any time in the past.

Yet one of the red flags of concern for the coming year is clearly third-party risk—and the perception that business partners and suppliers have weakened over the last several years. This risk is even greater for Europe, in general, than it is for other global regions, as Europe's third-party related security controls and countermeasures lag behind those in the rest of the world. (Figure 19)

Finding #17. Like most of the world, South America's armory of information security defenses is rusting. As the region's confidence in its security plummets, it thirsts for cash.

While the economy's negative impacts on information security appear to be easing in South America, most of the region's reported levels are just as high—or even higher—than those reported in Europe. That helps explain, perhaps, why financing for security remains extremely tight. In fact, budget deferrals and cut-backs for security initiatives have increased enormously since 2009.

Point by point, reported levels for key capabilities in the region keep declining—for both privacy and security measures and across people- and process-related competencies. Some of these declines are incremental—such as conducting personnel background checks, which slipped from 55% in 2009 to 53% this year. Other declines are precipitous—such as the reduction from 50% to 38% in respondents who report that their organization uses a centralized security information management process.

Two key metrics, at least, improved this year. South American organizations are more likely than in 2009 to have a CISO at the helm and have an overall information security strategy in place.

These are positive developments, especially given another revelation in this year's survey results. South Americans reported a tremendous decline in confidence in the effectiveness of their organization's information security (71% vs. 89% in 2009) and in that of their partners and suppliers (70% vs. 86% in 2009). (Figure 19)

Figure 19: Differences in regional information security practices

	Europe		South America	
	2009	2011	2009	2011
Regulatory environment has become more complex and burdensome	47%	53%	61%	58%
Risks to the company's data have increased due to employee layoffs	34%	42%	52%	48%
Cost reduction efforts make adequate security more difficult to achieve	42%	46%	61%	53%
Threats to the security of our information assets have increased	32%	38%	50%	44%
Our business partners have been weakened by the economic conditions	33%	51%	53%	48%
Our suppliers have been weakened by the economic conditions	33%	48%	52%	46%
Deferred initiatives for security-related capital expenditures	39%	56%	49%	68%
Deferred initiatives for security-related operating expenditures	35%	54%	44%	63%
Reduced budgets for security-related capital expenditures	43%	57%	50%	66%
Reduced budgets for security-related operating expenditures	41%	56%	48%	66%
Have overall security strategy in place	59%	59%	56%	60%
Employ Chief Information Security Officer	45%	51%	45%	53%
Implemented a centralized security information management process	43%	34%	50%	38%
Conduct personnel background checks	44%	44%	55%	53%
Have inventory of all 3rd parties handling employee/customer personal data	20%	18%	27%	25%
Require third parties to comply with our privacy policies	31%	22%	32%	28%
Use intrusion detection tools	50%	58%	59%	57%
Have web content filters	55%	72%	64%	72%
Are confident that our organization's information security is effective	73%	62%	89%	71%
Are confident that our partners/suppliers' information security is effective	65%	62%	86%	70%

Source: The 2012 Global State of Information Security Survey®
Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

What this means for your business

Look at the leaders. Learn from what they have done—and how they are electing to address the future.

Revisiting the reams of data generated by this survey, we carved out a much narrower bracket of respondents. We based this bracket on responses to four questions selected from a short list we believe reflects the hard-won insights, trade-offs and commitments that set apart executives and organizations we consider leaders in information security.

A new working definition of a leader

Included in our "leader cut" was any respondent who reported that their organization has:

- An overall information security strategy in place;
- Their CISO or equivalent security leader reporting to the "top of the house"—i.e., either the CEO, the CFO, the COO or legal counsel;
- Both measured and reviewed the effectiveness of its information security policies and procedures within the past year; and,
- An understanding of exactly what type of security events have occurred over the past 12 months.

The profile of our new "leadership" group

This group is 13% of the survey. Forty percent of them (40%) are business executives and 60% are IT executives. Regionally, 39% are from Asia, 25% from South America, 19% from Europe and 16% from North America. The industries most represented are technology (15%), industrial manufacturing (13%), and financial services (10%)—followed by engineering and construction (9%), telecommunications (8%) and consumer products and retail (8%). Interestingly, the industries with low participation levels in this bracket include health (4%), government (4%), energy and utilities (4%) and aerospace and defense (2%).

What these leaders are seeing—and doing—that's different

They're reporting half as many incidents, on average (1,274 per year vs. 2,562 for all survey respondents). Yet they're encountering significantly higher levels of exploitation—of data (45% vs. 26%), of mobile devices (36% vs. 23%), of applications (30% vs. 20%), of systems (40% vs. 29%) and of networks (40% vs. 28%).They're also much more likely to suspect that the attacks are initiated by employees (38% vs. 32%), former employees (41% vs. 26%) and hackers (50% vs. 35%).

How are they addressing these risks? Not surprisingly, they report capability levels that are, on the whole, 15 to 25 percentage points higher than survey averages. This gap narrows to approximately 10 points in the few areas where many companies have been concentrating their investments this past year: prevention, detection and web-related technologies.

The greatest gaps between these leaders' responses and those of the survey as a whole are, among others, the following:

- Employ a CISO (84% vs. 45%)
- Employ a CSO (75% vs. 40%)
- Have an overall information security strategy (100% vs. 63%)
- Both measured and reviewed the effectiveness of security policies and procedures over the past year (100% vs. 54%)
- Employ dedicated security personnel who support internal business departments (72% vs. 46%)

Finally, 93% of these leaders have confidence in the effectiveness of their information security. What about spending expectations for the next twelve months? Three out of four (76%) expect it to increase.

The implications for your business

As interesting as these results may be, they don't represent a fully actionable roadmap for your business or any other. The preparations these leaders are making are based on a broader foundation of capabilities than most organizations enjoy—one that has taken years to develop. And it's been carefully crafted to reflect each of their organizations' unique business requirements and outlooks.

Instead, use this information to help define a vision for your information security program. Ask us for further information on this bracket of leaders in areas critical to your information, operations, and assets. Then define or refine your own information security strategy. At minimum, make sure it brings an acute and prioritized focus on these four critical elements: (1) leadership, (2) strategy, (3) alignment with the business and (4) a customer-centric approach.

www.pwc.com/pl/giss2012

For more information, please contact:

Piotr Urban
Partner
Risk Assurance Services
+48 502 18 4157
Piotr.Urban@pl.pwc.com

Adam Wnęk
Director
Risk Assurance Services
+48 502 18 4499
Adam.Wnek@pl.pwc.com

Jeremi Gryka
Senior Manager
Risk Assurance Services
+48 502 18 4472
Jeremi.Gryka@pl.pwc.com

Mariusz Walkiewicz
Manager
Risk Assurance Services
+48 502 18 4291
Mariusz.Walkiewicz@pl.pwc.com

Or visit: www.pwc.com/pl/risk